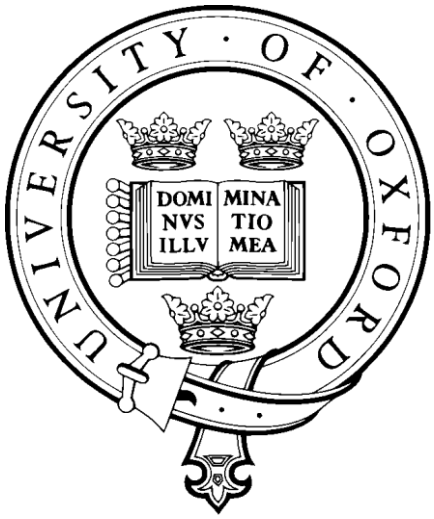


University of Oxford
Centre for Doctoral Training in Cyber Security

Managing Risk to The Media from Emerging Networked Technologies

A thesis submitted for the degree of
Doctor of Philosophy

Anjuli Radhika Kumar Shere
New College

Hilary 2023

Abstract

The consumer Internet of Things (IoT) poses unprecedented security challenges to certain sections of society, including the news media. Many consider the press to be a branch of critical national infrastructure in democracies, as attacks on journalists have implications for individual human rights and national and international security. Focussing on democratic countries, this research considers how members of the press can improve their identification of, protection from, and resilience against threats from the IoT.

This interdisciplinary research utilises mixed methods and qualitative and quantitative thematic analysis, including literature reviews, comparative case study methodologies, online surveys, and interviews. Participants include experts in journalism, cyber security, law, technology, relevant policy, and states' capabilities relating to technological exploitation.

This research includes the findings from an exploratory study to scope the novelty of focusing on journalists as a specific population threatened by the IoT. This mini-study interviewed and surveyed journalists and cyber security experts to determine how high-risk members of the media might perceive and combat consumer device threats to their work and wellbeing. This research found a sizeable gap between cyber security expertise and journalistic practice regarding risk assessment and management. Specifically, although journalists are at particularly high risks of many forms of attack, their awareness of, and protections against, IoT threats were clearly found to be limited.

Therefore, this thesis comprises a multi-piece toolkit that enables members of the press to identify threats from IoT devices to themselves and their work, and then identify the countermeasures best suited to their context.

The toolkit includes: A conceptual model to categorise IoT devices by environment (location), via systematic literature review. This model demonstrated to members of the media the scope and scale of where IoT devices may present threats. A second conceptual categorisation, also created by literature review of currently feasible capabilities and validated by surveying states' capabilities experts, explores threats to information, as well as related legal and physical threats to journalists and their work from the IoT. The main contribution of this thesis is an interactive framework of countermeasures to these IoT threats to enable members of the media to decide how to protect themselves. The countermeasures are linked to phases of the overarching editorial workflow, to ensure that their implementation is feasible and that they are clearly useful by and for specific role categories within the media.

This toolkit is also informed by the thesis' comparative profiling of the privacy, security, and data protection policy and law environments in the United Kingdom, the United States of America, Taiwan, and Australia. These profiles, combined with the recommendations of academic, governmental and non-governmental experts, and synthesis of multiple disciplines of academic literature, ensure that the toolkit created and presented in this thesis is versatile and realistic to help members of the media combat threats posed by the IoT to their societal function.

Declaration of Authorship

I declare that this thesis is entirely my own work, and except where otherwise stated, describes my own research.

Declaration of Funding

This work was funded by a doctoral training grant from the UK Engineering and Physical Sciences Research Council. This grant, titled "Cyber Security CDT Phase Two (University of Oxford)", falls under the Centre for Doctoral Training scheme and its reference number is EP/P00881X/1. The period of support for this DPhil was from October 2018 to April 2023.

Acknowledgements

I know that it is an unusual choice to include three pages of Acknowledgements, but this thesis exists because of the invaluable involvement and dedication of many people, some of whom were indispensable in getting me to this point long before I even knew of the DPhil. I cannot ever pay you all back for investing in me, but I promise I will try to pay it forward.

My brain gave up as soon as I had a first draft of this thesis and there are too many of you to write down here, so I'm sorry if I forget anyone and I promise that I will try to thank you individually. On these pages, however, given that this research has drilled into me the importance of OpSec, I've decided to try to balance that imperative with my desire to acknowledge as many people in this Acknowledgements section as possible. Therefore, not all of you will be named and some of your initials or nicknames will be included instead.

First and foremost, my deep gratitude goes to my supervisors, Professors Andrew P. Martin and Jason R. C. Nurse, for their years of guidance and honest feedback - and for their wisdom regarding taking breaks instead of having breakdowns. I would also like to thank my examiners, Professors Paul Lashmar and Dave De Roure, for turning what could have been the scariest exam of my life into one of the most affirming and enjoyable conversations I've ever had. Thank you to my milestone viva examiners, Professors Max Van Kleek, and Helena Webb, for engaging with and elevating my thinking with their insightful discussions. This thesis also grew out of my two first-year studies; my thanks go to Professors Ivan Flechais and Ian Loader for their supervision of those mini projects. I am further grateful to the Engineering and Physical Sciences Research Council and the United Kingdom Research Institute for my scholarship, without which this research would not have occurred.

It is an honour and a privilege that so many expert participants were willing to so graciously contribute their time and knowledge to this research, many of whom responded to cold emails. My thanks go to them, and to the Association for International Broadcasting (AIB) team, Simon Spanswick, Clare Dance, Di Davis and Gunda Cannon, for taking a chance on me, taking me on adventures, and then taking a keen interest in this research; I am inspired daily by the work done by the AIB. In particular, I would like to thank Tom Wragg for mentoring me at work and in life.

I owe a boundless debt to my "life supervisor", Dr. Miranda Dragon Melcher, who gave me valuable guidance from the inception of this project and has patiently waded through every draft. She is thanked in every paper I've written and should probably be thanked in my epitaph for keeping me going for so long, unflinchingly. When the world was on my shoulders, she made sure I didn't disappear under the weight. Ye savit me, Cap'n.

Similarly, I must thank my family, who imbued in me a love of stories, superheroes, and their journalist alter-egos, and who never let me avert my gaze or attention from difficult but important issues. You have comforted and convinced me, and helped me become someone who not only wanted a doctorate

but is resilient enough to actually achieve one, on a topic about which I care deeply. I hope that the person I have grown into over the course of this DPhil makes you proud. This thesis is dedicated to you.

I am so grateful to be able to undertake this research that I love. I could not have done so without some truly brilliant, caring teachers. My thanks to my referees, who have consistently facilitated my eagerness to learn: Dr. Daniel Sabbagh, Dr. Hassan Elbahtimy, Dr. Danny Steinmetz-Jenkins, Dr. Chris Pierson, Dr. Matthew Rendall, Dr. Viktoriya Fedorchak. Also, my appreciation goes to my favourite school teachers and librarians, Signora Marchini, Ms. Trinder, and Mrs. Pullin, for challenging me in the best ways.

I would like to thank people who have made undertaking this DPhil much less daunting and lonely: Dr. Jean Debarros for adroitly guiding me through the complexities of life as a doctoral researcher with unwavering joie de vivre. Alex Brown (and the DAS) for her positivity and patient assistance. David Hobbs, as "kindness" is insufficient to describe how he went above and beyond to make the CDT feel like somewhere I belonged. Maureen York for being so certain of what I brought to the CDT and for reminding me of the importance of taking time to just breathe and exist during the exhausting first year. Katherine Fletcher for her counsel regarding ethics applications and her attempts to share my research both within and outside the CDT. Janet Sadler for shepherding me through the final months of my DPhil and of the CDT, and Jordan Summers for being the best pre-viva new buddy I could have stumbled upon. Last, but never least: Dr. Barbara Haws for her spectacular and unwavering commitment to being a kind, generous and anti-racist person.

Also, of course, thank you to members of my CDT cohort for their friendship, years of commiseration, encouragement and stimulation, and a lifetime to come of knowing them as good people doing important work to protect us all. In particular: Doctors Yashovardhan Sharma, Fatima Zahrah, Anirudh Ekambaranathan, Matthew Rogers, and Claudine Tinsman.

Several people from previous cohorts also integrated me into their networks of cyber scholars and helped me find direction through their own interest in research to improve the world: my thanks to Greg Walton, and Doctors Monica Kaminska, Valentin Weber, Jamie Collier, and Ari Schuler Scott.

Regarding scholars who proposed I apply for the DPhil, I must thank soon-to-be Dr. Meghan Iverson for championing my potential. I also have to say thank you to Professor Aacha, who has given me insightful (and, yes, consistently correct) commentary that was not appreciated fully until I had grown into a grizzled fourth-year. I love you, and greatly appreciate your excellent sense of humour, meticulous attention to detail, and challenging questions.

Both within and outside the DPhil, I must particularly thank Oli Sturrock for being and providing an escape from Sunnydale, as well as all of "Oxford eat all D&D" for being the best pre-, mid-, and post-apocalyptic party of chaos mongers in all the worlds.

Even amidst a global pandemic, I benefited inestimably from diverse intellectual settings, as for the last two years of the DPhil, I moved from Oxford to Cambridge (MA). This is a dream that would not have

been accomplished at all – or as joyously – without Prof. Matthew Baum (and colleagues at the COVID States Project and Misinformation Review), Susan Ocitti-Mahoney, Dr. Marya Mtshali, Kevin Wren, Carmen Nobel (and the Journalist's Resource team), Prof. Jim Waldo, Laura Manley, Nancy Gibbs, and the rest of the fantastic core staff and Fellows at Harvard's Shorenstein Center on Media, Politics and Public Policy. I owe a very special thanks to everyone whose perspective and enthusiasm regarding my research motivated lively discussions and debates that clarified key issues.

I must also thank "The Nunnery of St. Chai" for long study and confidant sessions. Once Stateside, I was so lucky to find an in-person support network of scholars and gentlewomen who made the transition so smooth, including Diana Lysenko. I am especially thankful for "The Friends of Nim" for welcoming me home.

On the subject of being at home, my thanks go to "The Peanut Gallery" for being my favourite people with whom I've shared a flooded kitchen, a stolen Christmas tree, and a Dorian Grey-esque slice of my soul.

Speaking of a sense of belonging, my thanks go to the wonderful PBnJaM for making me feel buttressed and beloved as I finish the DPhil and start the next phase of my life.

Throughout the DPhil, I have worked on other jobs, such as the CyberPATH programme for the UK National Cyber Resilience Centre Group. My thanks go to CyberPATH's Abdullah Khan, who is an amazing manager, mentor and friend in cyber security. During the first and last summers of the DPhil, I also filmed Channel 4's Hunted and Celebrity Hunted. I want to thank my Hunter Family for giving me the confidence to believe I can do any job, anywhere, because I will always have the world's biggest badasses in my corner. I want to especially name and shame Doug Ipperciel for seemingly seeing unlimited potential in me and always holding me accountable. I'd also like to thank Jenny Radcliffe and Colin Crowden for thinking of me for jobs and for making sure I'm both excited and comfortable in any situation, and Julie Jones for being an inspiration personally and professionally. Thanks also to "The PAs" for being a steadfast safe space and cheer squad, whether we're in the same room or an ocean apart. I wouldn't be able to do any of the work that I do now without an unlikely opportunity from Nigel Parsons that led to the rest of my life, so a huge thanks to Answers Investigations. On that note, I thank Doods' Mum, Cornelia and Insa Funke, and Angie Colls for providing community, both real and imaginary, that has lasted me my whole life thus far.

Speaking of friends who I've known forever, thanks to EDC for showing small-me that it was okay to be exactly who I am, unashamedly. Thanks also to Baby Bro for being someone onto whom I could pass that lesson, and for sending it back to me whenever I need a reminder. I thank JASF, JAJ, Pyjamas, JPS, Poopin' J, Work Hubs, Pup, and my CERN Buddy for moments of joy that gave me faith in myself and the future.

Special thanks also go to: Zinks for being my Fadas, there's no better, truer way to say that. Penguin for being my tall twin through many degrees and dark times between the two of us - and for giving me

Notes On A Thesis, which reminded me that to get through the PhD I needed “the charm of a lunatic too absorbed in their studies to care what other people think”. The Raccoon Queen for being to me during the pandemic what trash is to raccoons – a goshdarned miracle. Also, SDM for our two-woman “circle of non-judgement and trust” that gives me a kick to be fearless.

Finally, to Sharpie, with admiration for your wit and much affection. Thank you for motivating me to be the best and fullest version of myself, feeding me, keeping me rested and sane, and sharing my highs and lows through these last stages of the process. I can’t wait to do the same for you.

Final words, better said by others and co-opted by me: like the great adventurer Dr. Delbert Doppler, I will strive to disprove the image of doctorates as unhelpful beyond academia (“You can't help people with a doctorate. You just sit there and you're useless!"), and I take solace in Billy Joel’s thoughts, whatever comes next: "She can't be convicted, she's earned her degree."

Table of Contents

Abstract 2
Declaration of Authorship 3
Declaration of Funding 3
Acknowledgements 4
Table of Contents 8
Table of Tables 15
Table of Figures 16
Chapter 1: Introduction 17
1.1 Background 17
1.2 Literature gap 19
1.3 Overarching research question 22
1.4 Scope 23
1.4.1 “Internet of Things” devices 23
1.4.2 National Institute of Standards and Technology (NIST) frameworks 24
1.4.3 “News” and “Media organisations” 26
1.5 Thesis aims and contributions 27
1.6 Publications arising from this thesis 29
Chapter 2: Synthesis of Relevant Literature 31
2.1 Introduction 31
2.2 What is the Internet of Things and how can it effectively be categorised? 31
2.2.1 Defining the scope of the IoT 31
2.2.2 Smart cities and scoping 34
2.2.3 Categorising the IoT and its threats 35
2.3 How are privacy and security relevant to the IoT and journalism? 38
2.3.1 Defining security and privacy for this thesis 39
2.3.2 Threats from IoT data collection 42
2.3.3 Privacy and Security by Design and Default 47
2.3.4 The relevance of surveillance studies to this thesis 49
2.4 How do states regulate the IoT? 51

2.5 What is the current state of literature on IoT threats to the free press? 53
2.5.1 Existing cyber security guidance for journalists 53
2.5.2 Literature discussing IoT protections 59
2.6 Conclusion 62
Chapter 3: Methods 63
3.1 Introduction 63
3.2 Research design 65
3.2.1 Literature reviews and syntheses 65
3.2.2 Interview guides 67
3.2.3 Questionnaires 67
3.2.3.1 Exploratory study questionnaires 67
3.2.3.2 Questionnaires for validation of framework content 68
3.2.4 Country profiles 69
3.2.4.1 Comparative case study methodology rationale 69
3.2.4.2 Case selection 70
3.3 Participants 72
3.3.1 Ethics 72
3.3.2 Participant recruitment 73
3.3.2.1 Recruitment for interviews 73
3.3.2.1.1 Exploratory study interviewee recruitment 73
3.3.2.1.2 Country profile interviewee recruitment 73
3.3.2.2 Recruitment for questionnaires 74
3.3.2.2.1 Exploratory study questionnaires recruitment 74
3.3.2.2.2 Validation study survey recruitment 74
3.3.2.3 Breakdown of Country Profiles interviewees' areas of expertise 75
3.3.2.4 Breakdown of Validation Study respondent expertise 78
3.4 Data collection 80
3.4.1 Exploratory study interview procedure 80
3.4.2 Country Profile interview procedure 81
3.4.3 Piloting the questionnaires for validation of framework content 82
3.5 Data processing 83
3.5.1 Thematic analysis of qualitative data 83

3.5.1.1 Comparative case study analysis for the Country Profiles 84
3.5.2 Conceptual models 85
3.5.2.1 Compiling the Environmental IoT Model 85
3.5.2.1.2 Presentation of the Environmental IoT Model 87
3.5.2.2 Creating and compiling threat models for the threat categorisation 88
3.5.2.2.1 Threat modelling approach 88
3.5.2.2.2 Organisation of the threat categorisation 90
3.5.3 Codebook for Country Profile interview development and analysis 91
3.5.4 Analysing validation survey results 92
3.6 Conclusion 93
Chapter 4: Exploratory Study: Investigating How Journalists Perceive and Respond to Risks from the Internet of Things 94
4.1 Introduction 94
4.2 Research Questions 95
4.3 Results 96
4.3.1 Participants 96
4.3.2 Media industry participants' responses 97
4.3.2.1 Threats to Information 98
4.3.2.2 Legal Threats 99
4.3.2.3 Physical Threats 99
4.3.2.4 Protective tools and methods that journalists use to increase their cyber security 101
4.3.2.5 Physical protection strategies for journalists 101
4.3.2.6 Allocation of responsibility for journalists' cyber security 102
4.3.3 Comparing expert recommendations with media members' risk mitigations to determine their efficacy 102
4.4 Discussion 103
4.4.1 Threats to Information 104
4.4.2 Legal Threats 104
4.4.3 Physical Threats 105
4.4.4 Allocation of responsibility for journalists' cyber security 106
4.4.5 Threat vectors 107
4.4.5.1 Privacy-related threats 108

4.4.5.2 Access Control-related threats 109
4.4.6 Who is responsible for IoT device vulnerabilities? 110
4.5 Conclusion 112
4.5.1 Relevance to this thesis 112
4.5.2 Limitations of this exploratory study 113
Chapter 5: Conceptual Models 114
5.1 Introduction 114
5.2 Conceptual model 1: IoT devices by environment 115
5.2.1 Conceptual model 1 - IoT Devices by Environment (visualisations) 116
5.2.2 Conceptual model 1 - IoT Devices by Environment (tables with description) 119
5.2.3 Discussion 125
5.2.3.1 Significant threats within each category 125
5.2.3.2 Challenging areas and limitations 127
5.2.4 Conceptual model 1 - Summary 128
5.3 Conceptual model 2 - IoT threat categorisation system 129
5.3.1 Conceptual model 2 - IoT Threat Models 130
5.3.1.1 Regulatory Gaps 132
5.3.1.1.1 Third party supply chain actors accessing data 132
5.3.1.1.2 Data manipulation as a result of consent requirements 133
5.3.1.1.3 Data harvesting from decommissioned devices 133
5.3.1.1.4 Botnet creation 133
5.3.1.2 Legal Threats 134
5.3.1.2.1 Abuse of data and privacy laws 134
5.3.1.2.2 Weaponisation of financial penalties 135
5.3.1.2.3 Warrantless bulk data purchase 135
5.3.1.3 Profiling Threats 136
5.3.1.3.1 Continuous surveillance 136
5.3.1.3.2 Abusing health and biometric information 137
5.3.1.3.3 Data linkage and aggregation 138
5.3.1.4 Tracking Threats 138
5.3.1.4.1 Informal additions to state surveillance networks 138
5.3.1.4.2 SOCMINT and IoT interrogation by law enforcement 138

5.3.1.4.3 Predictive analysis of location data to facilitate physical attacks 139
5.3.1.5 Data and device modification threats 139
5.3.1.5.1 Sensor-level attacks on data confidentiality or integrity 139
5.3.1.5.2 Altering user-facing device and data attributes 140
5.3.1.5.3 Hijacking connected social media and communications accounts 140
5.3.1.5.4 Manipulation of devices' physical activities 141
5.3.1.6 Networked devices threats 142
5.3.1.6.1 Voice stealing 142
5.3.1.6.2 Denial of Service attacks 143
5.3.2 Discussion 144
5.3.2.1 Example threat scenarios 145
5.3.2.2 Challenging areas and limitations 147
5.3.3 Conceptual model 2 - Summary 148
5.4 Conclusion 149
Chapter 6: Main IoT risks perceived by interviewees: Laws 150
6.1 Introduction 150
6.2 Theme 1: Domestic government overreach 151
6.2.1 Carve-outs in laws 153
6.2.2 Surveillance laws 154
6.2.3 Bulk data collection 160
6.3 Theme 2: Domestic government inadequacy 163
6.3.1 Insufficient journalist legal protections 163
6.3.2 Insufficient IoT regulation 165
6.3.3 Incompetent data protection 170
6.3.4 Cyber-physical criminal threats exacerbated by insufficient IoT regulation 174
6.4 Conclusion 177
Chapter 7: Additional IoT risks perceived by interviewees: Geopolitical and Organisational Considerations 179
7.1 Introduction 179
7.2 Theme 3: Geopolitical risk factors 180
7.3 Theme 4: Status of existing protections and mitigations for journalists 185
7.3.1 Risk assessments and training 185

7.3.2 Sharing threat intelligence between media organisations and journalists 190
7.4 Conclusion 193
Chapter 8: Framework 195
8.1 Introduction 195
8.2 Framework overview 195
8.2.1 Framework definitions 196
8.2.1.1 Defining “Countermeasures” (column 2) 197
8.2.1.2 Defining “Disadvantages” (column 3) 198
8.2.1.3 Defining “Function of countermeasure,” i.e. “How is it estimated that this protection will help against a given threat?" (column 5) 198
8.2.1.4 Defining “Beneficiaries of these countermeasures” (column 6) 200
8.2.1.5 Defining “Workflow phases” (column 7) 201
8.2.1.6 Defining “Role Umbrellas” (column 8) 202
8.2.1.7 Defining “Feasibility” (column 9) 203
8.3 Framework contents 204
8.3.1 Column 2: Countermeasures (and their assigned letter label in column 1) 207
8.3.2 Column 3: Disadvantages to each countermeasure 213
8.3.3 Column 4: Threats addressed by each countermeasure 214
8.3.4 Column 5: Function of countermeasure 216
8.3.5 Column 6: Beneficiary 217
8.3.6 Column 7: Phase(s) of the editorial workflow to which this countermeasure is most relevant 218
8.3.7 Column 8: Category of media roles that is most likely to be responsible for implementation of this countermeasure 218
8.3.8 Column 9: Feasibility of the countermeasure 219
8.4 Using the framework 219
8.5 Discussion 227
8.5.1 Assessment of cyber security and states capabilities experts’ validations of countermeasures 227
8.5.2 Assessment of media experts’ validations of countermeasures 228
8.5.3 Implications of countermeasures for the media sector 229
8.6 Conclusion 230
Chapter 9: Discussion and Conclusion 232

9.1 Introduction 232
9.2 Summary of chapters and synthesis of research findings 232
9.2.1 Thesis aims and findings 232
9.2.2 How the chapters came together 233
9.3 Contributions 234
9.3.1 Contributions to academic scholarship 235
9.3.2 Contributions to policy 238
9.3.3 Contributions to industry 240
9.4 Discussion: Emerging trends and outlook 242
9.5 Limitations 243
9.6 Future work 247
9.7 Conclusion 248
Appendices 250
Appendices from Chapter 4: Exploratory Study 250
Appendix A: Interview Guide 250
Appendix B: Association for International Broadcasting survey matrix 253
Appendix C: Academic experts in cyber security survey matrix 255
Appendices from Chapter 5: Conceptual Models 258
Appendix D: Old “Taxonomy” of IoT threat models 258
Appendices from Chapters 6 and 7: Country Profiles 273
Appendix E: Participant Information Sheet and Oral Consent Form 273
Appendix F: List of questions asked for Country Profile interviews 280
Appendices from Chapter 8: Framework 286
Appendix G: Validator Invitations 286
Appendix H: Validation study media expert survey 288
Appendix I: Validation study cyber security expert survey - Feasibility and Function 295
Appendix J: Validation study cyber security expert survey - Matching threats to countermeasures & countermeasures to disadvantages 305
Appendix K: Validations study state capabilities’ expert survey 316
Appendix L: Framework (static version) 327
Bibliography 348

Table of Tables

Table 1: Job categories for Country Profile interviewees 75
Table 2: Expertise categories for Country Profile interviewees 76
Table 3: Country Profile interviewees' subject matter expertise and years of experience 78
Table 4: Cyber security (threats-countermeasures matching) survey respondents' expertise 79
Table 5: Cyber security (function and feasibility) survey respondents' expertise 79
Table 6: Media survey respondents' expertise 79
Table 7: States' capabilities survey respondents' expertise 80
Table 8: Codebook for Country Profile interview development and analysis 92
Table 9: Details of Interviewees 96
Table 10: Details of AIB Survey Respondents. Respondents to the AIB survey were all journalists. 97
Table 11: Actors identified by study participants as being responsible for IoT vulnerabilities 111
Table 12: Private homes category 121
Table 13: Public spaces category 123
Table 14: Workplace category 124
Table 15: Wearable category 125
Table 16: Demonstration of the first two rows of the framework 206
Table 17: Conversion of old countermeasures to new countermeasures 213
Table 18: Conversion of old threats to the new threats categorisation 216
Table 19: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), and 3 (disadvantages of countermeasure) 330
Table 20: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), and 4 (threats addressed by each countermeasure) 336
Table 21: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), 5 (function of countermeasure), and 6 (beneficiaries of countermeasure) 339
Table 22: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), 7 (editorial workflow phases to which countermeasure is most relevant), and 8 (media roles most likely to be responsible for implementation of countermeasure) 344
Table 23: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), and 9 (feasibility of implementation of the countermeasure) 347

Table of Figures

Figure 1: Visual overview of chapters 64
Figure 2: Technology used by media industry respondents 98
Figure 3: IoT devices organised by environment 117
Figure 4: Private homes category 118
Figure 5: Public spaces category 118
Figure 6: Workplace category 119
Figure 7: Editorial workflow diagram, co-created with the AIB 202
Figure 8: Demonstration of multiple options within the same cell 220
Figure 9: Demonstration of filtering process 221
Figure 10: Demonstration of filtering by a specific threat 223
Figure 11: Demonstration of simultaneous filtering using two columns 224
Figure 12: Demonstration of simultaneous filtering using three columns 224
Figure 13: Demonstration of filtering by a specific workflow phase 225
Figure 14: Demonstration of filtering by a specific function 225
Figure 15: Demonstration of filtering by a specific beneficiary 226
Figure 16: Demonstration of filtering by threat and reviewing countermeasure disadvantages 226
Figure 17: Demonstration of filtering by role umbrella to highlight tasks for corporate actors 227
Figure 18: Stealing information from journalists 258
Figure 19: Tracking journalists and sources 262
Figure 20: Altering information 264
Figure 21: Assuming control over intended device functionality to discredit or physically harm journalists 266
Figure 22: Limiting device functionality 269
Figure 23: Screenshot to show survey question about feasibility 292
Figure 24: Screenshot to show survey question about function 299
Figure 25: Screenshot of survey question matching threats to countermeasures 308
Figure 26: Screenshot of survey question assigning disadvantages to countermeasures 309
Figure 27: Screenshot of survey question assigning current realism score to threats 320
Figure 28: Screenshot of survey question assigning future realism score to threats 322

Chapter 1: Introduction

1.1 Background

Public access to factual information about powerful people and organisations is key to an educated electorate that can regulate the state.[1] As such, the existence and maintenance of a free press can be used as a barometer for the state of a democratic society. Attempts to curtail or attack transparent, accessible, and free journalism can thus be seen as threats to a branch of the critical national infrastructure of a democracy, and to the democratic state itself. This has potential implications for individual human rights, and international relations and security.[2]

In cases of attempted attacks, whether related to physical, cyber, or cyber-physical security, there is often an asymmetry between the resources, skills and imagination of adversaries and defenders. This asymmetry is evident in the media industry, with respect to the targeting of journalists and news organisations. For example, in 2019, 59% more journalists were killed in countries at peace than in war-zones, with 63% of deaths attributed to deliberate targeting.[3] Further, a record number of journalists were detained in 2022, with 194 convicted and 339 not yet tried.[4] Around the world, news organisations and journalists are increasingly under threat of surveillance, censorship and intimidation from a variety of vectors and highly capable actors,[5] including democratic and authoritarian governments.[6] This has been highlighted by Google's Threat Analysis Group, which noted that state-affiliated cyber attackers are increasingly targeting journalists.[7] Reporters without Borders released a list of actors who are responsible

[1] Strömbäck J (2005) In Search of a Standard: four models of democracy and their normative implications for journalism. Journalism Studies 6(3): 331–345. DOI: 10.1080/14616700500131950; Sulzberger AG (23 September 2019) "Opinion | The Growing Threat to Journalism Around the World", New York Times. Available at: https://www.nytimes.com/2019/09/23/opinion/press-freedom-arthur-sulzberger.html [Accessed 25 September 2019]; Pickard V (2020) Restructuring Democratic Infrastructures: A Policy Approach to the Journalism Crisis. *Digital Journalism* 8(6). Routledge: 704–719. DOI: 10.1080/21670811.2020.1733433; Bühlmann M, Merkel W, Müller L, et al. (2012) The Democracy Barometer: A New Instrument to Measure the Quality of Democracy and its Potential for Comparative Research. *European Political Science* 11(4): 519–536. DOI: 10.1057/eps.2011.46; Stotzky IP (2001) The Role of a Free Press and Freedom of Expression in Developing Democracies. University of Miami Law Review 56: 255; Coleman WTJ (1984) Free Press: The Need to Ensure an Unfettered Check on Democratic Government between Elections. *Tulane Law Review* 59: 243; Voorhoof D and Cannie H (2010) Freedom of Expression and Information in a Democratic Society. *International Communication Gazette* 72(4–5). SAGE Publications Ltd: 407–423. DOI: 10.1177/1748048510362711; Reporters without borders (2018) *Worldwide round-up of journalists killed, detained, held hostage, or missing in 2018.* 1 December. Available at: https://rsf.org/sites/default/files/worldwilde_round-up.pdf (accessed 9 September 2019).

[2] Privacy International (2016) Why the Internet of Things Begs for a Paradigm Shift in Internet Security. Available at: http://www.privacyinternational.org/blog/862/why-internet-things-begs-paradigm-shift-internet-security (accessed 9 September 2019).

[3] Reporters without borders (2019) *Worldwide round-up of journalists killed, detained, held hostage, or missing in 2019*. 1 December. Reporters without borders. Available at: https://rsf.org/sites/default/files/rsf_2019_en.pdf (accessed 20 December 2019).

[4] Reporters Without Borders (RSF) (2022) *2022 Round-Up: Journalists detained, killed, held hostage and missing*. 1 December. Paris, France: Reporters Without borders. Available at: https://rsf.org/sites/default/files/medias/file/2022/12/RSF_Bilan2022_EN.pdf (accessed 14 December 2022).

[5] Council of Europe (2019) The 2019 Annual Report by the partner organisations of the Council of Europe's Platform for the Protection of Journalism and Safety of Journalists: 'Democracy at Risk: threats and attacks against media freedom in Europe'. Annual Report by the partner organisations of the Council of Europe's Platform for the Protection of Journalism and Safety of Journalists, February. France: Council of Europe: 12. Available at: https://rm.coe.int/annual-report-2018-democracy-in-danger-threats-and-attacks-media-freed/1680926453 (accessed 11 January 2020).

[6] Datta A (17/02/2020) Governments of the world just ramped up spying on reporters. Available at: https://www.cjr.org/first_person/ft-nations-surveillance-attacks.php (accessed 18 February 2020).

[7] Zorz Z. Government-backed cyber attackers increasingly targeting journalists [Internet]. Help Net Security. 2020 [cited 2020 Sep 11]. Available from: https://www.helpnetsecurity.com/2020/03/27/cyber-attackers-targeting-journalists/

for harassment, censorship or surveillance of journalists in 2020, as well as spreading disinformation.[8] This included government-backed groups from five different continents as well as non-state actors. Motivated by the imperative to address this asymmetry between state and well-resourced non-state threat actors, and media industry defenders, this thesis emphasises the importance for the media to develop their own identification and protection techniques based on relevant vulnerabilities.

Journalists and the media are under increased attack across various domains, both from long-standing threats like imprisonment and execution, as well as from cyber-threats enabled by newer technologies.[9] Over the last decade, whistleblowers released documentation of intelligence agencies' investigations into journalists deemed threats to national security in many countries, from the United Kingdom to Ukraine.[10] The Edward Snowden disclosures on this topic revealed that hacking of journalists' phones and computers, to compromise source confidentiality and future scoops is widespread.[11] Snowden-era hacking has given rise to another high-profile form of smartphone infiltration: spyware. One such example is the NSO Group's Pegasus software, which has already been purchased by government officials across at least twenty countries and used against at least 180 journalists.[12] This spyware makes phone-hacking easier and more streamlined, exfiltrates all data held on the device, infects associated devices and contacts, and activates the phone's recording features for surveillance.

[8] Reporters Without Borders. RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders [Internet]. RSF. 2020 [cited 2020 Sep 11]. Available from: https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators

[9] The Economist: Daily Chart (2021) A record number of journalists are in prison. *The Economist*, 14 December. Available at: https://www.economist.com/graphic-detail/2021/12/14/a-record-number-of-journalists-are-in-prison (accessed 12 April 2022).

[10] Ball J (2015) GCHQ captured emails of journalists from top international media. The Guardian, 19 January. Available at: https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post (accessed 9 September 2019); European Centre for Press & Media Freedom (2017) Ukraine: Authorities block journalists as threats to national security. In: Mapping Media Freedom. Available at: https://mappingmediafreedom.org/index.php/2017/09/13/ukraine-journalists-threat-national-security/ (accessed 9 September 2019); Lashmar P (2020) *Spies, Spin and the Fourth Estate: British Intelligence and the Media*. Edinburgh, Scotland: Edinburgh University Press.

[11] Lashmar P (2017) No More Sources? Journalism Practice 11(6). Routledge: 665–688. DOI: 10.1080/17512786.2016.1179587; Wahl-Jorgensen K, Hintz A, Dencik L, et al. (2017) Introduction: Journalism, citizenship and surveillance. Digital Journalism 5(3). Routledge: 256–261. DOI: 10.1080/21670811.2016.1266134.

[12] Kenyon M (2019) Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes. The Citizen Lab, 1 April. Available at: https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/ (accessed 9 September 2019); Rueckert P (2021) Pegasus: The new global weapon for silencing journalists. Forbidden Stories, 18 July. Available at: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ (accessed 12 April 2022); Woodhams S (2021) Spyware: An Unregulated and Escalating Threat to Independent Media. Center for International Media Assistance, 25 August. Available at: https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/ (accessed 12 April 2022); Marczak B, Scott-Railton J, Senft A, et al. (2018) The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. Citizen Lab Research Report No. 115, 1 October. The Citizen Lab: University of Toronto. Available at: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/ (accessed 12 April 2022); Pegg D, Lewis P, Safi M, et al. (2021) FT editor among 180 journalists identified by clients of spyware firm. The Guardian, 20 July. Available at: https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware (accessed 12 April 2022); Scott-Railton J, Marczak B, Razzak BA, et al. (2017) Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware. Citizen Lab Research Report No. 93, 19 June. The Citizen Lab: University of Toronto. Available at: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (accessed 12 April 2022).

In 2021, Reporters Without Borders noted that independent journalism was stymied in 132 of 180 countries,[13] and the 2021 Nobel Peace Prize to members of the press for the first time.[14] The prevalence of Pegasus and other similar spyware used against journalists both in democracies as well as authoritarian countries, is evidence of a trend in which press freedom is progressively curtailed globally.[15] To counter this, organisations such as Reporters Without Borders and UNESCO have released guidelines instructing journalists on how to maximise their cyber security in high-risk environments.[16] While such guidance recognises the problem of smartphone-targeting spyware, it neglects another class of under-regulated emerging technology that is far more prevalent: the consumer Internet of Things (IoT).

The IoT is a vast, interconnected network of devices, present in both the public and private spheres.[17] IoT devices are connected to at least one other device, some are connected to the Internet, so they can all be controlled or influenced remotely.[18] They are often designed to replace older instruments with fewer functionalities (such as fridges and doorbells), and have many spyware functions. These newer devices deviate from older technologies in two significant ways: First, because some IoT devices add the ability to activate an object's function remotely or to access the Internet (e.g. smart kettles and smart vehicles), the IoT can facilitate physical threats. Second, IoT devices and much of the data they collect can be legitimately accessed, enabling legal threats to journalists and sources.[19]

1.2 Literature gap

There is guidance advising journalists on traditional cyber and physical security practices.[20] However, there is a gap in how accurately the press understand how to mitigate risks associated with IoT devices (see: Chapters 2 and 4).

News organisations have long had to consider how best to protect their staff, their sources, and their scoops from emerging and evolving threats, including spy craft that risks source confidentiality. There have been studies that have assessed how best to protect journalists from conventional cyber-threats to

[13] Reporters Without Borders (2021) 2021 World Press Freedom Index: Journalism, the vaccine against disinformation, blocked in more than 130 countries. Available at: https://rsf.org/en/2021-world-press-freedom-index-journalism-vaccine-against-disinformation-blocked-more-130-countries (accessed 12 April 2022).

[14] The Nobel Prize (2021) The Nobel Peace Prize 2021. Available at: https://www.nobelprize.org/prizes/peace/2021/press-release/ (accessed 12 April 2022).

[15] Deibert RJ (2020) *Reset: Reclaiming the Internet for Civil Society*. 1st ed. United Kingdom: September Publishing.

[16] UNESCO and Reporters without borders (2015) SAFETY GUIDE FOR JOURNALISTS: A handbook for reporters in high-risk environments. Reporters without borders. Available at: https://rsf.org/sites/default/files/guide_journaliste_rsf_2015_en_0.pdf (accessed 9 September 2019).

[17] Shere ARK, Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.

[18] Nurse J, Erola A, Agrafiotis I, et al. (2015) Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things. In: Proceedings of the 2015 International Workshop on Secure Internet Of Things (SIoT), Vienna, Austria, 21 September 2015. DOI: 10.1109/SIOT.2015.10.

[19] Lashmar P (2020) *Spies, Spin and the Fourth Estate: British Intelligence and the Media*. Edinburgh, Scotland: Edinburgh University Press.

[20] Electronic Frontier Foundation (2019) Surveillance Self-Defense: Tips, Tools and How-Tos for Safer Online Communications. Available at: https://ssd.eff.org/en (accessed 9 September 2019); Posetti J (2017) Protecting Journalism Sources in the Digital Age. UNESCO SERIES ON INTERNET FREEDOM. UNESCO. Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/protecting_journalism_sources_in_digital_age.pdf; Digital Defenders Partnership (2019) The Digital First Aid Kit – Introduction. In: Digital Defenders Partnership: Hivos International. Available at: https://www.digitaldefenders.org/digitalfirstaid/ (accessed 9 September 2019); GJS (2019) Digital Safety Curriculum for Newsrooms. Available at: https://www.gjs-security.com/digital-safety-curriculum-for-newsrooms/ (accessed 9 September 2019).

phones, laptops and communications channels, such as "Investigating the Computer Security Practices and Needs of Journalists,"[21] and "Individual versus Organizational Computer Security and Privacy Concerns in Journalism."[22] Regarding novel devices, the 2017 Canadian Journalists For Free Expression study report assessing the digital security of journalists in distress did not reference the IoT, except for one sentence in its conclusion. Furthermore, the report determined that journalists who are in distress often disregard digital risks, often due to lack of knowledge.[23]

In fact, McGregor and Watkins found that many journalists relied on an incomplete mental model of information security. These journalists assumed that they should take more security measures than a private citizen only if their stories were sensitive to governments.[24] Similarly, Henrichsen recognised the growing role of information security trainers in newsrooms, but noted that the 24-hour news cycle creates pressure for journalists to rely on methods that provide insufficient protection against new technological threats.[25] Watkins argued that one reason for a lack of updated procedures was the off-putting complexity of cyber security procedures and explanations, resulting in ad-hoc and inconsistent security and privacy strategies.[26] McGregor *et al.* examined one of the most secure recent large-scale journalistic efforts, the Panama Papers, but still did not consider threats from or protections against the IoT, signalling that awareness of this issue is low.[27] Further, a 2015 study by Milosavljević *et al.* demonstrated institutional inaction within the Slovenian media industry, in spite of journalists' self-reported awareness of "the issues related to potential surveillance and new technologies." [28] The lack of reference to the IoT in these findings underscores the need for clear guidelines on threats enabled by the IoT and how they may be minimised.

Additionally, reports such as UNESCO's 2015 "Survey of Selected Issues" about journalists' digital security did not mention the IoT but did note three challenges, all of which are exacerbated by the IoT: First, the increasing prevalence and decreasing cost of technologies that enable surveillance, data retention and cyber-attacks. Second, the use of location tracking technologies to identify the press and their sources. Third, accounts and devices being illegitimately accessed to compromise journalists' networks.[29]

---

[21] McGregor SE, Charters P, Holliday T, et al. (2015) Investigating the Computer Security Practices and Needs of Journalists. In: Proceedings of the 24th USENIX Security Symposium, Washington, D.C., 12 August 2015, p. 17. USENIX Association.

[22] McGregor S, Roesner F and Caine K (2016) Individual versus Organizational Computer Security and Privacy Concerns in Journalism. In: Proceedings on Privacy Enhancing Technologies 2016. DOI: 10.1515/popets-2016-0048.

[23] Blanchard T (2017) Journalists in Distress: Assessing the Digital Viability of a Global Emergency Assistance Network. The Digital Security of Journalists in Distress: Report 3. Toronto, Canada: Canadian Journalists For Free Expression: 26 Available at: https://d3n8a8pro7vhmx.cloudfront.net/cjfe/pages/2913/attachments/original/1484964569/Report_3_-_The_Digital_Security_of_Journalists_in_Distress.pdf?1484964569 (accessed 11 January 2020).

[24] McGregor SE and Watkins EA (2016) "Security by Obscurity": Journalists' Mental Models of Information Security. *#ISOJ* 6(1). The Multimedia Edition of the Official Research Journal of the International Symposium on Online Journalism. Available at: https://isojjournal.wordpress.com/2016/04/14/security-by-obscurity-journalists-mental-models-of-information-security/ (accessed 15 February 2020).

[25] Henrichsen JR (2019) Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. *Digital Journalism* 0(0): 1–19. DOI: 10.1080/21670811.2019.1653207.

[26] Watkins EA (2017) *Workers' Sensemaking for Information Security: A Research Agenda for the Future of Work*. ACM. Available at: https://drive.google.com/file/d/1llLwRsXCSqnPxuRueHk2M1cYD2x4U1BZ/edit?usp=embed_facebook (accessed 9 September 2019).

[27] McGregor SE, Watkins EA, Al-Ameen MN, et al. (2017) When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. In: *Proceedings of the 26th USENIX Security Symposium*, Vancouver, BC, Canada, 16 August 2017, p. 19. USENIX Association. Available at: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-mcgregor.pdf.

[28] Milosavljević M, Amon Prodnik J and Kučić LJ (2015) Securing the Communication of Journalists with their Sources as a Form of Source Protection – Editorial Policy of Slovenian Media Regarding Communication and Technology. *Teorija in praksa* 52(4): 612–630.

[29] Henrichsen J, Betz M and Lisosky JM (2015) Building Digital Safety for Journalism: A Survey of Selected Issues. UNESCO Series on Internet Freedom. Paris: UNESCO:17-18 Available at: https://unesdoc.unesco.org/ark:/48223/pf0000232358.

Compromised accounts have already been used to disseminate disinformation and attribute it to legitimate press organisations.[30] This threat is amplified by the vast number of IoT devices that allow consumers to access their online accounts, highlighting the need for this research. These points reflect that the ubiquity of the IoT signals an escalation both in scale and intensity of threats to the free press.

Even institutions that should be at the forefront of cyber security, such as the United States military, have demonstrated a lack of awareness of the vulnerabilities inherent in these recent technologies. For example in 2017, when the locations and layout of their secret bases were unintentionally revealed due to open-source user data released by the Strava fitness app.[31] This is a relatively new realm, where security threats have multifaceted vectors and consequences (i.e. legal, physical, and cyber threats). It is difficult for individual users to predict and patch vulnerabilities and outpace offensive capabilities, especially as the design and implementation of such technologies vary drastically. In the Strava example above, as information leakage is an intentional design feature of the app's functionality, privacy threats are not necessarily breaches.[32] These problems are thus exacerbated for users because of the structure of the technology industry, in which data is a commodity.[33]

As is explored in-depth in Chapter 5 of this thesis, the rise in connected data collection technologies considerably expands the level of risk exposure of highly targeted groups. It does so because any apparently innocuous IoT device can function as a bridge into a seemingly secure network or private environment. The IoT can be used to pinpoint where journalists meet sources, to record and transmit their conversations, or even to delete their work, without the need for a massive, coordinated attack. These issues represent a novel kind of oppressive threat to individuals, organisations and information that is not easily comparable to those posed through traditional technological devices.[34] Additionally, it is not enough to assess defensive capabilities and methods solely against contemporary threats, but defenders must also anticipate future threats.[35] The 2018 European Union Agency For Network and Information Security (ENISA) Threat Landscape Report found increasing attacks by state-sponsored actors on Industrial Internet of Things systems that are part of critical infrastructure, particularly for espionage.[36]

---

[30] Greenberg A (2020) Hackers Broke Into Real News Sites to Plant Fake Stories. *Wired*, 29 July. Available at: https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/ (accessed 19 October 2020).

[31] @DFRLab (2018) Data and Defense: The Case of Strava. Available at: https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2 (accessed 9 August 2019).

[32] Meteriz Ü, Fazıl Yıldıran N, Kim J, et al. (2020) Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In: *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, November 2020, pp. 464–473. DOI: 10.1109/ICDCS47774.2020.00063; Hassan WU, Hussain S and Bates A (2018) Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide? In: *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 497–512. Available at: https://www.usenix.org/conference/usenixsecurity18/presentation/hassan (accessed 19 April 2022).

[33] Käll J (2020) The Materiality of Data as Property. *Harvard International Law Journal* 61: 1–11; Sadowski J (2019) When data is capital: Datafication, accumulation, and extraction. *Big Data & Society* 6(1). SAGE Publications Ltd: 2053951718820549. DOI: 10.1177/2053951718820549.

[34] He H, Maple C, Watson T, et al. (2016) The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing other computational intelligence. In: 2016 IEEE Congress on Evolutionary Computation (CEC), Vancouver, BC, July 2016, pp. 1015–1021. IEEE. DOI: 10.1109/CEC.2016.7743900; Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2017. p. 1; Perera C, Ranjan R, Wang L, et al. (2015) Big Data Privacy in the Internet of Things Era. IT Professional 17(3): 32–39. DOI: 10.1109/MITP.2015.34.

[35] Nurse JRC, Creese S and De Roure D (2017) Security Risk Assessment in Internet of Things Systems. IT Professional 19(5): 20–26. DOI: 10.1109/MITP.2017.3680959.

[36] European Union Agency For Network and Information Security (ENISA) (2019) ENISA Threat Landscape Report 2018. Report/Study, 28 January. Athens, Greece: European Union Agency For Network and Information Security (ENISA). Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed 15 January 2020).

It is therefore crucial to shift away from thinking about IoT threats to the press as "Black Swans,"[37] i.e. outliers or highly improbable events. Instead, IoT threats should be reframed as foreseeable threats with a high likelihood of occurring against specific, high-value targets. In lay terms, this message can be conveyed via The Ugly Duckling fable, in which the titular character was misjudged to be an unappealing and uncommon outlier, when it was in fact representative of the natural progression of swans as they grow. The tale ends with the Ugly Duckling becoming an adult swan, and joining a flock of similar birds – perhaps conceptually having the same level of impact and severity as a Black Swan event. Similarly, the perception of IoT risk to the media as rare is wrong; rather it is unanticipated because it is mischaracterised due to the lack of visible precedent from our current perspective, while likely being much more common.

Threat modelling in computer science often emphasises threats with the potential for the widest impact with regard to direct targets. However, there is not yet academic research into journalists' understanding of these personal and professional threats to them via novel IoT devices. This is likely because the IoT is a relatively new phenomenon, which contributes to popular perceptions of the IoT as low-risk, as security is not often an emphasised attribute.[38] For this reason, Chapter 4's discussion of the exploratory study focuses on the questions of whether journalists perceive threats from the IoT, how they combat these threats, and what protection mechanisms are and will be effective according to surveyed cyber security experts.

The available evidence to date underscores the vital need for clear, accessible guidelines addressing how to mitigate potential IoT threats. These new threats not only have direct cyber and physical consequences, they also result in an increase in the amount of data collection and retention that can be used to legally access journalistic information. These issues represent a novel oppressive threat to members of the news industry that is not easily comparable to other known threats. Already, there are IoT exploitation services for hire that demonstrate the close link between governments and commercial entities. One such example is the cyberoffense firm Toka, which was co-founded by a former Israeli premier and a former Israel Defense Forces cyber chief. [39] Toka has developed technology that enables both surveillance as well as has the ability to alter hijacked video feeds from IoT devices such as cameras and car security systems. These examples illustrate why legislation, although useful in a broad sense, cannot comprehensively protect against exploitation when attackers are targeting specific individuals, rather than indiscriminately searching for insecure devices to exploit. Furthermore, some states have legislative frameworks that are actually hostile to the press. The work presented in this thesis will detail the ways in which laws and policies might impact press freedom by exploiting the data available through the IoT.

1.3 Overarching research question

In response to this literature gap (see above section), the research question that underpins this DPhil is:

How can members of the press in democratic countries improve their identification of, protection from, and resilience against threats from the Internet of Things?

[37] Orlik A and Veldkamp L (2014) Understanding Uncertainty Shocks and the Role of Black Swans. Working Paper Series 20445, Working Paper. National Bureau of Economic Research. DOI: 10.3386/w20445.

[38] Williams M, Nurse JRC and Creese S (2019) Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. Computers in Human Behavior 99: 38–54. DOI: 10.1016/j.chb.2019.04.026.

[39] Benjakob O (2022) This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure - National Security & Cyber - Haaretz.com. Haaretz, 26 December. Available at: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000 (accessed 12 January 2023).

This thesis explores this question in part by profiling four case study democracies (see: Chapters 6 and 7). Per section 3.2.4 of Chapter 3, these countries were chosen to provide a cross-section of states with relevant similarities (e.g. historic cultural emphasis on press freedom) and differences (e.g. located on distinct continents). However, this research cannot and does not claim to be generalisable to all countries, democratic or otherwise. Rather, it is intended to analyse and give insights on the shared context of the four chosen countries, amplifying readers' understanding of their commonalities, including the way in which their democratic environments influence the ways in which the press are affected by IoT threats.

1.4 Scope

This section defines key terms used in this thesis and clarifies the overarching research question – with reference to an existing cyber security framework. More information on the selection process for the country profiles is presented in Chapter 3.

1.4.1 "Internet of Things" devices

Like Blythe and Johnson,[40] this thesis uses the term "IoT device" to refer to any piece of consumer technology that can connect wirelessly to the internet or to other devices. Consistent with recent research,[41] this thesis specifically focuses on new technologies, rather than on "legacy" or "traditional" technologies such as routers, phones, laptops, tablets, and desktop computers. Newer consumer IoT devices are the central focus of this thesis because of their novelty and relative lack of security when compared to smartphones and traditional computers. This distinction is acknowledged but not effectively addressed by recent Code of Practice attempts[42] and legislative proposals.[43] Also, as Blythe and Johnson noted, legacy devices are "high-capacity devices that have been on the market for a long time, have well developed operating systems and user interfaces, and the threats to these devices have been known for some time."[44] In contrast, IoT threats are barely present in literature aimed at protecting journalists from cyber security threats (see: Chapter 2). This is despite a 2021 experiment to assess the likelihood of hacking attempts targeting a smart home, which surpassed 12,000 cyber-attacks in one week.[45] This considered, while smartphones and other traditional devices are in an overlapping category with the IoT, they are not the main focus of the work as this thesis specifically examines the novelty that comes from the IoT (see: Chapter 2, section 2.2 for more detail).

[40] Blythe JM and Johnson SD (2019) A systematic review of crime facilitated by the consumer Internet of Things. Security Journal. DOI: 10.1057/s41284-019-00211-8.

[41] Mitchell P, Rowley L, Sherman J, et al. (2022) Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem. 26 September. Washington, D.C.: The Atlantic Council's Cyber Statecraft Initiative, under the Digital Forensic Research Lab (DFRLab). Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/ (accessed 24 October 2022), figure 4.

[42] Department for Digital, Culture, Media & Sport (2018) Code of Practice for Consumer IoT Security. 14 October. London, UK: Department for Digital, Culture, Media & Sport. Available at: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security (accessed 31 December 2020).

[43] NCC Group (2021) UK government announces plans for new IoT security law. In: NCC Newsroom. Available at: https://newsroom.nccgroup.com/news/uk-government-announces-plans-for-new-iot-security-law-425797 (accessed 23 April 2021).

[44] Blythe JM and Johnson SD (2019) A systematic review of crime facilitated by the consumer Internet of Things. Security Journal. DOI: 10.1057/s41284-019-00211-8.

[45] Mitchell P, Rowley L, Sherman J, et al. (2022) Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem. 26 September. Washington, D.C.: The Atlantic Council's Cyber Statecraft Initiative, under the Digital Forensic Research Lab (DFRLab). Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/ (accessed 24 October 2022), figure 4; Laughlin A (2021) How a smart home could be at risk from hackers - Which? News. Which?, 2 July. Available at: https://www.which.co.uk/news/article/how-the-smart-home-could-be-at-risk-from-hackers-akeR18s9eBHU (accessed 4 December 2022).

Another key reason for this focus is the size and rapid expansion of IoT devices in the profiled countries. The IoT market is expanding exponentially, with global device numbers predicted to reach over 29 billion IoT devices in 2030, up from roughly 9.7 billion in 2020. Of these, 60% are consumer items.[46] A 2015 McKinsey report anticipated that by 2025 the IoT market would represent over 10% of the global economy, with "an economic impact of between $3.9 and $11.1 trillion (US)."[47] As it is anticipated that "market forces and misaligned incentives will contribute to the proliferation of cheap [IoT] devices with minimal privacy protection,"[48] it stands to reason that many of these devices are present in the homes, offices and on the bodies of journalists themselves.

Crime facilitated by the IoT has the potential to take different forms, increasing risk from solely to information, to physical.[49] Myriad new threat vectors and an ever-more-expansive attack surface are particularly concerning for journalists, as only 9% of the world's population resides in a country considered by Reporters Without Borders to have "satisfactory" or "good" press freedom.[50] The 2019 Democracy Report by the V-Dem Institute at the University of Gothenburg mentioned that "Western Europe, North America, […] Australia, […] and Taiwan continue to be the strongest holds for democracy in the world,"[51] but that some of them (two of the thesis' country profiles: Taiwan and the US) are the most affected by foreign disinformation campaigns in the world.[52] This results in media fractionalisation, eroding the potency of their free press and challenging their democratic systems.

1.4.2 National Institute of Standards and Technology (NIST) frameworks

The phrasing in the thesis' overarching research question – "identification of, protection from, and resilience against" – is a reference to the US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, hereafter referred to as the NIST CSF.[53] The NIST CSF includes a "Core" comprising five "Functions": "Identify, Protect, Detect, Respond, Recover," four of which are explored through this thesis. NIST CSF was chosen because it is intended to be flexible enough to be applicable to all organisations, but particularly for those that form part of critical

[46] Vailshery LS (2022) Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (in billions). 22 November. Statista. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed 3 December 2022).

[47] Kamalipour YR (ed.) (2019) *Global Communication: A Multicultural Perspective*. 3rd edition. Rowman & Littlefield Publishers: xi.

[48] Nurse JRC, Williams M and Creese S (2016) The Perfect Storm: The Privacy Paradox and the Internet-of-Things. In: *11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, 31 September 2016. IEEE. DOI: 10.1109/ARES.2016.25.

[49] Blythe JM and Johnson SD (2019) A systematic review of crime facilitated by the consumer Internet of Things. Security Journal. DOI: 10.1057/s41284-019-00211-8.

[50] Reporters without borders (2019) Only nine percent of humankind lives in a country where press freedom is good. Available at: https://rsf.org/en/news/only-nine-percent-humankind-lives-country-where-press-freedom-good (accessed 9 September 2019).

[51] Varieties of Democracy (V-Dem) (2019) *V-DEM ANNUAL DEMOCRACY REPORT 2019: Democracy Facing Global Challenges*. V-DEM ANNUAL DEMOCRACY REPORT. V-Dem Institute at the University of Gothenburg, Sweden: Varieties of Democracy (V-Dem) Institute at the University of Gothenburg: 10 Available at: https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf (accessed 11 January 2020).

[52] Varieties of Democracy (V-Dem) (2019) *V-DEM ANNUAL DEMOCRACY REPORT 2019: Democracy Facing Global Challenges*. V-DEM ANNUAL DEMOCRACY REPORT. V-Dem Institute at the University of Gothenburg, Sweden: Varieties of Democracy (V-Dem) Institute at the University of Gothenburg: 5 Available at: https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf (accessed 11 January 2020).

[53] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018, 16 April. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.04162018.

infrastructure. It is widely lauded as introducing simple, non-country-specific standards for organisational cyber security, regardless of the business of the organisations in question.[54]

Although January 2020 saw the release of the new NIST Privacy Framework,[55] which is applicable to organisations affected by IoT data-collecting capabilities, the pre-existing NIST CSF is the basis of this thesis research. This decision was taken primarily because both NIST Frameworks cover privacy, but the NIST CSF is broad enough to recognise and include reference to potential cyber-physical risks stemming from systems like the IoT. Additionally, the current iteration of the NIST Privacy Framework appears to be aimed at organisations who create and proliferate technologies, rather than those who solely interact with them. This suggests a distinction between the privacy of individuals and the safety of organisations. This DPhil however addresses both. Finally, the NIST CSF recognises the importance of the free press as a particular audience under threat. This is seen through its acknowledgement: "Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities."[56]

Other frameworks that were considered include NIST SP 800-53 and ISO 27002. NIST SP 800-53 is a database of 272 recommended security controls for federal information systems and organisations,[57] with much more detailed and comprehensive procedures than the NIST CSF. It is possible to map NIST SP 800-53 requirements into a NIST CSF strategy, as the former is an example of a "Control framework" and the latter an example of a "Program framework," i.e. the NIST CSF's functions include "Build[ing] a comprehensive security program [and] simplify[ing] communications with business leaders."[58] In future work, Chapter 8's framework, which interprets the more strategic NIST CSF, could be supplemented using the similarly outcomes-based NIST SP 800-53, which was finalised in 2020.[59]

Additionally, the ISO/IEC 27000 series, including ISO/IEC 27002 are an advisory standard that comprises a code of practice for information security controls, established in 2013.[60] It has greater similarities to a "Program Framework" like the NIST CSF, but is older and focuses primarily on information security, rather than on the combination of cyber-physical and data security threats that are presented by IoT capabilities. ISO/IEC 27002 is an international standard, while those designed by NIST are intended to be specific to US federal agencies. However, ISO/IEC 27002 is designed for validation through independent auditing and certification, whereas the NIST CSF is reliant on organisations self-certifying. On balance, the NIST CSF

[54] Vigliarolo B (2017) NIST Cybersecurity Framework: A cheat sheet for professionals. Available at: https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/ (accessed 23 January 2020).
[55] National Institute of Standards and Technology (2020) *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. 16 January. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf (accessed 28 January 2020).
[56] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018, 16 April. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.04162018.
[57] Computer Security Division ITL (2020) NIST Releases FPD SP 800-53 Rev. 5 | CSRC. Available at: https://csrc.nist.gov/News/2020/nist-releases-fpd-sp-800-53-rev-5 (accessed 22 March 2020).
[58] DeNisco Rayome A (2019) How to choose the right cybersecurity framework. Available at: https://www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ (accessed 23 March 2020).
[59] Computer Security Division ITL (2020) NIST Releases FPD SP 800-53 Rev. 5 | CSRC. Available at: https://csrc.nist.gov/News/2020/nist-releases-fpd-sp-800-53-rev-5 (accessed 22 March 2020).
[60] International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) (2013) ISO/IEC 27002:2013. Available at: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54533.html (accessed 22 March 2020).

therefore seems to be designed to maximise its accessibility to the organisations implementing it and is therefore the most appropriate basis for this research.

1.4.3 "News" and "Media organisations"

Definitions of "news" are mainly derived from the idea of news as synonymous with the communication of "facts."[61] However, this thesis subscribes to the description offered by Harcup and O'Neill, who identified 15 "contemporary news values" that, along with "practical considerations" and "unconscious influences" such as those relating to bias and balance, usually determine the selection of potential news stories. Moving beyond a reductive perception of news as simply reporting facts, and recognising that it requires analysis and the careful presentation of facts, Harcup and O'Neill wrote that "news values […] inform the mediated world that is presented to news audiences, providing a shared shorthand operational understanding of what working journalists are required to produce to deadlines."[62] This more nuanced understanding of "news" is crucial to this dissertation's focus on both the journalistic work product, and the processes by which they conduct this work. In particular, the news value of "stories concerning powerful individuals, organisations, institutions or corporations" speaks to both a reason for the high-targeting of journalists by well-resourced threat actors, and the imperative of protecting the media's ability to continue in this role.

Additionally, this thesis refers to "media organisations" and "news organisations" interchangeably, with only slight clarification of the definition outlined by McNae's Essential Law for Journalists: "the term media organisations [is used to] encompass the publishers of newspapers, [news] magazines and [journalistic] websites, and [news] broadcasters. As we have acknowledged previously, the term is not wholly satisfactory, […] but we felt it remains the most practical option to reflect the technological convergence in how journalism is published."[63] This characterisation and justification of the continued use of the term "media organisations" reflect the fact that such institutions are still responsible for the mainstream investigation and proliferation of news. Clarification of some terms in the definition is needed because it is broadly common parlance in journalism to refer, for example, to news organisations that primarily air current affairs programmes via radio and television as "broadcasters;" however, this is not true of technologist communities, where the same word may refer to companies such as Netflix. Further, while the term "press" can be seen as referring only to print journalism, this thesis uses it interchangeably with "media" (as is common), to signify the importance of not neglecting the cyber security of traditional journalism, as new media is mostly digital.[64]

Despite the myriad of potential attack models that can threaten media companies through many other cyber-physical vectors, this thesis only briefly addresses attacks on media organisation infrastructure and supply chains.[65] This is because these aspects of the industry are in flux, and because there are so many smaller news organisations that are structured variably and so face different threats. Instead, this thesis focuses on the core, common feature of the press (including news organisations), irrespective of the shifting media landscape at present, i.e. journalists and their sources.

---

[61] Perkin G (1965) News. In: Revill L and Roderick C (eds) *The Journalist's Craft: A Guide to Modern Practice*. 1st ed. Sydney, Australia: Angus and Robertson.

[62] Harcup T and O'Neill D (2017) What is News? *Journalism Studies* 18(12). Routledge: 1470–1488. DOI: 10.1080/1461670X.2016.1150193.

[63] Dodd M and Hanna M (2018) *McNae's Essential Law for Journalists*. 24th ed. Oxford: Oxford University Press: vii.

[64] Kroon RW (2010) A/V A to Z: An Encyclopedic Dictionary of Media, Entertainment and Other Audiovisual Terms. North Carolina: McFarland.

[65] *Such as supply chain attacks that exploit insecure technological infrastructure of the entire industry such as communications equipment and hacks of internet-connected security systems and other remote-access devices.*

While conducting the exploratory study (see: Chapter 4), interviewees were asked where they believe the responsibility falls, regarding educating and training journalists on such threats. More respondents answered that this should be part of the role of media organisations than any other group, although "other journalists," "non-governmental organisations" and "professional unions" were also believed to play key parts in defending the press against attacks, both legal and cyber-physical. In addition, in January 2020 the UK Foreign and Commonwealth Office and Global Affairs Canada convened the first meeting of the Media Freedom Coalition. There, for the first time, there were references to "media organisations" along with individual journalists as facing threats from "overly restrictive laws, punitive legal measures, arbitrary or unlawful surveillance and physical violence."[66] Given this, and considering the substantial impact of large news organisations, both within the domestic media ecosystem of a country and even as actors with influence in the international arena, this thesis' toolkit (see: Chapter 8) is designed to be usable by large news organisations, as well as by freelancers and smaller national and local news outlets.

1.5 Thesis aims and contributions

Guided by the research question above, this section provides an overview of the aims and structure of this DPhil. This DPhil offers contributions to the fields of computer science and cyber security, as well as to journalism studies. The research additionally makes real-world contributions to media organisations and journalists currently working in the field. The primary objective of this DPhil research is to create a toolkit for improvement of the media's ability to recognise, understand and manage risk from the consumer Internet of Things (IoT). The aim of this toolkit is to be used in cyber security strategies to protect the press and their sources. To achieve this, the thesis offers four main contributions: (1) Assessing IoT risk to the media, (2) Conceptualising IoT risk to the media (3) Situating IoT risk within the media's real-world threat landscape, and (4) Providing tools for the media to manage IoT risk. This section provides an overview of the ways in which key themes throughout this thesis contribute novel insights. See Chapter 9 for a more extensive discussion of contributions and areas for further development.

(1) Assessing IoT risk to the media. The exploratory study (see: Chapter 4) investigated how some high-risk members of the media perceive and combat IoT threats to their work and wellbeing. The study found that most of the exploratory study's interviewees, who were all media experts, only had an abstract idea of IoT threats, thus highlighting the need for further research and resources. All interviewees said that their primary strategy for mitigation of IoT threats is simply to avoid interaction with IoT devices. However, 26 out of 34 surveyed cyber security experts said that they believed that it would be impossible for members of the general public to opt-out of interaction with the IoT within the next five years, which would render the primary strategy given by all journalist respondents completely redundant. Most exploratory study participants said that news organisations should be responsible for informing journalists of IoT threats and protections. This caused a component of the toolkit – the framework (see: Chapter 8) – to reference the overarching editorial workflow and the role types found at a typical news organisation.

To ensure that this research is tailored to the media rather than replicating the technical jargon often found in IoT research, Chapter 2 focused on removing definitional ambiguity of the concepts central to this research. The analytical strength of the literature review comes in part by bringing different bodies of literature uniquely together, drawing both from, for example, privacy and security debates within

[66] UK Foreign and Commonwealth Office (2020) *Policy paper: Statement by the Media Freedom Coalition on its first meeting*. 25 February. London, UK: UK Foreign and Commonwealth Office. Available at: https://www.gov.uk/government/publications/media-freedom-coalition-january-2020-meeting-statement/statement-by-the-media-freedom-coalition-on-its-first-meeting (accessed 5 March 2020).

computer science and surveillance studies, public policy analysis from law, and journalistic practice reflections from journalism studies. This literature synthesis builds a foundation for the compilation of categorisation systems of IoT devices and associated threats (see: Chapter 5). These aim to help the press with both risk assessments (see the gap identified in Chapter 4) and asset inventories, which are a key part of the first step, 'Identify', of the NIST CSF,[67] which underpins this thesis' final framework.

(2) Conceptualising IoT risk to the media. The first part of Chapter 5 presents a conceptual model of consumer IoT device categories, organised by environments in which journalists may encounter these devices and associated threats. This fills a gap in journalistic understanding of prevalence and relevance of IoT threats to them and their work which was noted in the literature review (see: Chapter 2) and discovered in practice when conducting the exploratory study (see: Chapter 4). Chapter 5's second conceptual model also addresses a clear and tangible gap in academic and journalistic literature so that the full impact of threats from the IoT may be understood. This is done by bringing together different kinds of IoT threats, including those with legal, cyber-physical and virtual consequences into one overarching conceptual presentation. Without adequate anticipatory threat modelling within the news industry, the rise in prevalence and sophistication of IoT devices could greatly exacerbate the adversary-defender asymmetry.[68] These models therefore provide a unique contribution to multiple areas of knowledge and research and act as a foundation for future research into both journalism and cyber security.

For instance, both models can inform computer scientists who are looking to identify and fill gaps in the range of consumer IoT technologies available commercially. Further, the second model presented in Chapter 5 can be of use to the Human-Computer Interaction (HCI) community because it collates information around IoT threats to stakeholders in the media, which has not yet been done either academically or journalistically. It may also be used to develop other IoT threat model categorisations for other, media-adjacent populations, such as activists.

Further, Chapter 8's framework is also intended to be of use to computer science because it highlights areas where more work is needed in both cyber security research and product development to meet these training, tool-creation, and threat modelling needs. Additionally, this toolkit, as discussed in Chapter 9, represents an example of academic research improving practice in a critical industry. The fact that this intersection of journalism and the IoT is so sparse in terms of research means that there is potential for this thesis to have a huge impact in practice. In fact, this research has already garnered interest from stakeholders such as civil society organisations whose work aims to improve the security of vulnerable and highly targeted groups, such as journalists and activists. To this end, both Chapter 2 and Chapter 9 highlight areas for further academic research in computer science, cyber security, and journalism studies.

(3) Situating IoT risk within the media's real-world threat landscape. Drawing from the exploratory study revealing the extent of the gap in journalistic protective practices (see: Chapter 4), building on the conceptual models illustrating environments and vectors through which journalists may face threats from the IoT (see: Chapter 5), Chapters 6 and 7 examine how journalists working in the US, UK, Australia, and Taiwan perceive IoT threats to their work. These four investigations involved interviewing experts about the IoT market, data-related legislation, and the journalism landscape in each of the four countries. These

[67] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018, 16 April. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.04162018.

[68] Kazansky B (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society 8(1). SAGE Publications Ltd: 2053951720985557. DOI: 10.1177/2053951720985557.

interviews document how policy and legislation decisions have affected and will affect how the IoT can threaten the press, building on Chapter 2's illustration of the relationship between state surveillance and the IoT. The chapters analyse similarities and differences between the countries, to feed into the final framework (see: Chapter 8) and ensure its applicability across a range of democratic countries.

The country profiles (see: Chapters 6 and 7) are of use to computer scientists because they make it possible to ground any technical recommendations, frameworks, and further research in existing real-world practice. These studies are also of use to computer science because they provide contemporary insights into the different legislative and policy considerations that affect IoT security and prevalence, as well as into market perceptions from users in different countries, which could inform future technological design considerations. These studies benefit journalists by analysing existing legal threats (especially in terms of surveillance) and where geopolitical pressures may arise that could impact both IoT availability and create threats that could impact their work and wellbeing.

(4) Providing tools for the media to manage IoT risk. The intention of this thesis is to create a peer-to-peer effect, whereby members of the press are motivated to share threat intelligence and participate in any training that arises using the toolkit in this thesis. The creation of an information-rich framework contributes a mechanism for continual risk assessment by the media. This enables journalists to develop habits of detecting and mitigating IoT threats, which is more likely to be successful than attending one-off training sessions.[69] They can also benefit from a political climate of increased awareness of IoT threats to press freedom and possible solutions that could arise as a consequence of the publication of this thesis. The goal is for the framework presented in this thesis to contribute the equivalent of a journalism-specific "informative reference," such that members of the media may use it to create a more informed NIST "Framework Profile."[70]

Finally, this thesis supports the work currently being undertaken by the HCI academic community to push for design requirements to be shifted to incorporate better device security. Crucially, this keeps the onus from being on users to be experts in managing ambient security, a theme reflected in this thesis's toolkit. Further, the exploratory study (see: Chapter 4) surfaced a lack of existing tools and frameworks to address ways in which IoT devices can be used to perpetrate physical, legal, and virtual threats against the press and free speech more broadly. Additionally, this thesis investigates a situation in which there is a security asymmetry between attackers and targets, so research into this could shed light on other problems of this nature.

1.6 Publications arising from this thesis

Various components of this thesis have been presented and published separately as peer-reviewed papers. Each of the three studies that form Chapters 4 (exploratory study) and Chapter 5 (conceptual models) were peer-reviewed individually for the 2020 IEEE European Symposium on Security and Privacy Workshops,[71] the International Conference on Cybersecurity, Situational Awareness and Social

[69] Oliver J (2018) Journalism schools still behind on cybersecurity training, new survey finds. Available at: https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php (accessed 15 November 2020).

[70] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018, 16 April. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.04162018.

[71] Shere ARK, Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.

Media,[72] and the International Association for Media and Communication Research 2022.[73] The "related work" and "methodology" sections from these articles are included in Chapter 2 (literature review and synthesis) and Chapter 3 (methodologies) respectively. Three other peer-reviewed publications also contributed to Chapter 2, in The Sciences Po Cybersecurity Association's Academic Journal,[74] the Journal of Cyber Policy,[75] and The New Collection.[76] Two of these influenced the legal and policy parts of Chapters 6 (legislative and policy challenges for the press) and Chapter 7 (geopolitical and organisational challenges for the press).[77]

Further, throughout this doctoral research, pieces of these studies influenced non-peer-reviewed outreach materials that were released to help raise awareness of IoT risk, relevant legal threats and cyber-attacks on the media. These were published via platforms aimed at journalistic and policy audiences across the countries profiled in this thesis, and beyond, specifically *The Journalist's Resource*, *RUSI Newsbrief*, *The Conversation*, *Wavell Room*, *Jane's Intelligence Review*, and the *Shorenstein Center*'s commentary blog.[78]

[72] Shere ARK, Nurse JRC and Martin AP (2023) Threats to journalists from the consumer Internet of Things. In: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Springer Nature. Wales, UK: Springer, p. 230. Available at: https://link.springer.com/book/9789811964138.

[73] Shere A, Nurse J and Martin A (2022) "It's not paranoia if they really are out to get you": navigating risk to journalists when connected devices are everywhere. In: *Presented at IAMCR 2022*, Beijing, China, 11 July 2022. The International Association for Media and Communication Research (IAMCR). Available at: https://ora.ox.ac.uk/objects/uuid:f2c3134b-a6bc-4071-b207-ec7f7cedb118 (accessed 27 September 2022).

[74] Ashdown N and Shere ARK (2021) The Security Implications of Robotic Surveillance Pigeons – Sciences Po Cybersecurity Association. *The Sciences Po Cybersecurity Association's Academic Journal* 1(1). Available at: https://scpo-cybersecurityassociation.com/index.php/2021/03/29/the-security-implications-of-robotic-surveillance-pigeons/ (accessed 27 September 2022).

[75] Shere ARK (2020) Now you [don't] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy* 5(3). Routledge: 429–448. DOI: 10.1080/23738871.2020.1832129.

[76] Shere A (2020) Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis. *The New Collection* 14: 3–21.

[77] Shere ARK (2020) Now you [don't] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy* 5(3). Routledge: 429–448. DOI: 10.1080/23738871.2020.1832129; Shere A (2020) Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis. *The New Collection* 14: 3–21.

[78] Shere ARK (2022) 6 ways the Internet of Things poses security threats to journalists. In: *The Journalist's Resource*. Available at: https://journalistsresource.org/media/6-ways-the-internet-of-things-poses-security-threats-to-journalists/ (accessed 6 December 2022); Shere A (2021) How the Internet of Things poses a threat to journalists. In: *The Journalist's Resource*. Available at: https://journalistsresource.org/home/how-the-internet-of-things-poses-a-threat-to-journalists/ (accessed 5 May 2022); Shere ARK and Nurse JRC (2020) Police surveillance of Black Lives Matter shows the danger technology poses to democracy. *The Conversation*, 24 July. Available at: http://theconversation.com/police-surveillance-of-black-lives-matter-shows-the-danger-technology-poses-to-democracy-142194 (accessed 29 March 2022); Shere ARK and Melcher M (2020) Investigating the Information Commissioner's Office: Is It Fit for Purpose? *RUSI Newsbrief*, 13 November. Whitehall, London, UK. Available at: https://www.rusi.org/publication/investigating-information-commissioner%E2%80%99s-office-it-fit-purpose (accessed 27 September 2022); Shere ARK (2021) Legal tiptoeing: the Integrated Review, Data-Sharing, and the EU. In: *Wavell Room*. Available at: https://wavellroom.com/2021/06/22/legal-tiptoeing-the-integrated-review-data-sharing-and-the-eu/ (accessed 27 September 2022); Shere ARK and Ashdown N (2020) Growth of privately held data increases risk of espionage. *Jane's Intelligence Review*. Available at: https://www.janes.com/images/assets/638/94638/Growth_of_privately_held_data_increases_risk_of_espionage.pdf; Shere ARK (2023) Threats To Press Freedom In The COVID-19 Era. In: *Shorenstein Center*. Available at: https://shorensteincenter.org/commentary/threats-press-freedom-covid-19-era/ (accessed 19 June 2023).

Chapter 2: Synthesis of Relevant Literature

2.1 Introduction

This thesis focuses on ascertaining how members of the press in democratic countries can improve their identification of, protection from, and resilience against threats from the Internet of Things (IoT). This chapter therefore evaluates the literature that exists on the intersections between journalism, democracy and the IoT, to establish a knowledge gap.

This literature review and synthesis is intended to assess current evidence relating to how the IoT threatens journalists' security and privacy. Therefore, it is organised by four specific questions to establish the gap this thesis fills. First, as the IoT is relatively novel, this chapter discusses "What is the Internet of Things and how can it effectively be categorised?" This subsection defines the scope of this research, focusing on systems of categorisation to assess the utility of different lenses for specific audiences. Second, the chapter addresses the question "What is the relationship between the IoT and privacy and security?" It particularly focuses on the former as the mass data collection, storage and transfer properties that are inherent to the IoT have implications for privacy that may subsequently cause insecurity. Third, this chapter asks, "How do states regulate the IoT?", which is particularly relevant to Chapters 6 and 7. Fourth, the chapter answers the question "What is the current state of literature on IoT threats to the free press?", appraising literature relevant to technological threats to the free press, specifically looking for any on IoT threats, per Chapter 5. This section assesses whether any available materials are useful to the press, which relates to the framework and thus Chapter 8.

2.2 What is the Internet of Things and how can it effectively be categorised?

This section examines how this thesis will define what counts as the Internet of Things (IoT), and reviews existing categorisation methods. Although the term IoT is concise, in fact it belies multiple decades of technological development and continued debates over how to effectively categorise devices that have multiple stated and potential functionalities. This subsection will delve into this development to determine the most relevant definition for use in this thesis. In addition to reviewing definitional choices, this section also considers how IoT devices have been categorised in existing research. Reviewing categorisation of the IoT is important for this research for two reasons: First, to define the scope of this thesis. Second, as also discussed in sections 2.5 and 3.5.2, because communicating risk to the media is most effective when the language and the framing are matched to the needs of those implementing recommendations. [79]

2.2.1 Defining the scope of the IoT

There is currently no single accepted definition of the IoT.[80] Such technologies are considered to have originated with the idea of the "Disappearing Computer" in the late 1980s,[81] because of a desire for technology to forego physical interactive interfaces. Devices were conceptualised that could implicitly

[79] Rasmussen, L.B.: The narrative aspect of scenario building - How story telling may give people a memory of the future. AI & Soc. 19, 229–249 (2005). https://doi.org/10.1007/s00146-005-0337-2.

[80] Goumagias N, Whalley J, Dilaver O, et al. (2021) Making sense of the internet of things: a critical review of internet of things definitions between 2005 and 2019. *Internet Research* 31(5). Emerald Publishing Limited: 1583–1610. DOI: 10.1108/INTR-01-2020-0013.

[81] Privacy International (2016) Why the Internet of Things Begs for a Paradigm Shift in Internet Security. Available at: http://www.privacyinternational.org/blog/862/why-internet-things-begs-paradigm-shift-internet-security (accessed 9 September 2019).

intuit user needs through connection to the internet that would "benefit from pervasive sensing."[82] The specific term "Internet of Things" originated in 1999, as a buzzword created for marketing purposes during an industry presentation.[83] The initial presentation extolled the potential of "enabl[ing] computers to observe, identify and understand the world—without the limitations of human-entered data."[84] Similar concepts at the time, such as "ubiquitous computing" or "pervasive computing," lost traction as phrases compared to "the IoT." Since then, both academic and popular understandings of the IoT have evolved, alongside the unfettered growth of an industry that produces diverse internet-connected devices. It must be noted that the term "IoT" appeared to be designed to make the devices seem novel to industry executives and consumers.

The popular impression made by the proliferation of the IoT has facilitated the creation of multiple nebulous definitions.[85] For example, Heer *et al.* defined the IoT as denoting "the interconnection of highly heterogeneous networked entities and networks following a number of communication patterns such as: human-to-human (H2H), human-to-thing (H2T), thing-to-thing (T2T), or thing-to-things (T2Ts)."[86] Miorandi *et al*. described the IoT as using the Internet "for interconnecting physical objects that communicate with each other and/or with humans in order to offer a given service."[87] Owing to the heterogeneity of the devices that comprise the IoT, these general characterisations are vague enough that they do not conflict. The main similarity between these two definitions is their focal point, as both Heer *et al*. and Miorandi *et al*. centred the connection between devices, i.e. they were "Internet-oriented."[88] In contrast, the attempt at consolidation of IoT definitions by Minerva *et al.* emphasised the capabilities of the individual devices ("Things") and how their functions can be altered through other devices in the network.[89]

This thesis does refer to the "IoT", although the term creates an artificial distinction between the technologies underpinning some IoT devices and legacy devices (e.g. phones, tablets, laptops, and desktop computers). While the IoT makes use of some relatively new technologies (e.g. 5G connectivity), it would be misleading to frame this research as though the IoT constitutes an entirely new set of systems. In fact,

[82] Privacy International (2016) Why the Internet of Things Begs for a Paradigm Shift in Internet Security. Available at: http://www.privacyinternational.org/blog/862/why-internet-things-begs-paradigm-shift-internet-security (accessed 9 September 2019).

[83] Gabbai A (2015) Kevin Ashton Describes 'the Internet of Things'. Available at: https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/ (accessed 11 May 2022); Elder J (2019) How Kevin Ashton named The Internet of Things. Available at: https://blog.avast.com/kevin-ashton-named-the-internet-of-things (accessed 11 May 2022).

[84] Ashton K (2009) That 'Internet of Things' Thing. *RFID Journal*. Available at: https://www.rfidjournal.com/articles/view?4986 (accessed 8 February 2020).

[85] Goumagias N, Whalley J, Dilaver O, et al. (2021) Making sense of the internet of things: a critical review of internet of things definitions between 2005 and 2019. *Internet Research* 31(5). Emerald Publishing Limited: 1583–1610. DOI: 10.1108/INTR-01-2020-0013.

[86] Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K (2011) Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications* 61(3): 527–542. DOI: 10.1007/s11277-011-0385-5.

[87] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10(7): 1497–1516. DOI: 10.1016/j.adhoc.2012.02.016.

[88] Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K (2011) Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications* 61(3): 527–542. DOI: 10.1007/s11277-011-0385-5; Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10(7): 1497–1516. DOI: 10.1016/j.adhoc.2012.02.016.

[89] Minerva R, Biru A and Rotondi D (2015) *Towards a definition of the Internet of Things (IoT)*. IEEE Internet Initiative, 27 May. IEEE. Available at: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed 9 September 2019).

many IoT devices utilise common technical architectures and platforms,[90] including low-compute and embedded systems. “Things” have been connected to computers for decades, for example via dedicated serial lines and dial-up modems; IoT represents a push to standardise some of those diverse connections. What makes the IoT notable is its prevalence and permeation across all spheres of life. It unobtrusively replaces devices that were previously not at all computational or connected, in a clear move towards hyperconnectivity and miniaturisation that are intended to reduce overall cost and increase flexibility.[91]

The IoT can be called “smart,”[92] but this can also be used to denote machine learning capabilities (which applies to some but not all IoT devices).[93] This thesis recognises the multifaceted understandings of the term “smart” and will avoid using “smart devices” except when necessary. One such instance will be to engage with or refer to responses provided by research participants who are familiar with the meaning of “smart” as IoT devices that are connected and able to respond to their environment, without necessarily including artificial intelligence.

Dorsemaine *et al.* consider legacy technologies to be part of IoT communication chains, as they may be used to send commands to IoT devices.[94] However, in this thesis instead a clear distinction between legacy and IoT devices is drawn;[95] it views IoT devices as “dedicated objects” that have specific primary purposes in addition to their connectivity (e.g. “vending machines, jet engines, connected soap dispensers.”)[96] This is because the crux of this research is that taking a purely technical perspective on the capabilities of IoT devices is insufficient to address the myriad of social, policy and legislation-based threats that can exploit these technologies. Additionally, the term IoT suits the communication needs of the target beneficiaries of this research, and to disregard this entirely would be to ignore the effect that name recognition created by marketers has on non-technical experts, including journalists.

---

[90] Smith S (2017) *The Internet of Risky Things: Trusting the Devices That Surround Us*. 1st ed. Sebastopol, CA, USA: O’Reilly Media, Inc.

[91] Nurse J, Erola A, Agrafiotis I, et al. (2015) Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things. In: Proceedings of the 2015 International Workshop on Secure Internet Of Things (SIoT), Vienna, Austria, 21 September 2015. DOI: 10.1109/SIOT.2015.10; Smith S (2017) *The Internet of Risky Things: Trusting the Devices That Surround Us*. 1st ed. Sebastopol, CA, USA: O’Reilly Media, Inc.

[92] Department for Digital, Culture, Media & Sport (2018) Smart devices: using them safely in your home. Available at: https://www.gov.uk/government/publications/smart-devices-using-them-safely-in-your-home/smart-devices-using-them-safely-in-your-home (accessed 4 March 2020); Gradinar A, Van Kleek M, Pschetz L, Coulton P, Lindley J (2019) The Little Book of the Internet of Things for the Home. Lancaster: Lancaster University. DOI: https://eprints.lancs.ac.uk/id/eprint/136910/1/Little_Book_of_IoT_Home_Online.pdf; Silverio-Fernández M, Renukappa S and Suresh S (2018) What is a smart device? - a conceptualisation within the paradigm of the internet of things. Visualization in Engineering 6(1): 3. DOI: 10.1186/s40327-018-0063-8; Motta RC, de Oliveira KM and Travassos GH (2018) On challenges in engineering IoT software systems. In: Proceedings of the XXXII Brazilian Symposium on Software Engineering, Sao Carlos, Brazil, 17 September 2018, pp. 42–51. SBES ’18. Association for Computing Machinery. DOI: 10.1145/3266237.3266263.

[93] Indu K and Aswatha KM (2019) A Study on Machine Learning Techniques for Internet of Things in Societal Applications. In: 2019 International Conference on Data Science and Communication (IconDSC), March 2019, pp. 1–6. DOI: 10.1109/IconDSC.2019.8816970.

[94] Dorsemaine B, Gaulier J-P, Wary J-P, et al. (2015) Internet of Things: A Definition Taxonomy. In: *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, September 2015, pp. 72–77. DOI: 10.1109/NGMAST.2015.71.

[95] Weinberg BD, Milne GR, Andonova YG, et al. (2015) Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons* 58(6). SPECIAL ISSUE: THE MAGIC OF SECRETS: 615–624. DOI: 10.1016/j.bushor.2015.06.005; Minerva R, Biru A and Rotondi D (2015) *Towards a definition of the Internet of Things (IoT)*. IEEE Internet Initiative, 27 May. IEEE. Available at: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed 9 September 2019); Blythe JM and Johnson SD (2019) A systematic review of crime facilitated by the consumer Internet of Things. Security Journal. DOI: 10.1057/s41284-019-00211-8.

[96] Pettey C (2015) The Internet of Things and the Enterprise. Available at: //www.gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise/ (accessed 22 January 2020).

Therefore, given the prevalence of guidance on mature technologies (phones, laptops, tablets, and desktop computers), this research considers the IoT to exclude the aforementioned traditional devices and any well-known and well-studied threats that are not unique to or exacerbated by the IoT.[97] Phones and laptops have been the main target of attacks against journalists in the past. This thesis will build upon relevant literature and knowledge gained from attacks and research on these traditional targets, including those relating to smartphone spyware. This will enable this thesis to establish an understanding of how corresponding attacks could occur in the IoT space.

Further, to avoid repetition and because NIST definitions refer to the IoT as both "connected" and "a network,"[98] "IoT" is used interchangeably in this thesis with "connected,"[99] or "networked,"[100] which are objectively true and not indicative of a judgement on their capabilities, like "smart." NIST definitions are the industry standard and are used in other ways throughout this dissertation (see: Chapters 1 and 9). Therefore, the term "IoT" in this thesis covers a range of devices from voice assistants (like Alexa and Google Home) to equipment that was not previously connected but has had this capability built into later models (like smart fridges and video-equipped doorbells).

2.2.2 Smart cities and scoping

The total of the IoT encompasses everything from consumer or smart home IoT to Industrial IoT (such as that used in transport), public sector IoT (such as systems used by law enforcement agencies, and to IoT used for national infrastructure. Given the broad scope of all these applications, this thesis focuses solely on consumer IoT, some of which can also be found in public spaces (such as wearable devices). However, this subsection will nevertheless briefly address the scholarship on "smart cities" because smart cities and their associated data protection privacy threats are sufficiently relevant to journalists in understanding how their surroundings might facilitate ambient threats, per Chapter 5's environmental IoT model.[101]

There are many applications of the IoT that are directly linked to political governance, including smart cities. These have no formal definition but are often loosely depicted as an abstract large-scale system of systems. Morabito describes smart cities as "an advanced connectivity through a highly networked city infrastructure via intelligent assets" and smart city infrastructure as "the bundle of Internet of Things solutions for city infrastructure management and intelligent infrastructure-citizen interfaces."[102] Hashem *et al.* emphasised the significance of Big Data collection and "information sharing" in smart cities, saying

[97] Blythe JM and Johnson SD (2019) A systematic review of crime facilitated by the consumer Internet of Things. Security Journal. DOI: 10.1057/s41284-019-00211-8

[98] National Institute of Standards and Technology (NIST) (2022) Internet of Things (IoT) - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/internet_of_things_IoT (accessed 11 May 2022).

[99] Bugeja J, Davidsson P and Jacobsson A (2018) Functional Classification and Quantitative Analysis of Smart Connected Home Devices. In: 2018 Global Internet of Things Summit (GIoTS), Bilbao, June 2018, pp. 1–6. IEEE. DOI: 10.1109/GIOTS.2018.8534563.

[100] Simmon ED, Kim K, Subrahmanian E, et al. (2013) A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems. NIST Interagency/Internal Report (NISTIR)-7951, NIST Interagency/Internal Report (NISTIR), 26 August. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/publications/vision-cyber-physical-cloud-computing-smart-networked-systems (accessed 11 February 2020).

[101] Department for Digital, Culture, Media & Sport and Lopez (MP) J (2022) Secure connected places (smart cities) guidance collection. Available at: https://www.gov.uk/government/publications/secure-connected-places-smart-cities-guidance-collection (accessed 5 December 2022); Arroub A, Zahi B, Sabir E, Sadik M (2016) A literature review on Smart Cities: Paradigms, opportunities and open problems. In: 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), October 2016, pp. 180–186. DOI: 10.1109/WINCOM.2016.7777211.

[102] Morabito V (2015) *Big Data and Analytics: Strategic and Organizational Impacts*. New York, NY: Springer Berlin Heidelberg. Available at: http://index-of.co.uk/Big-Data-Technologies/Big%20Data%20and%20Analytics%20-%20bb.pdf: 26.

that this is "achieved by seamless ubiquitous sensing, data analytics, and information representation with cloud computing as the unifying framework."[103]

According to Söderström *et al,* discourse around standardising a definition of smart cities is often laden with vested interest from actors involved in every aspect of a city, from overall political conceptualisation to corporate construction of specific segments, such as smart electricity grids.[104] This is a particularly relevant insight for this thesis, as the multitude of stakeholders in IoT environments, including states, complicates attempts at regulation. Additionally, this thesis subscribes to the portrayal offered by Zanella *et al.* of smart cities as an effort to mitigate issues stemming from rising global populations. Zanella *et al.* argue that smart cities more effectively harnessing public resources to deliver high quality civic services through the use of an "urban IoT" that has two main functions: First, through management of "traditional public services, such as transport and parking, lighting, surveillance and maintenance of public areas", etc., and second, through the IoT's pervasive Big Data collection to optimise a city's services.[105] Although this research has not yet found any academic sources looking at the ways in which smart cities might specifically harm the free press, there are a wealth of readings on smart city governance and threats to civilian privacy and security,[106] which informed the journalism-specific IoT threats categorisation system (see: Chapter 5).

2.2.3 Categorising the IoT and its threats

IoT devices can be categorised in a number of ways, including by methods of connectivity and device capabilities. Beyond organising functions, IoT categorisation structures can examine aspects such as the targets of IoT threats and the audience to whom the information must be conveyed. This dissertation requires categorisation of IoT devices, associated threats and potential protective and mitigative mechanisms in ways that are clear and intuitive for members of the media. This section therefore discusses how categorisation mechanisms are a well-established academic and educational tool for aiding understanding of the IoT. It also determines why it is necessary to design one specifically for the media community.

One recurring feature across much of the literature was the presentation of IoT taxonomies of various types,[107] many of which will be discussed below. However, in all versions, they commonly catered to an audience with the skills to recognise technical distinctions between devices. For example, Dorsemaine *et al*. intended that their taxonomy be useful for "a corporate environment"; their categories were largely technical. Therefore, for an individual to sort IoT devices into their taxonomy, one would have to, for example, be able to differentiate between which part of an IoT network (i.e. 'the object' or 'the pickup point') initiates communications.[108] Similarly, Mountrouidou *et al*.'s target user group was technically proficient, as it relies on, for example, practitioners being able to tell whether a device has one or more

[103] Hashem IAT, Chang V, Anuar NB, et al. (2016) The role of big data in smart city. *International Journal of Information Management* 36(5): 748–758. DOI: 10.1016/j.ijinfomgt.2016.05.002.
[104] Söderström O, Paasche T and Klauser F (2014) Smart cities as corporate storytelling. *City* 18(3): 307–320. DOI: 10.1080/13604813.2014.906716.
[105] Zanella A, Bui N, Castellani A, et al. (2014) Internet of Things for Smart Cities. *IEEE Internet of Things Journal* 1(1): 22–32. DOI: 10.1109/JIOT.2014.2306328.
[106] Kitchin R (2016) The ethics of smart cities and urban science. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374(2083): 20160115. DOI: 10.1098/rsta.2016.0115.
[107] Mountrouidou X, Billings B and Mejia-Ricart L (2019) Not just another Internet of Things taxonomy: A method for validation of taxonomies. *Internet of Things* 6: 100049. DOI: 10.1016/j.iot.2019.03.003.
[108] Dorsemaine B, Gaulier J-P, Wary J-P, et al. (2015) Internet of Things: A Definition Taxonomy. In: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9 September 2015, pp. 72–77. IEEE. DOI: 10.1109/NGMAST.2015.71.

communications channels, which is not part of journalists' training.[109] There is therefore a need to create a new categorisation method of devices specifically for the media, as they have little pre-existing knowledge of the devices as a concept and a potentially limited technical understanding. They also have a personal and professional stake in obtaining information on the full spectrum of functionalities and locations of the IoT as quickly and easily as possible due to the heightened risk to their community as a result of the spread of the IoT.

Given the key beneficiaries of this thesis are members of the media, conceptual models rather than taxonomies were the chosen method in order to make the information more easily understandable by users. However, existing taxonomies were informative in developing the content of these models. More details about the rationale for using conceptual models can be found in Chapters 3 and 5.

Nevertheless, existing taxonomies had many useful principles and information this thesis builds on. For example, Mountrouidou *et al*.'s validation taxonomy proposed three principles for verifying the utility of an IoT categorisation system: that "it has to be complete, precise, and inclusive to lead to appropriate tools and security techniques," which are principles used in writing Chapter 5. For Weinberg *et al*., their taxonomy was application-based, which provides a similar classification system to Chapter 5's IoT device model, with the following categories: "wearables," "health care," "building and home automation," "smart manufacturing," "smart cities" and "automotive."[110]

As a key motivation for compiling the IoT devices organisational model was to help journalists identify IoT risk, it was determined that a useful way to structure it was to map devices to the locations in which journalists were likely to passively interact with them (see Chapter 5 for more detail). It was therefore important to review literature that organised the IoT in a similar system. For example, one of the dimensions that Alkhabbas *et al*. specified to define IoT "Things" is "physical locations where they are installed"[111] including in "buildings, human bodies, and cities." This was a useful starting point but needed more granularity to ensure it was sufficiently useful to lay-people readers. In contrast, Smith's comprehensive map of IoT business development activity was aesthetically clear, but it placed IoT devices into mutually exclusive categories that are not practical – for example, 'buildings' and 'consumer and home' are two separate categories that both include lights and are not visually portrayed as overlapping.[112]

Some taxonomies, like van Zoonen *et al.*'s more recent research resolved this issue by noting that smartphone use cannot be siloed in either personal or professional spheres. [113] While this highlighted the blurred boundaries of personal technologies, they did not extend this consideration into including IoT devices in their study. A more relevant taxonomy of connected devices features was by Bugeja *et al.* who

[109] Mountrouidou X, Billings B and Mejia-Ricart L (2019) Not just another Internet of Things taxonomy: A method for validation of taxonomies. Internet of Things 6: 100049. DOI: 10.1016/j.iot.2019.03.003.
[110] Weinberg BD, Milne GR, Andonova YG, et al. (2015) Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons* 58(6). SPECIAL ISSUE: THE MAGIC OF SECRETS: 615–624. DOI: 10.1016/j.bushor.2015.06.005.
[111] Alkhabbas F, Spalazzese R and Davidsson P (2019) Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. *Internet of Things* 7: 100084. DOI: 10.1016/j.iot.2019.100084.
[112] Smith S (2017) *The Internet of Risky Things: Trusting the Devices That Surround Us*. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.
[113] van Zoonen W, Sivunen A and Rice RE (2020) Boundary communication: how smartphone use after hours is associated with work-life conflict and organizational identification. *Journal of Applied Communication Research* 48(3). Routledge: 372–392. DOI: 10.1080/00909882.2020.1755050.

categorised smart home devices based on the technical features of different consumer devices.[114] However, Bugeja *et al.*'s analysis argued that those with fewer capabilities pose less risk, which is not necessarily true for high-risk user-groups such as journalists. Therefore, while these materials were relevant to the structure of Chapter 5's organisational model, they did not share the necessary scope or audience and thus demonstrate the gap this research aimed to fill.

In addition to categorising the IoT, there are ways to conceptualise threats that can arise from them. Having an organised way of thinking about threats is helpful for assessing and managing risk, and modelling threats demonstrates the interlinked nature of different threats from the same system. This is useful as a conceptual foundation for systematically organising emerging threats (see: Chapter 5) within an existing framework[115] or to create a new framework (see: Chapter 8). Xiong and Lagerström discussed that articles in this area either introduce a new method, use an existing threat modelling approach, or present work on the threat modelling process.[116] Chapter 5's threat categorisation aims to do the first and third of these, i.e. to explore an IoT-related threat model that is specific to and can be used by members of the media. This is a gap even within journalism studies: McGregor *et al*.'s study assessing the cyber security behaviours and needs of journalists did not include the IoT.[117]

However, the human-computer interaction and cyber security does have literature relating to IoT threat modelling that spans academic, policy and commercial materials. Each sphere has produced categorisation systems or risk assessment considerations with different classifications, according to the needs of their target audience. Chapter 5's IoT threat categorisation system explicitly focuses on the press as its target population, in order to cater to their specific needs. This builds on existing work in cyber security literature, such as Gulzar and Abbas's taxonomic structure which linked aspects of the IoT with vulnerabilities and threats. However, unlike Chapter 5, their work did not address the practical consequences of these threats.[118] Similar to a home-based IoT security evaluation by Alrawi *et al*.,[119] Nawir *et al*.'s taxonomy of attacks on IoT security was largely categorised by vector.[120] However, some of the attacks in their taxonomy are described in terms of consequences, rather than technique (e.g. "Denial of Service attacks"). Chapter 5's threat categorisation therefore builds on both of these taxonomies to make them directly applicable and relevant to a specific user population, and incorporates them especially into

[114] Bugeja J, Davidsson P and Jacobsson A (2018) Functional Classification and Quantitative Analysis of Smart Connected Home Devices. In: 2018 Global Internet of Things Summit (GIoTS), Bilbao, June 2018, pp. 1–6. IEEE. DOI: 10.1109/GIOTS.2018.8534563.

[115] Electronic Frontier Foundation (2020) Threat model. Available at: https://ssd.eff.org/en/glossary/threat-model (accessed 11 September 2020); Fruhlinger J (2020) Threat modeling explained: A process for anticipating cyber attacks. Available at: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html (accessed 11 September 2020); Torr P (2005) Demystifying the threat modeling process. *IEEE Security Privacy* 3(5): 66–70. DOI: 10.1109/MSP.2005.119; Uzunov AV and Fernandez EB (2014) An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces* 36(4). Security in Information Systems: Advances and new Challenges.: 734–747. DOI: 10.1016/j.csi.2013.12.008.

[116] Xiong W and Lagerström R (2019) Threat modeling – A systematic literature review. *Computers & Security* 84: 53–69. DOI: 10.1016/j.cose.2019.03.010.

[117] McGregor SE, Charters P, Holliday T, et al. (2015) Investigating the Computer Security Practices and Needs of Journalists. In: Proceedings of the 24th USENIX Security Symposium, Washington, D.C., 12 August 2015, p. 17. USENIX Association.

[118] Gulzar M and Abbas G (2019) Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET), Lahore, Pakistan, February 2019, pp. 1–6. IEEE. DOI: 10.1109/CEET1.2019.8711834.

[119] Alrawi O, Lever C, Antonakakis M, et al. (2019) SoK: Security Evaluation of Home-Based IoT Deployments. In: 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2019, pp. 1362–1380. IEEE. DOI: 10.1109/SP.2019.00013.

[120] Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660.

the networked devices threats category. It does so by including example hypothetical consequences, to illustrate risk for journalists.

The threat categorisation system (see: Chapter 5) relies on the use of narrative hypothetical consequences, similar to the scenarios in other informal threat modelling systems for conventional cyber threats to journalists.[121] This is an emerging method of risk communication, called "FicInt" (Fictional Intelligence), which conveys research and intelligence through imaginative storytelling to forecast trends in technologies and threats.[122] However, existing literature on journalistic threat models does not appear to investigate the expanded threat landscape resulting from the increasing prevalence of the IoT. Further, although these other threat models for journalists may touch upon physical and legal threats from legacy devices, going into depth regarding consequences of these types of threats is often beyond their scope. Chapter 5's threats categorisation, in contrast, explores the effects of privacy threats to members of the media as both users and bystanders, as journalists are observers in a multitude of environments.

As discussed in the next section, privacy threats are germane to journalists, who must consider not only the maintenance of their own privacy but the protection of their confidential sources. This priority is therefore included both in Chapter 5's conceptual models as well as a key aspect of Chapter 8's framework. The taxonomy by Weinberg *et al.* focuses on privacy, but does not discuss threats to physical security.[123] These threats are possible due to the physical functionalities of IoT devices and so are investigated in this thesis's categorisation of IoT threats (see: Chapter 5). Like Weinberg *et al*., Dorsemaine *et al*. had a similar long-term aim: to create classes that can help to structure a risk analysis and frame countermeasures.[124] While Chapter 5's IoT device model differs, in that it is environment-focused, compared to the function-centric viewpoint of Dorsemaine *et al.*, they share the same goal, which informs both the categorisation of IoT threats (see: Chapter 5) and the subsequent framework of countermeasures (see: Chapter 8).

2.3 How are privacy and security relevant to the IoT and journalism?

This section focuses on explaining the concepts and relevance of two key aspects of this thesis: the impact that IoT devices have on privacy and security of users. It first defines privacy and security for the purpose of this thesis, then specifically discusses threats related to IoT data collection, before covering the goals of privacy and security by design and default in the IoT, and finally examining the utility of surveillance studies perspectives when evaluating IoT risk to the media. All of these subsection topics represent potential threats to journalists that are categorised and analysed in Chapter 5, explored in country profiles in Chapters 6 and 7, and that are addressed through the design and validation of countermeasures in Chapter 8.

---

[121] Bradshaw P (2014) Why every journalist should have a threat model (with cats). In: *Online Journalism Blog*. Available at: https://onlinejournalismblog.com/2014/07/16/why-every-journalist-should-have-a-threat-model-with-cats/ (accessed 11 September 2020); Stray J (2014) Security for Journalists, Part Two: Threat Modeling. Available at: https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/ (accessed 11 September 2020); Szathmari G (2017) Threats | Threat Modeling | Privacy for Journalists. Available at: https://privacyforjournalists.org.au/threat-modeling-for-journalists (accessed 11 September 2020).

[122] *The True Story of Using Fiction to Enhance Risk Intelligence* (2021) The Association of International Risk Intelligence Professionals (AIRIP). Available at: https://www.youtube.com/watch?v=qP_i94eP2Ho (accessed 18 January 2023).

[123] Weinberg BD, Milne GR, Andonova YG, et al. (2015) Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons* 58(6). SPECIAL ISSUE: THE MAGIC OF SECRETS: 615–624. DOI: 10.1016/j.bushor.2015.06.005.

[124] Dorsemaine B, Gaulier J-P, Wary J-P, et al. (2015) Internet of Things: A Definition Taxonomy. In: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9 September 2015, pp. 72–77. IEEE. DOI: 10.1109/NGMAST.2015.71.

2.3.1 Defining security and privacy for this thesis

This thesis views privacy and security threats from the IoT as inseparable and entangled, for reasons that will be explored in this section. First, it will relate security and then privacy to both the IoT and journalism. This section will then offer context on the conceptual understanding of privacy in the four countries profiled in this thesis, before expanding on the implications of privacy and national security issues regarding press freedom. Finally, it will conclude by explaining how the interconnectedness of privacy and security will be interrogated in the following sections and throughout the thesis.

Perspectives on privacy in journalism practice often relate to the ethics of journalistic activities regarding sourcing of information.[125] That is beyond the scope of this thesis, which primarily takes a cyber security view of privacy, as is increasingly the case in the nascent research into journalists' privacy and security.[126] Further, the issue of data collection – through various means, including having IoT equipment lost, stolen and accessed — is considered in Chapter 5 as a key privacy and data protection threat to the media. This thesis will link threats to privacy to threats to security, as physical threats or legal threats can bridge both. The use of NIST definitions to underpin this view of security (including information security) threats as being linked to the consequences of threats to privacy is consistent with other NIST definitions being used as key foundations of this thesis (see: Chapter 8).

A key reason that this thesis considers privacy and security to be inherently linked is the vast data collection capacities of the IoT and how threats to privacy and physical security can both stem from this single source.[127] This amount of data collected and shared by IoT devices is controversial due to its use by third-parties, such as advertisers, to increase convenience at the expense of user privacy,[128] which can threaten their security both physically and regarding data. Nurse *et al.*'s paper explored the potential for innumerable insider attacks on businesses due to use of various portable IoT devices by employees.[129] All of these debates are relevant to journalists' perceptions of and interactions with the IoT and are explored in Chapter 5's threats categorisation system.

The definition of security used in this thesis is from NIST, specifically: as "a condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach."[130] Regarding the media, security means facilitating

[125] Frost C (2015) Journalism Ethics and Regulation. Oxford, United Kingdom: Routledge.

[126] Di Salvo P (2022) Information security and journalism: Mapping a nascent research field. Sociology Compass 16(3). John Wiley & Sons, Ltd: e12961. DOI: 10.1111/soc4.12961; Holcomb J and Mitchell A (2015) Adoption of Digital Security Tools. In: *Pew Research Center's Journalism Project*. Available at: https://www.pewresearch.org/journalism/2015/02/05/adoption-of-digital-security-tools/ (accessed 9 December 2022).

[127] Troncoso C (2021) *Privacy & Online Rights Knowledge Area*. The Cyber Security Body Of Knowledge Version 1.0.2. Lausanne: Ecole Polytechnique Federale de Lausanne. Available at: https://www.cybok.org/media/downloads/Privacy_Online_Rights_v1.0.2.pdf (accessed 27 April 2022); Ando R, Shima S and Takemura T (2016) Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment. *IEICE TRANSACTIONS on Information and Systems* E99-D(8). The Institute of Electronics, Information and Communication Engineers: 1974–1981.

[128] Perera C, Ranjan R, Wang L, et al. (2015) Big Data Privacy in the Internet of Things Era. IT Professional 17(3): 32–39. DOI: 10.1109/MITP.2015.34.

[129] Nurse J, Erola A, Agrafiotis I, et al. (2015) Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things. In: Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT), Vienna, Austria, 21 September 2015. DOI: 10.1109/SIOT.2015.10.

[130] National Institute of Standards and Technology (NIST) (2022) security - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/security (accessed 28 April 2022).

the free collection, curation and dissemination of the news by minimising the extent to which malicious actors can compromise this process and the actors involved.[131] Cyber security is therefore informed by information security, and covers the prevention of "unwanted physical actions," specifically in the context of the IoT.[132]

When it comes to defining privacy, this thesis draws on the complexities raised by Solove, who struggled to establish a single definition of privacy, citing authors from fields such as legal theory, philosophy and political science, all of whom attested that the concept is both "sweeping" and intangible.[133] According to Thomson, privacy is a "negative right," i.e. it exists by virtue of non-interference, as well as a "derivative right."[134] This latter description means that "the right to privacy" is a non-existent concept that instead appears to be a colloquial reference to other, legally enshrined rights.[135] In contrast to the idea of privacy as a "negative right," Tsui and Lee argued that it has specific implications for the press that are more akin to positive rights, such as the "freedom to produce specific types of 'sensitive' stories, which require a capability to communicate privately and securely with your colleagues, editors, and source."[136] There is likewise overlap between NIST's definitions of "privacy,"[137] "information security"[138] and "security,"[139] all of which mention "confidentiality," with security definitions building on privacy's individual focus to also consider the usability of systems and organisations. Therefore, to understand threats posed to journalists and journalism from the IoT, it is necessary to view both privacy and security from a cyber security perspective as inherently linked concepts.

Solove's additionally useful contribution to the understanding of privacy in this thesis was his argument that privacy relates to issues with both information collection (e.g. surveillance) and information processing (e.g. the creation and use of databases of personal information).[140] Surveillance is particularly likely to inhibit free speech, which Solove acknowledged to be essential for democracy.[141] Meanwhile the latter facilitates further threats such as data aggregation, which could risk identification of sources and threaten their security.[142] Privacy threats create and uphold a power imbalance between those whose

[131] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press: 3-4.
[132] Martin A, Rashid A, Chivers H, et al. (2021) The Cyber Security Body of Knowledge v1.1.0, 2021. University of Bristol. Available at: https://www.cybok.org/.
[133] Solove DJ (2008) Understanding Privacy. Cambridge, Mass: Harvard University Press: pp. 1-4; See further debates on this topic, for example from: Thomson JJ (1975) The Right to Privacy. Philosophy & Public Affairs 4(4): 295–314; Feldman D (1994) Secrecy, Dignity, or Autonomy? Views of Privacy as a Civil Liberty. Current Legal Problems 47(Part_2): 41–71. DOI: 10.1093/clp/47.Part_2.41; and Whitman JQ (2004) The Two Western Cultures of Privacy: Dignity Versus Liberty. The Yale Law Journal 113(71).
[134] Thomson JJ (1975) The Right to Privacy. Philosophy & Public Affairs 4(4): 295–314.
[135] Thomson JJ (1975) The Right to Privacy. Philosophy & Public Affairs 4(4): 312-313.
[136] Tsui L and Lee F (2019) How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. Journalism 00(0). SAGE Journals: 1–23. DOI: 10.1177/1464884919849418.
[137] National Institute of Standards and Technology (NIST) (2021b) privacy - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/privacy (accessed 11 November 2021).
[138] National Institute of Standards and Technology (NIST) (2021a) information security - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/information_security (accessed 11 November 2021).
[139] National Institute of Standards and Technology (NIST) (2021c) security - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/security (accessed 11 November 2021).
[140] Solove DJ (2011) Nothing to Hide: The False Tradeoff Between Privacy and Security. New Haven, UNITED STATES: Yale University Press: 26-27; Solove DJ and Hartzog W (2022) Breached!: Why Data Security Law Fails and How to Improve It. Oxford, New York: Oxford University Press.
[141] Solove DJ (2011) Nothing to Hide: The False Tradeoff Between Privacy and Security. New Haven, UNITED STATES: Yale University Press: 26-27.
[142] Lashmar P (2017) No More Sources? *Journalism Practice* 11(6). Routledge: 665–688. DOI: 10.1080/17512786.2016.1179587.

information is being gathered and used, and those who are gathering and using it.[143] Solove identified harms caused by the erosion of privacy, which is exacerbated by technologies such as the IoT – "indifference, error, abuse, frustration, and lack of transparency and accountability."[144] These are also the problems that journalism, as a "fourth estate" or "watchdog", is responsible for illuminating and so preventing.[145] For this reason, this section investigates the relevance of both concepts to journalists and the IoT.

The politicisation of privacy has specific consequences for members of the free press in two ways: First, due to the implication that states must be complicit in safeguarding or challenging privacy. Second, the interpretation of privacy as the absence of surveillance or interference. According to McStay, journalism's democratic role as a watchdog creates a privacy paradox that stems from the need to breach (to an extent) the privacy of those in power in the name of "public interest," while maintaining the confidentiality of sources.[146]

Although there is not a unified set of media ethics shared by all democratic countries, UNESCO held a series of regional conferences with the intention of developing a universal code of ethics for the media that includes the topics of "global security, human security, privacy, [and] transparency."[147]
While individual privacy and national security are often seen as being at odds, the former is positively correlated with individual security, so the disclosure of personal information about journalists or sources could threaten their security.[148] Per Lisosky and Henrichsen, almost 90% of journalists killed on the job were operating in their home country and 89% of journalist murders result in "little or no prosecution."[149]
While surveillance alone may be considered simply a passive breach of privacy, the technologies needed to effectively surveil an individual may be intrusive to the extent that they threaten individual security, and yet be freely available to consumers. For this reason, it is necessary for these consumer IoT devices to be catalogued and their capabilities made understandable to journalists (see: Chapter 5). Further, Solove debunks the "all or nothing fallacy" that security measures necessarily compromise privacy.[150]

It is important to note, however, that conceptions of privacy and security vary, particularly pertaining to the four countries specifically studied for this thesis. In the Global West, "privacy" is often framed as a "civil liberty," setting it at odds with the equally amorphous concept of "national security" in popular and academic discourse.[151] Whitman distinguished between eighteenth century American and European

[143] Solove DJ (2011) Nothing to Hide: The False Tradeoff Between Privacy and Security. New Haven, UNITED STATES: Yale University Press: 26-27.
[144] Solove DJ (2011) Nothing to Hide: The False Tradeoff Between Privacy and Security. New Haven, UNITED STATES: Yale University Press: 27.
[145] Riaz S (2008) Government Influence on Print Media Content in Pakistan: Pakistani Journalists' Perspective. *Global Media Journal* 1(1). Pakistan Edition. Available at: https://www.aiou.edu.pk/sab/gmj/artical5.asp (accessed 7 February 2020); Christians CG, Glasser T, McQuail D, Nordenstreng K, White RA (2009) *Normative Theories of the Media: Journalism in Democratic Societies.* Urbana and Chicago: University of Illinois Press: 114-137; Lashmar P (2020) *Spies, Spin and the Fourth Estate: British Intelligence and the Media*. Edinburgh, Scotland: Edinburgh University Press.
[146] McStay A (2017) Privacy and the Media. London: SAGE: 27-28.
[147] Capurro R and Britz JB (2010) In search of a code of global information ethics: The road travelled and new horizons. Ethical space: the international journal of communication ethics 7(2/3): 28–36.
[148] Wintterlin F (2020) Trust in distant sources: An analytical model capturing antecedents of risk and trustworthiness as perceived by journalists. Journalism 21(1). SAGE Publications: 130–145. DOI: 10.1177/1464884917716000.
[149] Lisosky JM and Henrichsen JR (2011) War on Words: Who Should Protect Journalists? Washington, USA: Praeger.
[150] Solove DJ (2011) Nothing to Hide: The False Tradeoff Between Privacy and Security. New Haven, UNITED STATES: Yale University Press: 33-38.
[151] Feldman D (1994) Secrecy, Dignity, or Autonomy? Views of Privacy as a Civil Liberty. *Current Legal Problems* 47(Part_2): 41–71. DOI: 10.1093/clp/47.Part_2.41.

ideals of privacy as a derogable human right (i.e. it is non-negotiable); he argued that "protecting privacy means both safeguarding the presentation of self and inhibiting the investigative and regulatory excesses of the state,"[152] the latter of which is a central function of the press. Kerr noted that claims of a "threat to national security" are used to validate "arbitrary executive power" and thus circumvent rights that were previously viewed as "inalienable."[153] For example, post-9/11 global trends were identified in states' behaviours that were seen to infringe individuals' privacy in the name of national security; these included unrestrained data-harvesting through "increased communications surveillance; weakened data protection regimes; increased data sharing; and increased profiling and identification;"[154] all of these are relevant to threats facilitated by the IoT (see: Chapter 5). These trends were not exclusive to the United States or its European allies, but were also noted in Asian countries.[155]

Regarding the relation between these Western conceptions and the Taiwanese case study, Ess wrote that Asian countries are broadly communal, rather than viewing privacy as individual.[156] Still, Ho argued that, owing to the nation's unique cultural and political history, "the notion of privacy has been configured as a fundamental right in Taiwan" and enshrined in legal protections such as Taiwanese Constitutional Court J.Y. Interpretation 585, which "demonstrates the Court's position on respecting autonomy, which it treats as a fundamental value for a liberal democracy."[157] Additionally, Taiwan's media landscape follows an intentionally similar model to other liberal democracies to avoid state interference (see: Chapters 6 and 7).[158]

2.3.2 Threats from IoT data collection

Regardless of the category of system, Seliem *et al*. stated that both the raw data and the intelligence processed by IoT technologies are at risk of leakage that threaten data confidentiality and integrity, which in turn affect security of individuals and systems in which IoT technologies are deployed.[159] As such, there is a growing pool of literature concerning the privacy and security implications of IoT devices. This ranges from high-level categorisation of privacy threats[160] to in-depth technical reviews of features such as

[152] Whitman JQ (2004) The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal* 113(71): 1219.
[153] Kerr THD (2004) Australia's Legislative Response to Terrorism: Strengthening Arbitrary Executive Power at the Expense of the Rule of Law. *Alternative Law Journal* 29(3). SAGE Publications Ltd: 131–134. DOI: 10.1177/1037969X0402900305.
[154] Gomez J (2004) Dumbing Down Democracy: Trends in Internet Regulation, Surveillance and Control in Asia. *ASIARIGHTS* (1). Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.512.9523&rep=rep1&type=pdf.
[155] The Electronic Privacy Information Center (EPIC) (2002) *Privacy & Human Rights 2002: An International Survey of Privacy Rights & Developments*. Washington DC: ELECTRONIC PRIVACY INFORMATION. Available at: https://www.powells.com/book/privacy-human-rights-2002-an-international-survey-of-privacy-rights-developments-9781893044166?partnerid=24075 (accessed 15 March 2020).
[156] Ess C (2005) 'Lost in Translation'?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia). *Ethics and Information Technology*; Dordrecht 7(1): 1–6. DOI: http://dx.doi.org/10.1007/s10676-005-0454-0.
[157] Ho C (2019) Configuration of the Notion of Privacy as a Fundamental Right in Taiwan—A Comparative Study of International Treaties and EU Rules. In: Cohen JA, Alford WP, and Lo C (eds) *Taiwan and International Human Rights: A Story of Transformation. Economics, Law, and Institutions in Asia Pacific*. Singapore: Springer, pp. 423–436. DOI: 10.1007/978-981-13-0350-0_24.
[158] Reporters Without Borders (2020) Taiwan: Media independence on hold | Reporters without borders. Available at: https://rsf.org/en/taiwan (accessed 15 March 2020).
[159] Seliem M, Elgazzar K and Khalil K (2018) Towards Privacy Preserving IoT Environments: A Survey. *Wireless Communications and Mobile Computing* (Article ID 1032761): 15. DOI: https://doi.org/10.1155/2018/1032761.
[160] Medaglia CM and Serbanati A (2010) An Overview of Privacy and Security Issues in the Internet of Things. In: *The Internet of Things* (eds D Giusto, A Iera, G Morabito, et al.), New York, NY, 2010, pp. 389–395. Springer. DOI: 10.1007/978-1-4419-1674-7_38.

wireless sensor networks,[161] or cloud storage systems,[162] much of which informed the research underpinning the threat models explored in Chapter 5. Additionally, some privacy literature is specific to certain kinds of IoT technologies, such as wearables[163] or smart cars.[164] Privacy breaches for these devices divulge information that can lead to physical security threats, and thus much of this literature is relevant to the categorisation of IoT threats (see: Chapter 5).

The creation of consumer profiles by advertising companies has long signified a trade-off between personal privacy and increased ease of access to relevant websites. The prevalence of the IoT means that additional classes of information, such as current location, are included in this equation,[165] which increases the attack surface of vulnerable populations if hostile actors access their profiles. Users are motivated to save personal data on their fitness trackers, including their date of birth, weight, height, and gender, to ensure that the device's readings are as accurate as possible.[166] However, as demonstrated by the Strava incident,[167] knowledge of the ability to collect and divulge this information to users does not always correlate to said users understanding that their device can share this data more widely. Similarly, IoT consumers may be more inclined to claim a desire for privacy and yet exhibit contradictory actions, such as the purchase of IoT devices.[168] This so-called "Privacy Paradox" was attributed at least partially to a lack of awareness of IoT vulnerabilities and threats due to the devices' novelty and intricacy.[169] A 2014 whitepaper was one of the first to explore in depth the link between devices that can be used to track user whereabouts and intimate activities (through the correlation between heart-rate and physical exertion) in real time and the potential for stalking, profiling and extortion.[170]

Goulden *et al.* noted that pervasive monitoring by technologies built into homes forces the ongoing renegotiation of interpersonal relationships because inhabitants cannot avoid their data being collected and shared in a communal smart home.[171] Burdon and Cohen argued that smart homes result in

[161] Lopez J, Rios R, Bao F, et al. (2017) Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems* 75: 46–57. DOI: 10.1016/j.future.2017.04.045.
[162] Henze M, Hermerschmidt L, Kerpen D, et al. (2014) User-Driven Privacy Enforcement for Cloud-Based Services in the Internet of Things. In: *2014 International Conference on Future Internet of Things and Cloud*, August 2014, pp. 191–196. DOI: 10.1109/FiCloud.2014.38.
[163] Liu F and Li T (2018) A Clustering *K*-Anonymity Privacy-Preserving Method for Wearable IoT Devices. *Security and Communication Networks* Volume 2018. Security and Communication Networks: 8. DOI: https://doi.org/10.1155/2018/4945152.
[164] Xu W, Zhou H, Cheng N, et al. (2018) Internet of vehicles in big data era. *IEEE/CAA Journal of Automatica Sinica* 5(1): 19–35. DOI: 10.1109/JAS.2017.7510736.
[165] Powell A (2019) Chapter 7: The Mediations of Data. In: Hesmondhalgh D and Curran J (eds) *Media and Society*. 6th ed. London: Bloomsbury Publishing Inc., pp. 121–139. Available at: https://www.academia.edu/39303546/Media_and_Society_6th_edition (accessed 9 September 2019).
[166] Aktypi A, Nurse JRC and Goldsmith M (2017) Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In: *Proceedings of the 2017 on Multimedia Privacy and Security*, New York, NY, USA, 2017, pp. 1–11. MPS '17. ACM. DOI: 10.1145/3137616.3137617; Hill C (2015) Wearables – the future of biometric technology? Biometric Technology Today 2015(8): 5–9. DOI: 10.1016/S0969-4765(15)30138-7.
[167] @DFRLab (2018) Data and Defense: The Case of Strava. Available at: https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2 (accessed 9 August 2019).
[168] Williams M, Nurse J and Creese S (2017) 'Privacy is the Boring Bit': User Perceptions and Behaviour in the Internet-of-Things. In: *15th International Conference on Privacy, Security and Trust (PST)*, 28 August 2017. DOI: 10.1109/PST.2017.00029.
[169] Williams M, Nurse J and Creese S (2017) 'Privacy is the Boring Bit': User Perceptions and Behaviour in the Internet-of-Things. In: *15th International Conference on Privacy, Security and Trust (PST)*, 28 August 2017. DOI: 10.1109/PST.2017.00029.
[170] Barcena MB, Wueest C and Lau H (2014) *How safe is your quantified self?* Security Response, Whitepaper, 11 August. Symantec. Available at: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf.
[171] Goulden M, Tolmie P, Mortier R, et al. (2018) Living with interpersonal data: Observability and accountability in the age of pervasive ICT. New Media & Society 20(4). SAGE Publications: 1580–1599. DOI: 10.1177/1461444817700154.

modulation harms and therefore social shaping,[172] i.e. that digital pattern recognition can be used by commercial entities, to predict and shift user behaviours; this is particularly concerning for journalists, who have societal influence. Chapter 5's threat categorisation draws on this literature, specifically relating to the profiling and tracking categories.

These developments fuel the idea of "hybrid ownership"[173] – that these devices are not solely owned by the users, but also by the production companies and any organisations interacting with the data gathered by said devices. This results in a lack of active trust in the devices used, despite their ubiquity. Changes such as the implementation of the European Union (EU) General Data Protection Regulation (GDPR) are intended to strengthen privacy processes across the continent and set a global standard for data protection; however, a paper by Janeček revealed that there remain issues with legal definitions of personal data that would allow ownership of data collected by IoT devices to be contested.[174]

Further complicating ownership issues is a cultural trend that was spurred by the prevalence of personal devices and that shares many parallels between the threats posed to journalists and sources by the IoT: "Bring-Your-Own-Device" (BYOD). This refers to a corporate policy of allowing or encouraging employees to bring their personal devices to work and to use them to access company networks and information.[175] It is particularly relevant to journalists, as many of them rely on their own devices to conduct their work.[176] This expands the attack surface of news organisations, in comparison to endpoints that are supplied or managed by employers. Cox noted that IoT devices connected to enterprise Wi-Fi can be socially engineered or hacked for data exfiltration, Distributed Denial of Service attacks (DDoS) or ransomware dissemination at an organisation, but he does not acknowledge the dangers of IoT devices that collect information from an environment even while not connected to the network.[177] This is a problem regarding remote working scenarios in which employees use their home Wi-Fi networks to connect to work intranets, while using the same network to host IoT devices such as voice-activated assistants. These threats are further explored in Chapter 5 and countermeasures are suggested in Chapter 8.

In addition to data being shared beyond users' knowledge and control, the unobtrusive nature of IoT devices poses a challenge for users to even realise their data is being collected much less shared. For example, the capabilities of increasingly miniature and therefore near-invisible voice-activated home assistants made headlines for collecting user data without their consent. Users found that the device protocols were set to constantly capture sounds and that samples of user conversations were sent to the controlling companies for analysis in order to maximise performance, regardless of the implications for

[172] Burdon M and Cohen T (2021) Modulation Harms and The Google Home. Surveillance & Society 19(2): 154–167. DOI: 10.24908/ss.v19i2.14299.
[173] Keymolen E and Hof SV der (2019) Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. *Journal of Cyber Policy* 4(2): 143–159. DOI: 10.1080/23738871.2019.1586970.
[174] Janeček V (2018) Ownership of personal data in the Internet of Things. *Computer Law & Security Review* 34(5). Elsevier Ltd.: 1039–1052.
[175] National Cyber Security Centre (NCSC) (2016) BYOD: Executive Summary. Available at: https://www.ncsc.gov.uk/guidance/byod-executive-summary (accessed 17 February 2020); National Cyber Security Centre (NCSC) (2018) End user device (EUD) security guidance. Available at: https://www.ncsc.gov.uk/collection/end-user-device-security (accessed 17 February 2020); Morrow B (2012) BYOD security challenges: control and protect your most sensitive data. *Network Security* 2012(12): 5–8. DOI: 10.1016/S1353-4858(12)70111-3.
[176] Jokela T, Väätäjä H and Koponen T (2009) Mobile Journalist Toolkit: a field study on producing news articles with a mobile device. In: *Proceedings of the 13th International MindTrek Conference: Everyday Life in the Ubiquitous* Era, Tampere, Finland, 30 September 2009, pp. 45–52. MindTrek '09. Association for Computing Machinery. DOI: 10.1145/1621841.1621851.
[177] Cox G (2019) Managing the risks of shadow IoT. *Network Security* 2019(1): 14–17. DOI: 10.1016/S1353-4858(19)30010-8.

human privacy.[178] One notable example is that in the terms and conditions for a new smart television, Samsung mentioned that any information vocalised near the device, regardless of its sensitivity, would be recorded using voice recognition and sent to a third-party.[179]

Further, corporations are marketing IoT devices to law enforcement and civilian consumers simultaneously. One example is Amazon's 'Ring,'[180] an internet-connected doorbell and security camera that sends live footage of visitors to both the device owner and the local police. In some locations, police are able to access a map of all Ring devices installed in an area, which they can then use to request evidence from specific homeowners.[181] Any information accessed or copied by state processes, including search and seizure procedures, becomes more vulnerable to attackers.[182]

These are also clear instances of a threat to bystander privacy and therefore security, a recurring problem that Flammer argued originates because "bystanders are often considered a second-order phenomenon; in other words, 'human-centred design' really applies only to the user."[183] In their literature-based taxonomy of bystander privacy issues and solutions, Perez *et al.* described challenges to bystander privacy as scenarios in which "a device that collects sensor data (such as photos, sound, or video) can be used to identify third parties when they have not given consent to be part of the collection."[184] Their taxonomy identified seven challenges presented by the advent of ambient IoT devices that autonomously collect data: (1) facial recognition; (2) social implications and (3) social media sync (such as a lack of awareness of personal data collection, which may be immediately published online); (4) the constant fear of surveillance or sousveillance; (5) speech disclosure; (6) surreptitious audio-visual recording; and (7) location disclosure.[185]

Mass and targeted surveillance have been exacerbated by the rise in technologies and online forums that facilitate massive data collection, both due to the utility of open-source research[186] and the increased likelihood of data breaches.[187] State and corporate surveillance of journalists preceded the IoT's inception, but the prevalence of consumer IoT devices has increased the amount of personal data collated,

[178] Turow J (2021) Journalism and the Voice Intelligence Industry. Digital Journalism 9(7). Routledge: 1000–1006. DOI: 10.1080/21670811.2020.1829979; Cuthbertson A (2019) Google defends listening to private conversations on Google Home – but what intimate moments are recorded? The Independent, 12 July. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-home-recordings-listen-privacy-amazon-alexa-hack-a9002096.html (accessed 9 September 2019).
[179] Timm T (2016) The government just admitted it will use smart home devices for spying | Trevor Timm. The Guardian, 9 February. Available at: https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government (accessed 9 September 2019).
[180] Guariglia M (2019) Amazon's Ring Is a Perfect Storm of Privacy Threats. Available at: https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats (accessed 9 September 2019).
[181] Haskins C (2019) Amazon Told Police It Has Partnered With 200 Law Enforcement Agencies. In: Vice. Available at: https://www.vice.com/en_us/article/j5wyjy/amazon-told-police-it-has-partnered-with-200-law-enforcement-agencies (accessed 10 September 2019).
[182] CBP Public Affairs (2017) CBP Releases Statistics on Electronic Device Searches. Available at: https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0 (accessed 9 September 2019).
[183] Flammer I (2016) Genteel Wearables: Bystander-Centered Design. IEEE Security Privacy 14(5): 73–79. DOI: 10.1109/MSP.2016.91.
[184] Perez AJ, Zeadally S and Griffith S (2017) Bystanders' Privacy. IT Professional 19(3): 61–65. DOI: 10.1109/MITP.2017.42.
[185] Perez AJ, Zeadally S and Griffith S (2017) Bystanders' Privacy. IT Professional 19(3): 61–65. DOI: 10.1109/MITP.2017.42.
[186] Glassman M and Kang MJ (2012) Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior* 28(2): 673–682. DOI: 10.1016/j.chb.2011.11.014.
[187] De Groot J (2019) The History of Data Breaches. Available at: https://digitalguardian.com/blog/history-data-breaches (accessed 11 February 2020).

transferred, and stored. Documents leaked by Edward Snowden in 2013, regarding global surveillance coordinated by intelligence agencies, disclosed a reality in which there is increased likelihood of the compromise of source confidentiality.[188] The Snowden cache's disclosure that intelligence agencies engaged in mass surveillance and are therefore capable of de-anonymizing source communications facilitated a 'chilling effect' on sources,[189] preventing leaks to the press and self-censorship by writers.[190] Lashmar noted that this chilling effect is a well-documented effect of surveillance, which requires enhanced legal protections for journalists and their sources to avoid such a dilution of journalistic capabilities.[191]

There have already been accounts of democratic systems such as law enforcement and intelligence agencies using IoT data to solve crimes, such as by cross-referencing location data from criminals' fitness trackers with information on murders.[192] Specifically relevant to journalists, Lashmar and Di Salvo argue that surveillance of journalists is ever more pervasive and intrusive and is exacerbated by states outsourcing data collection to private companies.[193] In fact, Christensen *et al.* acknowledged the dangers of pattern recognition and the problems associated with devices' essential functions being reliant on opting into surveillance features,[194] which means that many such devices are unusable for journalists with something to hide; this is particularly relevant to the legal threats category in Chapter 5's threat categorisation.

However, there are many more reports of authoritarian regimes abusing IoT vulnerabilities to access and sometimes manipulate information. These include Russian state-sponsored group APT28's exploitation of default settings to hack corporate IoT devices,[195] an action that countries like the UK consider to be criminal. When discussing the consequences of smart homes in 2012, former CIA Director Petraeus claimed that the IoT's "effect on clandestine tradecraft" would be "transformational."[196] As discussed by Sanchez *et al.* even more secure IoT devices that use encrypted communication channels may be compromised and leak data if attacked using machine learning techniques.[197] Maple recognised that IoT processors are often small and low power, thereby forcing the devices to compromise on either

[188] Lashmar P (2017) No More Sources? *Journalism Practice* 11(6). Routledge: 665–688. DOI: 10.1080/17512786.2016.1179587.
[189] Lashmar P (2017) No More Sources? *Journalism Practice* 11(6). Routledge: 665–688. DOI: 10.1080/17512786.2016.1179587.
[190] PEN American Center (2013) *Chilling effects: NSA surveillance drives U.S. writers to self-censor*. 12 November. New York, NY, USA: PEN American Center and The FDR Group. Available at: https://pen.org//sites/default/files/Chilling%20Effects_PEN%20American.pdf (accessed 27 February 2020); Di Salvo P (2021) "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice* 0(0). Routledge: 1–18. DOI: 10.1080/17512786.2021.2014346.
[191] Lashmar P (2020) *Spies, Spin and the Fourth Estate: British Intelligence and the Media*. Edinburgh, Scotland: Edinburgh University Press.
[192] Missel R (2019) This Runner Is a Hitman. His GPS Watch Tied Him to a Mob Boss Murder. Available at: https://www.runnersworld.com/news/a25924256/mark-fellows-runner-hitman-murder/ (accessed 9 September 2019).
[193] Lashmar P (2020) Spies, Spin and the Fourth Estate: British Intelligence and the Media. Edinburgh, Scotland: Edinburgh University Press; Di Salvo P (2021) "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. Journalism Practice 0(0). Routledge: 1–18. DOI: 10.1080/17512786.2021.2014346.
[194] Christensen AT, Olesen H and Sørensen L (2021) On the Value of the Counterfactual and How the Smart Home Informs It. Surveillance & Society 19(2): 241–243. DOI: 10.24908/ss.v19i2.14301.
[195] Cimpanu C (2019) Microsoft: Russian state hackers are using IoT devices to breach enterprise networks. *ZDNet*, 5 August. Available at: https://www.zdnet.com/article/microsoft-russian-state-hackers-are-using-iot-devices-to-breach-enterprise-networks/ (accessed 9 September 2019).
[196] Ackerman S (2012) CIA Chief: We'll Spy on You Through Your Dishwasher. *Wired*, 15 March. Available at: https://www.wired.com/2012/03/petraeus-tv-remote/ (accessed 9 September 2019).
[197] Sanchez I, Satta R, Nai Fovino I, et al. (2014) Privacy leakages in Smart Home Wireless Technologies. In: *Proceedings - International Carnahan Conference on Security Technology*, 1 October 2014. DOI: 10.1109/CCST.2014.6986977.

performance or security in order to ensure that resource consumption is minimal, which impacts privacy features.[198]

These threats illustrate a major theme of this thesis: that it is so difficult to manage informational privacy in a surveillance capitalism age because every actor in the world wants to extract value in the form of data of various kinds. Every datum from a single device passes through a network of actors and services. This means that users, and bystanders who may have no idea that their data is being collected at all, can be affected by a breach of even one of those actors in the current regulatory system.

2.3.3 Privacy and Security by Design and Default

The financial incentive to design and release cheap internet-connected devices has resulted in an influx of resource-constrained IoT devices into the market. This results in large amounts of data being stored and transferred in plain text, thereby preventing users from controlling access to their data.[199] There are alternatives to this security-deficient approach to device design, from the concepts of Privacy and Security by Design and Default to that of privacy-enhancing technologies (PET), which are discussed in this subsection.

PET has roots in a perspective known as technological "Cornucopianism."[200] This is a viewpoint that is most often linked to climate change and environmentalist debates, claiming that technology and free market economies would make it possible for humankind to mitigate the effects of anthropogenic issues, such as climate change or, in this example, privacy infringements. Often, including privacy-enhancing features in IoT devices is referred to as "Privacy by Design" (PbD) or "Privacy by Default", i.e. the idea that potential privacy concerns must automatically be anticipated and negated through design requirements during the development phase instead of being retroactively addressed after such issues arise.[201] The principle of PbD was legitimised internationally at the 2010 International Conference of Data Protection Authorities and Privacy Commissioners, who recognised its significance in technology development by unanimously passing a Resolution on Privacy by Design.[202] This was reflected in the GDPR, which "requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights."[203]

Enshrining PbD in legislation was an important first step but, as an ENISA report stated: "the mere existence of concepts or implementations has been proven insufficient to extensively address the

---

[198] Maple C (2017) Security and privacy in the internet of things. *Journal of Cyber Policy* 2(2): 155–184. DOI: 10.1080/23738871.2017.1366536.

[199] Parra Rodriguez JD, Schreckling D and Posegga J (2016) Addressing Data-Centric Security Requirements for IoT-Based Systems. In: *2016 International Workshop on Secure Internet of Things (SIoT)*, September 2016, pp. 1–10. DOI: 10.1109/SIoT.2016.007; Hypponen M and Nyman L (2017) The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. *Technology Innovation Management Review* 7(4): 7.

[200] Ayres RU (1993) Cowboys, cornucopians and long-run sustainability. *Ecological Economics* 8(3): 189–207. DOI: 10.1016/0921-8009(93)90058-E.

[201] Cavoukian A (2010) *Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. May. Toronto, Ontario, Canada: Information and Privacy Commissioner of Ontario. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf.

[202] Data Protection and Privacy Commissioners (2010) Resolution on Privacy by Design. In: *32nd International Conference of Data Protection and Privacy Commissioners*, Jerusalem, Israel, 27 October 2010, p. 2. Available at: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

[203] Information Commissioner's Office (2019) Data protection by design and default. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (accessed 19 February 2020).

challenge of supporting the individual's right to privacy; privacy cannot be guaranteed by just technology, let alone by a few PET components embedded in a bigger ICT system."[204] In support of this notion, some researchers have turned to technology as a mechanism for shifting human understanding, expectations and norms regarding technologies that typically threaten privacy. This concept is demonstrated by the "Aretha" project: an example of privacy-enhancing IoT with an interface that is accessible enough to empower users to understand and actively protect their own privacy.[205] This builds on the functionality of a commercial voice assistant to make it a user-friendly first line of smart home defence by incorporating firewall capabilities with the voice-activated interface.[206]

Long before the IoT became prevalent, Barth *et al*. designed a "framework for contextual integrity" that marries expectations of privacy with situationally realistic practices.[207] Their framework provides a foundational basis for understanding the privacy threats from collection, storage and transfer of individuals' personal data, but does not present a way of mitigating these threats when they are presented on the scale of the IoT today.[208] Further, Hoepman examined existing data protection legislation to derive eight clear PbD principles that have since been enshrined in international regulations, such as the GDPR, but are not IoT-specific.[209] These examples are relevant to this thesis because, as Chapter 8's framework intends to demonstrate, IoT threats must be combated by centring users and bystanders on multiple levels: technology design, policy responses and legislative shifts, and operational protections for individuals, organisations and communities.

Where the cyber-physical IoT is concerned, PbD may be considered synonymous with "Security by Design" (SbD). For example, a survey of literature of IoT security and privacy issues authored by Yang *et al*. concludes that security should be a fundamental design feature.[210] Similarly, Alladi *et al*.'s article detailed some of the common cyber-attacks on consumer IoT devices: matching them with the relevant device vulnerabilities and recommending potential countermeasures, in order that better SbD be applied.[211] The article was aimed at IoT developers and manufacturers, rather than consumers, as the language used to annotate diagrams is not accessible to lay readers. Chapter 8's framework of countermeasures is likewise intended to provide countermeasures that address the IoT threats raised in Chapter 5's IoT threat categorisation, including those that result from regulatory gaps.

---

[204] European Union Agency For Network and Information Security (ENISA) (2014) *Privacy and Data Protection by Design - from policy to engineering*. Report/Study, December. Athens, Greece: European Union Agency For Network and Information Security (ENISA). Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (accessed 19 February 2020).

[205] Seymour W (2019) Privacy Therapy with Aretha: What If Your Firewall Could Talk? In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow, Scotland Uk, 2 May 2019, pp. 1–6. CHI EA '19. Association for Computing Machinery. DOI: 10.1145/3290607.3308449.

[206] Seymour W (2019) Privacy Therapy with Aretha: What If Your Firewall Could Talk? In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow, Scotland Uk, 2 May 2019, pp. 1–6. CHI EA '19. Association for Computing Machinery. DOI: 10.1145/3290607.3308449.

[207] Barth A, Datta A, Mitchell JC, Nissenbaum H (2006) Privacy and contextual integrity: Framework and applications. In: *Proceedings - 2006 IEEE Symposium on Security and Privacy, S+P 2006*, 2006, pp. 184–198. DOI: 10.1109/SP.2006.32.

[208] Barth A, Datta A, Mitchell JC, Nissenbaum H (2006) Privacy and contextual integrity: Framework and applications. In: *Proceedings - 2006 IEEE Symposium on Security and Privacy, S+P 2006*, 2006, pp. 184–198. DOI: 10.1109/SP.2006.32.

[209] Hoepman J-H (2014) Privacy Design Strategies. In: *ICT Systems Security and Privacy Protection* (eds N Cuppens-Boulahia, F Cuppens, S Jajodia, et al.), Berlin, Heidelberg, 2014, pp. 446–459. IFIP Advances in Information and Communication Technology. Springer. DOI: 10.1007/978-3-642-55415-5_38.

[210] Yang Y, Wu L, Yin G, Li L, Zhao H. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet Things J. 2017 Oct;4(5): p. 1252.

[211] Alladi T, Chamola V, Sikdar B, Choo K-KR. Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consum Electron Mag. 2020 Mar;9(2): pp. 17-25.

In recognition of the vital role that the IoT plays in essential services such as healthcare, Malina *et al*. proposed a framework of PbD and SbD strategies for the IoT, grouping privacy issues in the IoT into three classes: "threats" ("weaknesses and flaws of IoT services and systems that could be misused by other system entities"), "leakages" ("more serious problems and flaws that can directly breach user privacy"), and "attacks" ("intentionally performed by passive and active attackers in order to break user privacy and misuse the observed information for criminal activities").[212] All of these classes are relevant to the threats categorisation in Chapter 5. For example, IoT-compromise by state-affiliated agencies for surveillance of journalists or reconnaissance on stories that are about to break may not be "criminal," but is still an "attack."

The necessity of PbD in the IoT is supported by Porambage *et al*.'s paper, which discussed IoT PbD as vital, given that "available PETs for underlying IoT technologies aren't directly compatible with the IoT's heterogeneous characteristics."[213] Per Li *et al.,* it is crucial that any analysis of privacy and the IoT comprehensively includes the principles inherent in relevant legislation that covers both regulation of PET design and use in the IoT.[214] Some literature, such as by Koops and Leenes, evaluated the extent to which PbD can be both encoded into technology and embedded in data protection legislation. These papers determined that the fluid nature of legal norms is at odds with PETs and thus recommended that developers internalise these norms regularly, to ensure that there is a practical mix of technological and organisational privacy strategies involved in implementation.[215] Chapter 7 further explores regulatory gaps around IoT manufacture and development in the US, the UK, Australia, and Taiwan, Chapter 8's framework suggests legislative changes for the media sector to lobby for, and Chapter 9 explores this thesis' potential policy contributions.

2.3.4 The relevance of surveillance studies to this thesis

This section explores the way in which surveillance studies perspectives inform and link cyber security and journalism studies concerns, to create an interdisciplinary contribution that enhances all three fields. Surveillance studies combines elements of various fields, including law, sociology, politics and, increasingly, cyber security. These are all features that influence this thesis, separately and together.

As a core IoT threat is continual surveillance, this thesis was underpinned and motivated by theoretical frameworks from the three phases of surveillance theory explored by Galič *et al.*[216] within the field of surveillance studies. These phases, as discussed below, are: (1) centralised state-run panopticism, (2) surveillance networks that include non-state actors such as commercial entities, and (3) continuous surveillance of many kinds, by many actors. Supporting the pertinence of all of these elements of

[212] Malina L, Srivastava G, Dzurenda P, et al. (2019) A Privacy-Enhancing Framework for Internet of Things Services. In: *Network and System Security* (eds JK Liu and X Huang), Cham, 2019, pp. 77–97. Lecture Notes in Computer Science. Springer International Publishing. DOI: 10.1007/978-3-030-36938-5_5.

[213] Porambage P, Ylianttila M, Schmitt C, et al. (2016) The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing* 3(2): 36–45. DOI: 10.1109/MCC.2016.28.

[214] Li C and Palanisamy B (2019) Privacy in Internet of Things: From Principles to Technologies. *IEEE Internet of Things Journal* 6(1): 488–505. DOI: 10.1109/JIOT.2018.2864168.

[215] Koops B-J and Leenes R (2014) Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology* 28(2): 159–171. DOI: 10.1080/13600869.2013.801589.

[216] Galič M, Timan T and Koops B-J (2017) Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology* 30(1): 9–37. DOI: 10.1007/s13347-016-0219-1.

surveillance theory to this research is the exploratory study's finding (see: Chapter 4) that journalists are aware that the IoT is omnipresent and watching,[217] thereby effectively chilling reporting.

Specifically, the first phase, Bentham and Foucault's ideas of centralised and architectural panopticism, relate to this research because of the consistent threat of state overreach into journalists' affairs through IoT devices.[218] The second phase, per Haggerty and Ericson, directly accounts for a "surveillance assemblage" of ubiquitous networked devices that exponentially increase the capacity for surveillance by actors beyond the state.[219] Also characterised as part of the second phase of surveillance theory is Zuboff's theory of "surveillance capitalism."[220] Burgess and Hurcombe noted that concentration of proprietary power in the hands of certain technology companies, and particularly social media platforms, has undermined journalists' capabilities "to use these kinds of digital methods for the purposes of public oversight of the digital media environment." [221]

This is of course applicable to the IoT which, as demonstrated by Chapter 5's models, can be found in various physical environments and attacked in various ways to extract data at any point. The framework presented in Chapter 8 addresses the concerns raised by these phases of scholarship, including countermeasures that aim to mitigate both targeted and ambient surveillance, regardless of the perpetrators. This is likewise demonstrated in Chapters 6 and 7, as interviewees expressed anxiety about convoluted supply chains and the lack of regulation of the technology sector. It is particularly difficult to manage privacy and security in a surveillance capitalist age given these entangled supply and maintenance chains, as there are a myriad of actors whose goal is to extract value from data subjects via a single IoT device. This means that the odds of a data breach at some point in the chain are increased and could be devastating for a journalist. It is therefore clear that control held by such corporations, as by IoT manufacturers, is detrimental to the ability of the free press to hold them accountable for any lapses in judgement or execution. Countermeasures C (transparency reporting) and I (collaborative technology design) presented in Chapter 8 are particularly designed to try to combat the corporate hegemony in this regard.

The third phase, which Galič *et al.* framed as reviewing mass surveillance by states, corporations, individuals, all separately and together, includes Clarke's "dataveillance" and Mann's "sousveillance."[222] These ideas illustrate that IoT risk, particularly from data collection, is everywhere, all the time, and by all actors, and inspire this thesis's toolkit for managing that risk, as it cannot be eradicated. Kazansky and Milan noted that civil society subverts the typical construct of surveillance producers and victims by

[217] Lyon D (2018) *The Culture of Surveillance: Watching as a Way of Life*. 1st ed. Cambridge, UK: Polity Press. Available at: https://www.wiley.com/en-us/The+Culture+of+Surveillance%3A+Watching+as+a+Way+of+Life-p-9780745671734 (accessed 28 May 2019).

[218] Bentham J (2012) The Works of Jeremy Bentham, Vol. 4 (ed. J Bowring). RareBooksClub.com; Foucault M (1977) *DISCIPLINE AND PUNISH: The Birth of the Prison*. New York: Knopf Doubleday Publishing Group.

[219] D. Haggerty, Richard V. Ericson K (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605–622. DOI: 10.1080/00071310020015280.

[220] Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books Ltd.

[221] Burgess J and Hurcombe E (2019) Digital Journalism as Symptom, Response, and Agent of Change in the Platformed Media Environment. *Digital Journalism* 7(3). Routledge: 359–367. DOI: 10.1080/21670811.2018.1556313.

[222] Galič M, Timan T and Koops B-J (2017) Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology* 30(1): 9–37. DOI: 10.1007/s13347-016-0219-1; Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512. DOI: 10.1145/42411.42413; Mann S (2016) Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself). In: *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Toronto, Ontario, Canada, June 2016, pp. 1408–1417. IEEE Computer Society. DOI: 10.1109/CVPRW.2016.177.

attempting to expose the dangers and absurdity of such data collection, but that they can only do so in limited ways.[223] This is the gap Chapter 5's threat categorisation seeks to fill.

2.4 How do states regulate the IoT?

As specified in Chapter 1, this research focuses on four democratic countries. As such, this section explores some of ways in which democratic governments have approached regulating the IoT. It does so by providing some context for topics that are revisited in Chapters 6 and 7.

Regarding academic literature on "IoT regulation," there is a clear distinction between where different kinds of papers on this topic were published. Discussions of the legal and political challenges and responsibilities were almost exclusively found in social science journals, while journals on engineering and physical sciences focused on technical efforts to improve IoT security and privacy without necessarily acknowledging existing legislation. This is a finding by Veale *et al.*, who wrote that "PbD, and the [Data Protection by Design] now mandated by law, is seen increasingly as a synonym for the formal privacy enhancing technologies literature that take reducing unwanted information disclosure as their sole goal," and advocated for more holistic perspectives on data protection principles.[224]

Aside from academic literature, there were ample whitepapers written by corporate entities, such as vendors, and political organisations on the need for new regulatory standards. Some of these focused on the idea of IoT Security by Design, such as Australian "cyber agencies and industrial groups" in 2018, who discussed designing much-needed IoT security controls without "constituting a coordinated strategy detailing how government and industry can collaborate on the IoT."[225] Another example is that of UK laws proposed in 2020, which evolved from a 2014 government report that advocated for anticipatory regulation of emerging IoT technologies but recognised that there already exists substantial legislation on Big Data collection.[226] Additionally, Rustad noted that the GDPR's "expansive extraterritorial effect" meant that it applies to IoT manufacturers outside the EU, provided that sales still occur to users within the affected countries. Rustad concluded that operationalising the GDPR's requirement of IoT PbD will be a challenge for manufacturers but that "the largest challenge" is "to safeguard the data they process, and to detect espionage and stave off cyberattacks [sic]."[227] This is a particularly relevant issue for journalists who may not be able to avoid interaction with the IoT but must nonetheless maintain source confidentiality and the integrity of their work.

---

[223] Kazansky B and Milan S (2021) "Bodies not templates": Contesting dominant algorithmic imaginaries. *New Media & Society* 23(2). SAGE Publications: 363–381. DOI: 10.1177/1461444820929316.

[224] Veale M, Binns RDP and Ausloos J (2018) When data protection by design and data subject rights clash. *International Data Privacy Law* 8(2). Oxford University Press: 105–123.

[225] Chapman E and Uren T (2018) The *Internet of Insecure Things*. #ICPCIoT, 19 March. Canberra, Australia: Australian Strategic Policy Institute. Available at: https://www.aspi.org.au/report/InternetOfInsecureThings (accessed 26 February 2020).

[226] Department for Digital, Culture, Media & Sport (2020) Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation. Available at: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation (accessed 28 January 2020); UK Government Office for Science (2014) The Internet of Things: making the most of the Second Digital Revolution - A report by the UK Government Chief Scientific Adviser. Research and analysis: Internet of things: Blackett review GS/14/1230, 18 December. London, UK: Government Office for Science. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf: 9.

[227] Rustad ML (2019) How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices. *Suffolk University Law Review* 52(2): 227–272.

Walker *et al.* surveyed the current state of both "hard" and "soft" laws that could be applicable to the IoT across several EU and US jurisdictions and noted a lack of "international coherence in IoT security policy."[228] This may result from varying degrees of input from the myriad of stakeholders, though they also found that there appeared to be cultural differences in terms of decision-makers' policy approaches to the IoT. They argue that policymakers in the US favoured solutions derived through consultation with industry while those in Europe instead chose to develop regulatory principles and guidelines to be subsequently imposed on industry. This is evidence that democratic governments do not share a common policy perspective regarding legislation of emerging technologies, like the IoT. Rather, there are some states that prefer to control the legislative process and others that grant the free market more power in determining regulatory controls.

In the US, Quirk noted that consumer IoT devices are largely the same electronics that have long been governed by the US Federal Communications Commission (FCC), just with added wireless modules.[229] While this means that manufacturers, importers, and vendors must abide by ordained standards, practices, and procedures regarding quality, Quirk did not mention regulations regarding heightening device security. On this, Weber argued that a centralised regulatory body would be inappropriate in the US. However, Weber felt that there was a need for collaboration between state-affiliated entities for "democratic legitimacy," private sector and civil society partners to ensure that the IoT is both secure and confidential.[230]

Urquhart *et al.* stated that an aspect of regulation is accountability, so that parties involved in developing and creating multiple features of IoT devices (from potentially non-consensual data collection to inadequate user interfaces) are responsible for IoT performance to secure user trust.[231] Tusikov's book chapter recognised an oft overlooked facet of the regulatory discussion: ownership of devices.[232] Its relevance is that the companies that develop and copyright proprietary IoT technologies, particularly software, retain a disproportionate amount of "post-purchase control" over devices through contractually agreed surveillance and user data collection capabilities. According to Mulligan, the rise of the IoT facilitated a shift in the contractual and licensing language used by these companies, from referring to customers as device "owners" to calling them "users." Such choices provided the companies "downstream control" that is only legal because the devices contain chips rather than gears.[233] This indicated a lack of comprehension on the part of legislators and policymakers regarding digital devices and the contemporary manufacturer-customer relationship.

---

[228] Walker M, Shockey K, Neiman A, et al. (2018) Awakening Global Governments: An International Survey of Internet of Things Regulation. In: *TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018*, Rochester, NY, 16 March 2018. Social Science Research Network. Available at: https://papers.ssrn.com/abstract=3142105 (accessed 25 February 2020).

[229] Quirk RE (2017) Are Your Company's Consumer Electronics Exempt from FCC Marketing Regulations? [Future Directions]. *IEEE Consumer Electronics Magazine* 6(2): 22–26. DOI: 10.1109/MCE.2016.2640578; Kamalipour YR (ed.) (2019) *Global Communication: A Multicultural Perspective*. 3rd edition. Rowman & Littlefield Publishers: xi.

[230] Weber RH (2009) Internet of things – Need for a new legal environment? *Computer Law & Security Review* 25(6): 522–527. DOI: 10.1016/j.clsr.2009.09.002.

[231] Urquhart L, Lodge T and Crabtree A (2019) Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology* 27(1). Oxford Academic: 1–27. DOI: 10.1093/ijlit/eay015.

[232] Tusikov N (2019) Precarious Ownership of the Internet of Things in the Age of Data. In: Haggart B, Henne K, and Tusikov N (eds) Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century. International Political Economy Series. Cham: Springer International Publishing, pp. 121–148. DOI: 10.1007/978-3-030-14540-8_6.

[233] Mulligan C (2015) Personal Property Servitudes on the Internet of Things. Georgia Law Review 50(4): 1121–1168.

2.5 What is the current state of literature on IoT threats to the free press?

When creating a resource to improve journalistic security (see: Chapter 8), the current state of cyber security protection resources aimed at and used by the media community must be assessed. Although even recent research has considered information security relating to journalists to be "nascent,"[234] there are a range of relevant sources. However, some of the documents reviewed in this section are ambiguous about which devices they cover, others mainly pertain to digital hygiene fundamentals regarding legacy devices (i.e. phones, laptops, tablets) and secure communications (and thus cover the source-interaction element of an editorial workflow). This thesis builds on the guidance offered by this existing literature, while attempting to fill gaps specific to the IoT.

Therefore, this section assesses how these materials consider the IoT, and what countermeasures they present, irrespective of their technological focus, to ensure that the framework is tailored to the needs of journalists. This section also considers literature relating to IoT cyber protections that do not address threats to journalists, to see how these might be adapted and integrated into this thesis's portfolio of tools for assessing and managing risk (see: Chapters 5 and 8). The following subsections open with materials that discuss journalists' cyber security protections but do not mention the IoT, and then discuss materials that discuss IoT protections but do not mention journalists.

2.5.1 Existing cyber security guidance for journalists

The literature discussed in this subsection largely covers the fundamental digital hygiene basics, and is frequently referenced by sites and papers relating to journalist safety and security. When it comes to IoT devices specifically, some articles on this topic acknowledge IoT threats. However, there are no industry guidelines for instructing journalists on how to minimise their attack surface or mitigate the threats from the IoT.[235]

Prior to the exploratory study (see: Chapter 4), which focuses on journalists' perceptions of threats to their work and wellbeing through IoT devices, similar studies had been conducted into journalists' understanding of technological threats and risk. For example, McGregor and Watkins' study on "Journalists' Mental Models of Information Security" found that participants largely relied on a mental model of information security that allowed them to operate with minimal consideration for security precautions (deemed "security by obscurity"), "unless one is involved in work that is sensitive enough to attract the attention of government actors." [236] In their study, "sensitivity" was discussed as being highly subjective, with participants deciding whether or not their work qualified as high-risk through ad hoc estimations of the offence caused to and capabilities of the subjects of each piece. Even technology journalists find it quite difficult to maintain an awareness of their growing attack surface despite their relevant subject matter expertise. A 2019 *New York Times* article discussing the implications of "tech

[234] Di Salvo P (2022) Information security and journalism: Mapping a nascent research field. Sociology Compass 16(3). John Wiley & Sons, Ltd: e12961. DOI: 10.1111/soc4.12961.

[235] List of examples can be found at http://iotlineup.com/, https://internetofthingswiki.com/iot-devices/, and https://www.datamation.com/mobile-wireless/75-top-iot-devices-1.html

[236] McGregor SE and Watkins EA (2016) "Security by Obscurity": Journalists' Mental Models of Information Security. #ISOJ 6(1). The Multimedia Edition of the Official Research Journal of the International Symposium on Online Journalism. Available at: https://isojjournal.wordpress.com/2016/04/14/security-by-obscurity-journalists-mental-models-of-information-security/ (accessed 15 February 2020).

tools" used by a technology and media journalist did not mention IoT devices at all, but instead solely focused on smartphone applications and the consequences of targeted advertising.[237]

Focusing heavily on journalistic security related to high-risk collaborations, McGregor *et al.* reviewed the security-enhancing tools developed for and used during the Panama Papers process.[238] They found that 83% of participants considered these tools "essential" to the actual journalistic work they were doing, which is why uptake was good. For this reason, the framework in Chapter 8 of this thesis is structured to be included as part of different stages of a journalistic workflow. Although McGregor *et al.* did not mention the IoT, this journalistic investigation culminated in 2016 and the paper was published in 2017, so there is a chance that the IoT was not as widespread or relevant during these publication processes. Based on the findings of this literature review, Chapter 5's threat categories and threat titles are followed by hypotheticals that describe possible consequences of such threats for the press.

This complexity that is likely to be industry-specific therefore validates the finding of McGregor *et al.* that "journalistic organizations have unique characteristics that affect their computer privacy and security risks and outcomes." [239] This includes layered and diverse requirements for technological interaction by various stakeholders, thereby making them worthy of specific study. Further, the framing and linguistic choices for this thesis's toolkit, particularly Chapters 5 and 8, are influenced by Watkins' *et al.*'s study of the conflict between news organisational bureaucracy and the need to adapt journalists' cyber security practices to their contexts through communal security discussions and processes.[240]

Oliver's survey of journalism schools noted that one-off trainings were counterproductive; they imparted little long-term knowledge or support and could even cause vulnerabilities because of incomplete protective tool installations.[241] More successful is the increasing trend of habit-building by incorporating cyber security and risk assessments into existing courses and best practice - although Oliver noted that many staff are unprepared to teach on security of this kind. This article did not mention IoT training or awareness, but said that one participant recommended that journalists try not to control their own security alone, or use specific dictated tools. Rather, they recommended "seek[ing] out the technical knowledge and expert support they need to protect their professional practice—much like a journalist might call in a lawyer when legal issues arise."

Crete-Nishihata *et al.* reviewed both the individual and organisational elements of journalistic security culture, relating to beat and employment status.[242] They recommended ways in which newsrooms can effectively train their staff, and freelancers can be taught by their peers about basic information security

[237] Herrman J (2019) The Tools for Covering Tech Are the Same as in 2009. The New York Times, 31 July. Available at: https://www.nytimes.com/2019/07/31/technology/personaltech/tools-covering-tech-same-2009.html (accessed 9 September 2019).
[238] McGregor SE, Watkins EA, Al-Ameen MN, et al. (2017) When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. In: Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 16 August 2017, p. 19. USENIX Association. Available at: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-mcgregor.pdf.
[239] McGregor S, Roesner F and Caine K (2016) Individual versus Organizational Computer Security and Privacy Concerns in Journalism. Proceedings on Privacy Enhancing Technologies 2016. DOI: 10.1515/popets-2016-0048.
[240] Watkins EA, Al-Ameen MN, Roesner F, et al. (2017) Creative and Set in Their Ways: Challenges of Security Sensemaking in Newsrooms. In: Proceedings of Free and Open Communications on the Internet (FOCI) 2017 Workshop, USENiX, Vancouver, BC, Canada, August 2017, p. 11. USENIX Association. Available at: https://www.usenix.org/conference/foci17/workshop-program/presentation/watkins.
[241] Oliver J (2018) Journalism schools still behind on cybersecurity training, new survey finds. Available at: https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php (accessed 15 November 2020).
[242] Crete-Nishihata M, Oliver J, Parsons C, et al. (2020) The Information Security Cultures of Journalism. Digital Journalism 0(0). Routledge: 1–24. DOI: 10.1080/21670811.2020.1777882.

perceptions and practices. This is due to the influence that professional organisations have on journalists and the need to raise awareness of the impact of threats on the wider community, not just one single journalist. The focus on institutional recommendations is key for the "category of media roles that is most likely to be responsible for implementation of this countermeasure" column of Chapter 8's framework.

Although it is true that there is a rising number of freelance journalists, a recurrent suggestion from participants in the exploratory study (see: Chapter 4) is that news organisations should be held responsible for educating journalists about IoT threats. This echoes findings in the BYOD literature relating to the wealth of personal data held on the devices that are intermittently connected to the corporate enterprise private network, increasing the risk to both the personal and professional information.[243] Morrow argued for organisations to employ layered security strategies that continue from the design phase through to service delivery, including compartmentalising data to limit access, logging and auditing who has access to data, and controlling capabilities allowing the manipulation of data.[244] This strategy is likely to be effective for many IoT devices but, to Cox, overlooks devices that can collect ambient data such as audio-visual recordings, temporarily storing them and only transferring them when they are once again connected to the internet.[245]

Some of the threats in Chapter 5's categorisation are informed by academic articles in the journalism studies space that are beginning to raise awareness of the issues of IoT threats. For example, Turow recognised the long-term dangers of voice-enabled devices enabling companies to extrapolate user emotions and biometrics for profiling. Turow's piece argued that journalists do not cover voice assistants as critically as their dangers merit, and his research found that journalism about voice devices treats them as though IoT data collection is inevitable. However, he did not address the particular risk of IoT threats to the media, evidencing the need for a media-targeted resource to highlight IoT threats.[246] Conversely, Berger's article on the future of the press does explicitly consider the double-edged sword of massive data collection and how it may be exploited by actors who seek to harm the news industry. Still, even Berger's article only briefly mentioned that the media's infatuation with technology and Big Data could be accompanied by risks such as surveillance, hacking, harassment, and pressure on journalists to churn out sensationalist stories that erode the credibility of the press. Berger concluded that "this paradox is far from resolution."[247]

Similarly, McGregor's book focused on information security for journalists, and while the IoT was not explicitly mentioned, it did note that newer devices are designed to blend into the environment and recommended keeping a "device diary" (i.e. noting all the devices a journalist uses).[248] These points are useful reminders and tactics for increasing a reporter's awareness of and ability to manage IoT risk, and they highlighted the need for Chapter 5's IoT device model. The examples given in the works of Turow, Berger, and McGregor demonstrated the need for an in-depth review of the ways in which a range of IoT devices and capabilities can threaten journalistic freedom and security (see: Chapter 5), with subsequent

[243] Miller KW, Voas J and Hurlburt GF (2012) BYOD: Security and Privacy Considerations. IT Professional 14(5): 53–55. DOI: 10.1109/MITP.2012.93; Cox G (2019) Managing the risks of shadow IoT. Network Security 2019(1): 14–17. DOI: 10.1016/S1353-4858(19)30010-8.
[244] Morrow B (2012) BYOD security challenges: control and protect your most sensitive data. Network Security 2012(12): 5–8. DOI: 10.1016/S1353-4858(12)70111-3.
[245] Cox G (2019) Managing the risks of shadow IoT. Network Security 2019(1): 14–17. DOI: 10.1016/S1353-4858(19)30010-8.
[246] Turow J (2021) Journalism and the Voice Intelligence Industry. *Digital Journalism* 9(7). Routledge: 1000–1006. DOI: 10.1080/21670811.2020.1829979.
[247] Berger G (2018) Is There a Future for Journalism? *Journalism Practice* 12(8). Routledge: 939–953. DOI: 10.1080/17512786.2018.1516117.
[248] McGregor SE (2021) *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.

clear action points to enable the press to begin to mitigate and protect against such threats (see: Chapter 8).

Further, Access Now's "A First Look At Digital Security" informed some of the content of the framework, particularly the "beneficiaries of countermeasures" column. It reminded readers of the imperative of protecting sources, communications with editors and collaborators, drafts and research, online accounts, and time-sensitive research. However, this guidance only explicitly mentioned laptops, desktop computers and phones, ignoring relatively new smart devices such as internet-connected watches that are voice-enabled and could potentially be hacked to record audio of meetings.[249]

As noted by both Di Salvo and Henrichsen, academic literature looking at journalistic cyber security is emerging, and much of it emphasises the barriers to uptake of existing advice and tools.[250] This affects the ways in which the toolkit in this thesis is constructed to overcome these hurdles. Another key influence on Chapter 8's toolkit is Pierce *et al*.'s paper on cyber security toolkits,[251] which evaluated many of the resources used by journalists, including those created by the Electronic Frontier Foundation. Pierce *et al.* noted that many of the resources they reviewed did not adequately distinguish between individual, organisational and collective recommendations, an issue that the structure of the framework in this thesis attempts to address.

McGregor *et al.* provided a comprehensive overview of preceding academic work regarding the impediments and incentives to journalists' computer security needs and practices, noting that there are three major issues that tend to hinder effective implementation of security practices for journalists: First, choosing communication channels based on sources' preferences rather than matching them to the level of sensitivity of the information. Second, the existing options for technical tools do not take into account the needs of the journalistic workflow and so uptake is low. Third, available guidance does not acknowledge the importance of the security of other actors within the media ecosystem.[252] The exploratory study (see: Chapter 4) intends to address some of the limitations of McGregor *et al*.'s study, such as the fact that it only surveyed French and American journalists, and that it did not consider emerging technologies such as new IoT devices. Further, the structure of the framework (see: Chapter 8) takes these obstacles into account.

Other materials are particularly relevant to Chapter 8's framework. For example, Global Cyber Alliance (GCA) has created both a "Cybersecurity Toolkit for Journalists" and a forum for discussion of cyber-threats to journalists.[253] The former, which covered traditional threats but not the IoT, demonstrated how toolkits can be usefully designed for targeted at journalists, and informed the toolkit in this thesis, which

[249] Access Now (2018) A first look at digital security digital as of March 2018. March. Access Now. Available at: https://www.accessnow.org/cms/assets/uploads/2018/03/A-first-look-at-digital-security-digital-copy.pdf (accessed 9 September 2019).

[250] Henrichsen JR (2021) Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice* 0(0). Routledge: 1–20. DOI: 10.1080/17512786.2021.1927802; Di Salvo P (2021) "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice* 0(0). Routledge: 1–18. DOI: 10.1080/17512786.2021.2014346.

[251] Pierce J, Fox S, Merrill N, et al. (2018) Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. Proceedings of the ACM on Human-Computer Interaction 2(CSCW): 139:1-139:24. DOI: 10.1145/3274408.

[252] McGregor SE, Charters P, Holliday T, et al. (2015) Investigating the Computer Security Practices and Needs of Journalists. In: Proceedings of the 24th USENIX Security Symposium, Washington, D.C., 12 August 2015, p. 17. USENIX Association.

[253] Global Cyber Alliance (2020) Global Cyber Alliance Provides Cybersecurity Toolkit for Journalists. In: *GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk*. Available at: https://www.globalcyberalliance.org/global-cyber-alliance-provides-cybersecurity-toolkit-for-journalists/ (accessed 26 September 2022).

intends to raise awareness of the IoT so that it may be included in risk assessment and management protocols for members of the media. The latter GCA resource was a sign of the utility of and need for threat intelligence sharing platforms within the media, as acknowledged by countermeasure N in Chapter 8's framework. Further, it is in response to threats to journalistic confidentiality that "UNESCO and Reporters Without Borders 'Safety Guide for Journalists'' explicitly warned its readership that "a smartphone can be treacherous." Published in 2015, this guide included a chapter on procedural protocols to be taken to limit the potential attack surfaces of a phone and a laptop, without mentioning other connected devices. The protections suggested were aimed at individual journalists and included being wary of downloads and untrusted Wi-Fi networks and compartmentalising digital activities to protect sensitive data;[254] both considerations that are relevant to the IoT and Chapter 8's countermeasures framework.

Some of this literature demonstrated the need for the threat categorisation as a risk assessment tool. For example, the Electronic Frontier Foundation's "Surveillance Self-Defense" guide explicitly discussed threat models, which helps to define the need for the threat categorisation (see: Chapter 5).[255] Likewise, the Rory Peck Trust created an online risk assessment for journalists to use before they go on an assignment, to establish their threat model. However, neither of these resources, nor their links to further advice, mentioned IoT devices.[256] GJS's "Digital Safety Curriculum for Newsrooms" included "levels" of risk, adapting different intensities of risk assessment and management training for each level that build on each other, from Level 1 (Practicing Digital Hygiene) to Level 7 (Digital Counter Surveillance and Data Gathering).[257] Other than Level 7's teaching on how to use a drone for reporting, none of the levels in the syllabus discussed the IoT, but each level had a target audience (akin to the "beneficiaries" column of Chapter 8's framework) and clear objectives (i.e. protections) that ranged from building a threat model to authenticating a hack.

Several of the materials in this space, and Rader *et al.*'s research into using stories to communicate security information,[258] directly influence the narrative format of the "hypothetical consequences" feature of the threats categorisation (see: Chapter 5). For example, the way that "UNESCO and Reporters Without Borders 'Safety Guide for Journalists'" included digital security alongside physical and emotional security considerations provides a basis for the holistic nature of this research.[259] Further, Access Now's "A First Look At Digital Security" offered advice in small story-like chunks.[260] The Digital Defenders Partnership's "Digital First Aid Kit" also gave mitigation advice for once an attack is suspected. It linked to a series of other recommended resources and actors in case the person searching for advice is left

[254] UNESCO and Reporters without borders (2015) SAFETY GUIDE FOR JOURNALISTS: A handbook for reporters in high-risk environments. Reporters without borders. Available at: https://rsf.org/sites/default/files/guide_journaliste_rsf_2015_en_0.pdf (accessed 9 September 2019).
[255] Electronic Frontier Foundation (2019) Surveillance Self-Defense: Tips, Tools and How-Tos for Safer Online Communications. Available at: https://ssd.eff.org/en (accessed 11 September 2020).
[256] Rory Peck Trust (2019) Digital Risk Assessment. Available at: https://rorypecktrust.org/resources/Digital-Security-Guide/Digital-Risk-Assessment?cu=en-GB (accessed 9 September 2019).
[257] GJS (2019) Digital Safety Curriculum for Newsrooms. Available at: https://www.gjs-security.com/digital-safety-curriculum-for-newsrooms/ (accessed 9 September 2019).
[258] Rader E, Wash R and Brooks B (2012) Stories as informal lessons about security. In: Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12, Washington, D.C., 2012, p. 1. ACM Press. DOI: 10.1145/2335356.2335364.
[259] UNESCO and Reporters without borders (2015) SAFETY GUIDE FOR JOURNALISTS: A handbook for reporters in high-risk environments. Reporters without borders. Available at: https://rsf.org/sites/default/files/guide_journaliste_rsf_2015_en_0.pdf (accessed 9 September 2019).
[260] Access Now (2018) A first look at digital security digital as of March 2018. March. Access Now. Available at: https://www.accessnow.org/cms/assets/uploads/2018/03/A-first-look-at-digital-security-digital-copy.pdf (accessed 9 September 2019).

unsatisfied. It covered a variety of example threats, including device loss and seizure by law enforcement, suspicious device activity, being impersonated or harassed online, and losing data, all of which inform the threats and consequences categorised in Chapter 5.[261]

The Electronic Frontier Foundation's "Surveillance Self-Defense" guide included "common security scenarios" that directly influence both the Chapter 8 framework, and some of the threats explored in Chapter 5. These focus on the likely data protection threats appropriate mitigations for a variety of defenders, including "journalism students" and "journalists on the move."[262] The guide's preemptive protections were useful to pare down countermeasures in Chapter 8, particularly the ones relating to encrypting communications channels, creating strong passwords, and how to prepare for situations where law enforcement might try to access equipment.

UNESCO's handbook for "Protecting Journalism Sources in the Digital Age" was also useful for establishing the scope of the threats considered in this thesis. It covered legal threats including "national security and anti-terrorism legislation", "surveillance – both mass and targeted," "mandatory data retention policies and pressure applied to third party intermediaries - like ISPs, telcos, search engines, social media platforms - to release data which risks exposing sources," and outdated source and journalistic shield laws.[263] These helped curate protections for the framework that related to both individuals and institutional action. For example, advocacy for "systems for transparency and accountability regarding data retention" informs Chapter 8's countermeasure C (transparency reporting). Journalist security training and education aimed at journalists and sources relate to countermeasure O (top-down education), and strengthened modern source protection laws is an important feature of countermeasure Q (legal scrutiny in favour of press freedom), also in Chapter 8's framework.

Much of the literature discussed in this section on existing cyber security advice for journalists speaks to the diversity of journalists and their work – including their employment or self-employment, the medium in which they work, and their beat. It is therefore important for this thesis to be mindful of this heterogeneity in order to meaningfully represent ways in which members of the press may be affected by threats and could act to protect themselves. This variety is emphasised by the geographic differences outlined in the country profiles (see: Chapters 6 and 7), and the many interviews conducted for this research were intended to contribute different perspectives and to portray variation within the news industry.

As a result, the framework (see: Chapter 8) includes the following columns: "Beneficiary (i.e. Is the countermeasure intended to help an individual, a news organisation as a business, or the news media existentially?)," and "Category of media roles that is most likely to be responsible for implementation of this countermeasure." These were created to maximise relevance and clarity of the implementation and goals of each recommended countermeasure for each potential framework user. Further, the lack of standard workflow across journalism spurred a collaboration with the Association for International Broadcasting and its global membership base, resulting in the design and release of a resource outlining common workflow stages. This work is incorporated into the framework via the column "Phase(s) of the

[261] Digital Defenders Partnership (2019) The Digital First Aid Kit – Introduction. In: *Defenders Partnership: Hivos International*. Available at: https://www.digitaldefenders.org/digitalfirstaid/ (accessed 9 September 2019).
[262] Electronic Frontier Foundation (2019) Surveillance Self-Defense: Tips, Tools and How-Tos for Safer Online Communications. Available at: https://ssd.eff.org/en (accessed 11 September 2020).
[263] Posetti J (2017) *Protecting Journalism Sources in the Digital Age*. UNESCO SERIES ON INTERNET FREEDOM. UNESCO. Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/protecting_journalism_sources_in_digital_age.pdf.

editorial workflow to which this countermeasure is most relevant," to prevent users from being overwhelmed by the feeling that they are responsible for implementing all mitigations at all times.

2.5.2 Literature discussing IoT protections

In order to create a novel countermeasures framework for IoT threats to journalists, existing IoT protection advice must be reviewed to ascertain the extent to which it can be adapted to be useful to a journalistic audience. For this purpose, a range of sources is necessary, given the diversity of the consumer IoT and its user groups, including academic papers, civil society resources, government advice, published books and news media. Overall, these sources list a variety of protections but do not mention journalists as possible targets of IoT exploitation, either avoiding specifying a user community, or focusing on other vulnerable groups. While literature aimed at other vulnerable groups is relevant to journalists, its utility is diminished because journalists are unlikely to be aware that this is the case. Further, most of the cyber security academic and government-published literature focused on protections for users more than bystanders, and mainly noted the need for coherent and achievable IoT standards, especially for security and privacy by design.

Most of the academic computer science literature that discussed mitigations for IoT threats focused on security and privacy by design. Studies such as Chalhoub *et al.* and Barbosa *et al*. established how user experience and attitudes influence the poor security by design of the consumer IoT.[264] Further, like Hoffmann's policy proposal document on smart home policy,[265] Atamli and Martin provided recommendations for long-term changes such as IoT security and privacy properties by design that would address some of their identified threat model characteristics.[266] The threat categories presented in Chapter 5 could educate journalists about IoT threats until the IoT industry implements such principles; these issues specifically are addressed by the regulatory gaps threat category presented in that chapter.

Similarly, Cha *et al*. devised seven categories of protection mechanisms against IoT-related threats to privacy but did not discuss the risks and needs associated with different user communities.[267] This is also often the case with privacy-focused literature that proposes technological countermeasures, such as the "Bracelet of Silence" that can temporarily jam all microphones within a given radius of the wearer.[268] However, these also place the responsibility for maintaining privacy on individuals, rather than inspiring structural change. Projecting the idea that technological solutions are the only viable way to protect personal privacy turns it into a luxury commodity that not everyone can afford. Relatedly, Bellman and van Oorschot used legal, technical, and social perspectives to review the utility of the phrase "best

[264] Barbosa NM, Zhang Z and Wang Y (2020) Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In: Proceedings of the Sixteenth USENIX Symposium on Usable Privacy and Security, Virtual, 9 August 2020, pp. 417–435. USENIX Association. Available at: https://www.usenix.org/conference/soups2020/presentation/barbosa (accessed 9 February 2021); Chalhoub G, Flechais I, Nthala N, et al. (2020) Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In: Proceedings of the Sixteenth USENIX Symposium on Usable Privacy and Security, Virtual, 9 August 2020, p. 21. USENIX Association.

[265] Hoffmann S (2018) IoT Security Architecture and Policy for the Home - a Hub Based Approach. 15 November. Oxford, United Kingdom: IoT Security Foundation. Available at: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf (accessed 12 August 2020).

[266] Atamli AW and Martin A (2014) Threat-Based Security Analysis for the Internet of Things. In: 2014 International Workshop on Secure Internet of Things, September 2014, pp. 35–43. DOI: 10.1109/SIoT.2014.10.

[267] Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. IEEE Internet of Things Journal 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658.

[268] Hill K (2020) Activate This 'Bracelet of Silence,' and Alexa Can't Eavesdrop. The New York Times, 14 February. Available at: https://www.nytimes.com/2020/02/14/technology/alexa-jamming-bracelet-privacy-armor.html (accessed 17 February 2020).

practice" relating to the IoT. They noted that it can be used to redirect liability and to enable obscure technical recommendations before they can be accurately assessed in terms of feasibility.[269]

In fact, ambient threats that affect bystanders are difficult to resolve, given their surreptitious nature. For example, Flammer's article focused on the myriad social norms and conventions that intersect in any "public" space, arguing that wearables are designed to look subtle, a trend that prevents bystanders from comprehending that their privacy may be at risk and could lead to social instability as a result of loss of trust.[270] Further, Hasan *et al*.'s proposal of the use of machine learning techniques to identify and obfuscate bystanders included in photographic images would require clear delineation between intentional and incidental subjects, a classification that could become more difficult with artistic photos and those taken for journalistic purposes.[271] Datta *et al.*'s paper on the privacy concerns of wearable devices also assessed the relative merits of pre- and post-hoc methods of privacy preservation. It claimed that the use of deep-learning algorithms to remove identifying features of bystanders after they have already been included in data collection, like photos, is a more feasibly implementable approach than insisting that everyone constantly give or refuse to give consent.[272]

Literature on best practice protections offers guidance for individuals, ranging from information for the general public to resources aimed at vulnerable populations. An example of the first category is the UK Department for Digital, Culture, Media & Sport's white paper on smart home devices,[273] which put the onus on individual consumers to implement security measures. Despite a lack of enforced regulation regarding IoT security, their advice relied on the device allowing configuration of settings, multi-factor authentication, updates, and factory resets. In the second category is Cornell Tech's Clinic to End Tech Abuse's series of resources that were intended to educate and empower the targets of Intimate Partner Violence.[274] In particular, these included a questionnaire for suspected targets to identify what their vulnerabilities could be, as well as a list of apps and devices that may be in the possession of the respondent, with the advice to make a list of all currently owned devices - including "connected devices, like cameras, thermostats, smart speakers, and smart TVs."[275] The advice covered changing passwords, and configuring device and cloud settings, to prevent non-consensual access and subsequent threats. While possibly useful for individuals in their own home, this advice cannot address threats from devices owned by other people. As such, while many of these guidance points are included in Chapter 8's framework, they are distinguished from recommendations that are intended to mitigate and protect against covert and ambient threats.

---

[269] Bellman C and van Oorschot PC (2020) Best Practices for IoT Security: What Does That Even Mean? arXiv:2004.12179 [cs]. Available at: http://arxiv.org/abs/2004.12179 (accessed 7 June 2021).

[270] Flammer I (2016) Genteel Wearables: Bystander-Centered Design. IEEE Security Privacy 14(5): 73–79. DOI: 10.1109/MSP.2016.91.

[271] Hasan R, Crandall D, Fritz M, Kapadia A (2019) Understanding and Recognizing Bystanders in Images for Privacy Protection. In: 19th Privacy Enhancing Technologies Symposium, KTH, Stockholm, Sweden, 15 July 2019, p. 2.

[272] Datta P, Namin AS and Chatterjee M (2018) A Survey of Privacy Concerns in Wearable Devices. In: 2018 IEEE International Conference on Big Data (Big Data), December 2018, pp. 4549–4553. DOI: 10.1109/BigData.2018.8622110.

[273] Department for Digital, Culture, Media & Sport (2018) Smart devices: using them safely in your home. Available at: https://www.gov.uk/government/publications/smart-devices-using-them-safely-in-your-home/smart-devices-using-them-safely-in-your-home (accessed 4 March 2020).

[274] Clinic to End Tech Abuse (CETA), Cornell Tech (2021) Resources. Available at: https://www.ceta.tech.cornell.edu (accessed 7 June 2021).

[275] Clinic to End Tech Abuse (CETA), Cornell Tech (2020) Tech Disconnect: Checklist. Clinic to End Tech Abuse. Available at: https://82beb9a6-b7db-490a-88be-9f149bafe221.filesusr.com/ugd/c4e6d5_20fe31daffd74b2fb4b4735d703dad6a.pdf (accessed 19 October 2021); Clinic to End Tech Abuse (CETA), Cornell Tech (2020) Technology Assessment Questionnaire (TAQ) v5. Clinic to End Tech Abuse, Cornell Tech. Available at: https://9aa4dcb3-08e0-4365-9068-df09709ff0ca.filesusr.com/ugd/884c63_280fab3bd82e44348691bbc9b9038a7d.pdf (accessed 19 October 2021).

There are many key sources that put the onus of protection on institutional stakeholders, including government and corporate actors. For example, the US Department of Homeland Security's document, "Strategic Principles for Securing the Internet of Things," contained high level recommendations for IoT policymakers regarding both manufacturers (e.g. "build on proven security practices") and consumers (e.g. "connect carefully and deliberately").[276] A specific principle that aligns with the goal of this thesis's framework is "prioritise security measures according to potential impact." Further, the resource recommended that all stakeholders heighten their awareness of IoT risks and pledged that the Department of Homeland Security will facilitate this across sectors in the US. This included advising that IoT consumers are given sufficient information about which features of a device are necessary for it to function, so that they may decide which connections are in their best interest.

Similarly, Bellman and van Oorschot noted that governments' purchasing power allows them to put pressure on manufacturers to ensure product security and privacy measures.[277] They categorised IoT lifecycle stages and stakeholders, which enabled their paper to identify problems with discussions of best practice; for example, calling for government regulation has the benefit of enforcing these practices across a region, but also the disadvantages of "overreach, lengthy enactment periods, and inadequacy."[278]

Combining many of the aforementioned themes, the Online Trust Alliance's IoT Trust Framework was unusual.[279] This is because it considered potential policy shifts by multiple stakeholders (including governments and the need for both individual and collective action by consumers) to address the privacy and security vulnerabilities at each stage of an IoT product's entire lifecycle. It was further unique in that it covered an entire IoT ecosystem, from devices to apps. Their IoT Trust Framework included eight categories of principles that could decrease the risk associated with the consumer IoT: user authentication, encryption, security by design, updates, limitation of data collection, full disclosure of privacy threats, data-control by the consumers, and communications security to prevent social engineering attacks. These inform some of the threats outlined in the threat categorisation (see: Chapter 5).

Similarly, Mozilla Foundation's "buyer's guide for connected products" included both individual recommendations and ways for users to contribute their own ideas, thus prefacing the principles of co-creation and validation used in this research.[280] Their paper sorted the privacy and security considerations of specific IoT devices into the following categories: "All/Best Of/Dating Apps/Smart Home/Toys & Games/Entertainment/Wearables/Health & Exercise/Home Office/Pets/Sex Toys" - categories that influenced the structure of the IoT device organisational model in Chapter 5. To ensure accessibility by readers, Mozilla set standards for baseline security features, labelling products as "Privacy Not Included" if the authors cannot confirm that they have met these standards. Further, users of this rating system are

[276] US Department of Homeland Security (2016) Strategic Principles for Securing the Internet of Things (IoT). 15 November. Washington DC: US Department of Homeland Security. Available at: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf (accessed 7 June 2021).
[277] Bellman C and van Oorschot PC (2020) Best Practices for IoT Security: What Does That Even Mean? arXiv:2004.12179 [cs]. Available at: http://arxiv.org/abs/2004.12179 (accessed 7 June 2021).
[278] Bellman C and van Oorschot PC (2020) Best Practices for IoT Security: What Does That Even Mean? arXiv:2004.12179 [cs]. Available at: http://arxiv.org/abs/2004.12179 (accessed 7 June 2021).
[279] Online Trust Alliance (2018) OTA IoT Trust Framework. 22 May. USA: Internet Society. Available at: https://www.internetsociety.org/iot/trust-framework/ (accessed 7 June 2021).
[280] Mozilla Foundation (2021) *Privacy Not Included: A Buyer's Guide for Connected Products. Available at: https://foundation.mozilla.org/en/privacynotincluded/ (accessed 7 June 2021).

able to contribute their own opinions and experiences. This emphasises the need for corporations to increase their product security, while facilitating informed purchasing decisions by consumers - rather than prescribing increased individual protections by users, as in the framework in this thesis (see: Chapter 8).

2.6 Conclusion

In summary, this chapter reviewed the existing literature relevant to understanding how the Internet of Things (IoT) may threaten journalists and journalistic work. The chapter further examined how later chapters in this thesis build on and fill gaps within existing scholarship.

First, it defined the consumer IoT, explained the exclusion of smart city infrastructure from the scope of this research, and established the imperative to categorise both devices and their threats to aid journalists' understanding of IoT risk. Second, the chapter discussed the significance of the relationship between the IoT and privacy and security. It found that there is widespread acknowledgement of the various threats stemming from the IoT across the academic literature, but that these are rarely considered in a consolidated way. Third, it found that the literature currently concludes that, rather than effectively addressing potential IoT harms through law or policy, there are regulatory loopholes that enable exploitation of the data collection capabilities of the IoT. Fourth, it scrutinised any documented links between the IoT and journalism, and found a notable absence in identifying and examining these links in academic, grey, and journalistic literature. In particular, there is a lack of existing resources either in academic research or in other forms of literature that recommend IoT protections for the specific population of journalists. A key contribution of this thesis is therefore its novel countermeasures framework (see: Chapter 8), which aims to close this gap.

Chapter 3: Methods

3.1 Introduction

To avoid repetition between sections, this chapter will not discuss each chapter in turn. Rather, it will break down the research methods as follows: Section 3.2 will outline research design of the various studies that comprise this thesis. Section 3.3 will then discuss participants, including ethics, recruitment, and expertise. Section 3.4 will cover data collection. Finally, section 3.5 will present detailed descriptions of data processing methods and how the analyses fed into each chapter. Whilst for scientific detachment, mentions of the researcher are avoided, for the avoidance of doubt, all the research described here was undertaken by the author of the thesis.

Given its interdisciplinary nature, this research utilised primarily qualitative mixed methods (i.e. literature reviews, country profiles, online surveys, and interviews). This includes a review of published literature that is relevant to the protection of journalists from IoT-specific cyber threats, IoT-specific cyber-physical threats, and legal threats. A particular focus are those threats that are facilitated by an increase in the amount and kinds of data collected, stored, transferred, and analysed due to the prevalence of the IoT.

The use of mixed methods in this thesis is in line with Hesse-Biber and Burke Johnson's definition of mixed methods as "an approach to research in which the investigator collects, analyses, and interprets both quantitative and qualitative data (closed and open-ended information), integrates or combines the two approaches in various ways, and frames the study within a specific type of design or procedure."[281] They advocate for the use of mixed methods where research is being conducted in "border studies"[282] as in the case of this thesis, which links disciplines of cyber security and human-computer interaction, journalism studies and surveillance studies. The goal of mixed methods is to overlay different perspectives, methods, and types of information, to form judgements that combine the comparative strengths of these components to contextualise and address factors that would be neglected by each method or discipline alone.[283] This interdisciplinarity is necessary in this thesis because of the diverse ways in which IoT can threaten the press, requiring a range of tools and perspectives to develop user-relevant mitigations and countermeasures.

This thesis includes two chapters profiling and comparing two country profiles each (see: Chapters 6 and 7), to allow direct comparison of these countries. These were compiled through long-form, semi-structured qualitative interviews of members of the media, experts in the IoT industry and cyber security professionals in each place. Similarly, the exploratory study (Chapter 4) was informed by interviews, as well as online questionnaires. Further, Chapter 2's literature synthesis was updated to reflect the state of publications on the topic from 2018 to 2022, while the country profiles keep this research grounded in the practical reality of the situation regarding press freedom and IoT threats in each country. Building on these, Chapter 5's conceptual model and threats categorisation are intended to be flexible organisational

[281] Hesse-Biber, SN, & Johnson, RB (eds) 2015, The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry, Oxford University Press, Incorporated, Oxford. Available from: ProQuest Ebook Central: pp. xxxiii-xxxiv.
[282] Hesse-Biber, SN, & Johnson, RB (eds) 2015, The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry, Oxford University Press, Incorporated, Oxford. Available from: ProQuest Ebook Central: pp. xxxiii-xxxiv.
[283] Harrison RL, Reilly TM and Creswell JW (2020) Methodological Rigor in Mixed Methods: An Application in Management Studies. *Journal of Mixed Methods Research* 14(4). SAGE Publications: 473–495. DOI: 10.1177/1558689819900585; Bazeley P (2009) Editorial: Integrating Data Analyses in Mixed Methods Research. *Journal of Mixed Methods Research* 3(3). SAGE Publications: 203–207. DOI: 10.1177/1558689809334443; Furszyfer Del Rio DD, Sovacool BK and Griffiths S (2021) Culture, energy and climate sustainability, and smart home technologies: A mixed methods comparison of four countries. *Energy and Climate Change*: 100035. DOI: 10.1016/j.egycc.2021.100035; Creswell JW and Clark VLP (2017) *Designing and Conducting Mixed Methods Research*. United States of America: SAGE Publications.

methods for risk assessment and management. Finally, the use of questionnaires for validation of the final toolkit enabled more structured expert feedback on the utility of the output of this research (see: Chapters 8 and 9).

These specific research methods (interviews for the country profiles and surveys for the validation study) were chosen because they have "non overlapping weaknesses in addition to their complementary strengths."[284] For example, semi-directed interviews allow in-depth investigation and the gathering of "thick data" (i.e. "an in-depth understanding of people's beliefs and behaviours in their context,")[285] which enables the different chapters of this research to build conceptual models, literature reviews, and country profiles into an academically rigorous and practical final framework, all forming a security toolkit. Furthermore, this framework has been validated by three pools of experts via surveys, enabling larger numbers of structured responses and confirmation of the findings from multiple angles of expertise. To provide an introduction to the content in sections 3.4 and 3.5 of this chapter, Figure 1 below clarifies how the different chapters, and their specific methods of data collection and analysis were used. It is intended to outline how the chapters were formulated and work together:

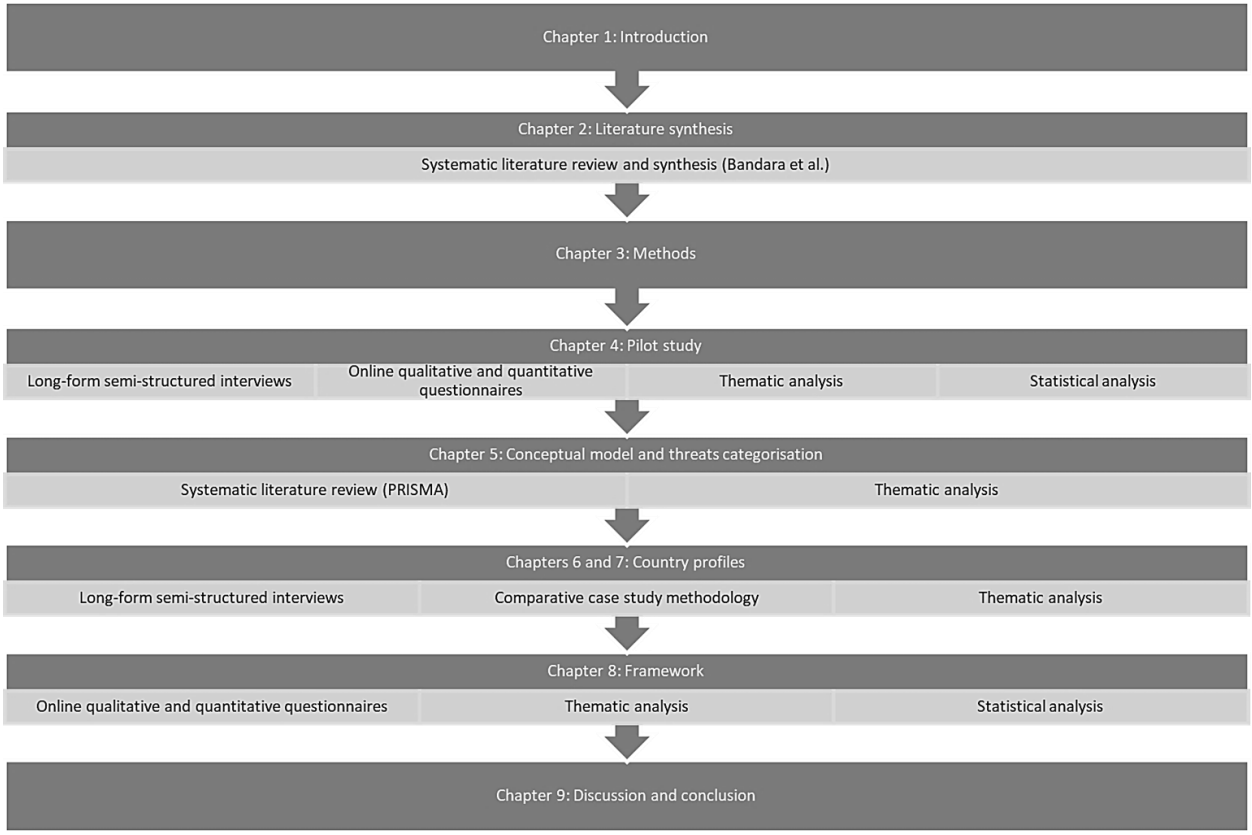


Figure 1: Visual overview of chapters

[284] Hesse-Biber, SN, & Johnson, RB (eds) 2015, The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry, Oxford University Press, Incorporated, Oxford. Available from: ProQuest Ebook Central: 5.
[285] Smets A and Lievens B (2018) Human Sensemaking in the Smart City: A Research Approach Merging Big and Thick Data. *Ethnographic Praxis in Industry Conference Proceedings* 2018(1): 179–194. DOI: 10.1111/1559-8918.2018.01203.

3.2 Research design

3.2.1 Literature reviews and syntheses

A key methodology of this research is analysis of both empirical and theoretical literature in order to fill the gap in understanding regarding IoT threats to journalism between members of the media and the academic communities. Chapter 2 comprises the main review and synthesis of the literature in this thesis. It compares different forms of literature on the IoT, covering perspectives from the computer science, cyber security, journalism, and national security communities. It also combines evaluations of IoT literature with analyses of publications on press freedom and threats to journalists and news organisations in the profiled countries, as well as an appraisal of the potential for IoT exploitation in each country.

Additionally, more focused literature searches were also part of other aspects of the research, including for the organisational models presented in Chapter 5 and the country profiles in Chapters 6 and 7. To ensure the literature synthesis and the literature reviews underpinning each chapter included all relevant contemporary academic material, a multifaceted search strategy was employed to methodically extract relevant papers, per Bandara *et al.*'s systematic literature review and synthesis method.[286]

To minimise selection bias as specific keywords were not consistently used across all publications, constrained snowball sampling of literature across a range of online databases, conference proceedings, journal ranking lists, including Web of Science, ACM Proceedings Digital Library and IEEE Xplore Digital Library, as well as the country-specific ACPHIS Journal Ranking.[287] This sampling required the use of the aforementioned keywords and others that recurred during online searches: journalists' names, specific instances of cyber-attack or vulnerabilities. These were arranged in different combinations. As advised by both Bandara *et al.* and Levy and Ellis, relevant papers were identified, then backward and forward searching was conducted to determine more publications that were cited by or that cited the identified paper.[288]

---

[286] Bandara W, Miskon S and Fielt E (2011) A systematic, tool-supported method for conducting literature reviews in information systems. In: *ECIS 2011 Proceedings* (eds M Rossi and J Nandhakumar), Brisbane, Australia, 2011, pp. 1–13. Queensland University of Technology. Available at: https://eprints.qut.edu.au/42184/1/42184c.pdf.

[287] Bandara W, Miskon S and Fielt E (2011) A systematic, tool-supported method for conducting literature reviews in information systems. In: *ECIS 2011 Proceedings* (eds M Rossi and J Nandhakumar), Brisbane, Australia, 2011, pp. 1–13. Queensland University of Technology. Available at: https://eprints.qut.edu.au/42184/1/42184c.pdf; Association for Computing Machinery (ACM) (2020) ACM Proceedings Digital Library. Available at: https://dl.acm.org/proceedings (accessed 14 April 2020); Australian Council of Professors and Heads of IS (2019) Australian Council of Professors and Heads of Information Systems (ACPHIS) Journal Ranking. Available at: https://www.acphis.org.au (accessed 14 April 2020); Institute of Electrical and Electronics Engineers (IEEE) (2020) IEEE Xplore Digital Library. Available at: https://ieeexplore.ieee.org/Xplore/guesthome.jsp?utm_source=mm_link&utm_campaign=vix&utm_medium=pubs&utm_term=Xplore%20guest (accessed 14 April 2020).
Thomson Reuters and Clarivate Analytics (2020) Web of Science [v.5.34] - Web of Science Core Collection Basic Search. Available at: https://apps.webofknowledge.com/WOS_GeneralSearch_input.do?product=WOS&search_mode=GeneralSearch&SID=C3pUmUGBBQzCxmoaLcM&preferencesSaved= (accessed 14 April 2020); Association for Computing Machinery (ACM) (2020) ACM Proceedings Digital Library. Available at: https://dl.acm.org/proceeings (accessed 14 April 2020); Institute of Electrical and Electronics Engineers (IEEE) (2020) IEEE Xplore Digital Library. Available at: https://ieeexplore.ieee.org/Xplore/guesthome.jsp?utm_source=mm_link&utm_campaign=vix&utm_medium=pubs&utm_term=Xplore%20guest (accessed 14 April 2020); Australian Council of Professors and Heads of IS (2019) Australian Council of Professors and Heads of Information Systems (ACPHIS) Journal Ranking. Available at: https://www.acphis.org.au (accessed 14 April 2020).

[288] Bandara W, Miskon S and Fielt E (2011) A systematic, tool-supported method for conducting literature reviews in information systems. In: *ECIS 2011 Proceedings* (eds M Rossi and J Nandhakumar), Brisbane, Australia, 2011, pp. 1–13.

Additionally, due to the quickly evolving nature of this topic, news articles offer an important alternative and contemporary perspective, albeit without the filtering and reflective analysis of a more academic study. As a result, search engines Google and DuckDuckGo were used to research relevant mass media materials and "grey literature."[289] This highlighted that the technological threat landscape is rapidly growing, and this thesis is necessitated by an absence of guidance for the media industry on countering IoT threats. However, to the extent that it is possible, general guidance that has been published on digital security for journalists was considered.[290]

Literature syntheses for the creation of Chapter 5's conceptual model and threats categorisation used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines.[291] Other systematic literature searching, collation and synthesis methods that were considered included PICO and The Cochrane Handbook,[292] both of which are primarily used in the medical field, whereas PRISMA also has proven examples of implementation in the security field.[293]

Sources for both Chapter 5's conceptual model and threats categorisation included academic publications (primarily in the fields of Journalism Studies, Law, Computer Science and Cyber Security), news articles, websites popular among journalists, and policy papers, to ensure that this research reviewed all germane perspectives. Using PRISMA to guide the information-gathering method facilitated finding the most contemporary and salient publications available relating to both the consumer IoT in general and its threats to the press. Thematic coding and analysis were conducted to curate the findings for use in both the conceptual model and threats categorisation (see: section 3.5 of this chapter).

Both Chapter 5 reviews began using assorted combinations of search terms: "consumer Internet of Things," "IoT," "smart home," "smart device," and "networked device." The threats categorisation research added "security," "privacy," "threat model" and "journalism." Keywords grew to include other recurring terms in the results: "journalist safety," "surveillance," "source confidentiality" and "legal threats."

Google Scholar Keyword Alerts were used to follow phrases that were found in recently published theses, chapters, and papers, particularly to support the country profiles in Chapters 6 and 7: "internet of things,"

Queensland University of Technology. Available at: https://eprints.qut.edu.au/42184/1/42184c.pdf; Levy Y and Ellis TJ (2006) A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Science Journal (9), 181-212.

[289] The New York Academy of Medicine (2019) "What Is Grey Literature?", Available at: www.greylit.org/about [Accessed 17 December 2019].

[290] Smyth F, Lowenthal T and O'Brien D (2012) *Journalist Security Guide: Covering the news in a dangerous and changing world*. Committee to Protect Journalists (CPJ). Available at: https://cpj.org/security/guide.pdf (accessed 15 January 2020); Carlo S and Kamphuis A (2014) *Information Security for Journalists v1.1*. Centre for Investigative Journalism. Available at: https://files.gendo.ch/Books/InfoSec_for_Journalists_V1.1.pdf (accessed 9 September 2019).

[291] PRISMA (2015) Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Checklist. Available at: http://prisma-statement.org/PRISMAStatement/Checklist.aspx (accessed 11 February 2021).

[292] Brown D (2020) A Review of the PubMed PICO Tool: Using Evidence-Based Practice in Health Education. Health Promotion Practice 21(4): 496–498. DOI: 10.1177/1524839919893361; Higgins JPT, Thomas J, Chandler J, et al. (2019) Cochrane Handbook for Systematic Reviews of Interventions. 2nd edition. Hoboken, NJ: John Wiley & Sons.

[293] Knight R and Nurse JRC (2020) A framework for effective corporate communication after cyber security incidents. Computers & Security 99: 102036. DOI: 10.1016/j.cose.2020.102036; Uchendu B, Nurse JRC, Bada M, et al. (2021) Developing a cyber security culture: Current practices and future needs. Computers & Security 109: 102387. DOI: 10.1016/j.cose.2021.102387; Okoli C (2015) A Guide to Conducting a Standalone Systematic Literature Review. Communications of the Association for Information Systems 37(1). DOI: 10.17705/1CAIS.03743.

"media suppression," "press freedom," "UK journalists," "Taiwan journalists," "Australia journalists," "US journalists" and "journalism." These key phrases were used individually and combined in as many novel ways as possible, to ensure that the resultant articles were maximally relevant.

3.2.2 Interview guides

In accordance with Hesse-Biber and Johnson's perspective on cross-disciplinary work, in addition to country profiling, the mixed methods research undertaken in this study includes long-form interviews.[294] As there is a gap in the literature relating to the impact of the IoT on journalism, the interviews were semi-structured, rather than fully structured interviews, to ensure the collection of thick qualitative data across a range of relevant topics.[295] Questions were formulated based on the overarching thesis research question and were phrased as neutrally as possible.

This kind of interview methodology was chosen in order for participants to talk openly about their experiences, expectations, and expertise. It allowed novel areas of interest to be raised organically and for later interviews to capitalise on new questions that arose. Other methods that were considered for this purpose were focus groups and group interviews. However, these options would have allowed respondents less scheduling flexibility and minimised the time available for each individual to share thoughts. Further, a drawback of group data collection methods is their potential to cause some participants to not contribute their perspective because louder participants are sharing the opposing view.[296] Both group interviews and focus groups were also discarded as options because of their prioritisation of participants interacting with each other, rather than responding to set questions from an interviewer.[297]

3.2.3 Questionnaires

This thesis refers to surveys and questionnaires interchangeably.

3.2.3.1 Exploratory study questionnaires

As part of the Chapter 4 exploratory study, two online questionnaires were developed, one for journalists (to supplement the interviews) and one for cyber security experts. The second survey collected concerns and recommendations to inform individuals on how to minimise or mitigate IoT threats. Here, questionnaire design will be discussed, while participants and the expert recruitment process are included in a later section.

The questionnaire for journalists who declined the semi-structured interviews was designed in collaboration with the Association for International Broadcasting (AIB). This questionnaire, like the semi-structured interviews, was intended to discover what journalists are doing to increase their security against third-party exploitation of new Internet of Things devices. Although there are few examples of qualitative surveys used as a substitute for some interviews, extending the reach of the data collection by ensuring flexibility for participants who preferred one method more than another increased the number

[294] Hesse-Biber, SN, & Johnson, RB (eds) 2015, The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry, Oxford University Press, Incorporated, Oxford. Available from: ProQuest Ebook Central: pp. xxxiii-xxxiv.
[295] Smets A and Lievens B (2018) Human Sensemaking in the Smart City: A Research Approach Merging Big and Thick Data. *Ethnographic Praxis in Industry Conference Proceedings* 2018(1): 179–194. DOI: 10.1111/1559-8918.2018.01203.
[296] Kitzinger J (1995) Qualitative Research: Introducing focus groups. BMJ 311(7000). British Medical Journal Publishing Group: 299–302. DOI: 10.1136/bmj.311.7000.299.
[297] Watts M and Ebbutt D (1987) More than the Sum of the Parts: research methods in group interviewing. *British Educational Research Journal* 13(1): 25–34. DOI: 10.1080/0141192870130103.

of participants without compromising the quality of responses.[298] The survey questions were formulated based on the interview guide (see: Appendices A and B). Although most responses were quantitative, the questionnaire also included space for long-form comments. Ethical approval for this study was granted by the University of Oxford Central University Research Ethics Committee (for approval numbers of each study, see the Ethics section of this chapter).

The survey for cyber security experts was designed to evaluate the protective tools and techniques used by journalists and members of the public against the IoT threats. This survey focused on three aspects: digital and physical threats associated with the use of smart devices, whether and how they would advise members of the public to cope with these threats, and the extent to which members of the general public can opt-out of the use of IoT devices now and in the future. As the journalist-focused part of the exploratory study revealed that journalists were not aware of even basic IoT risks that could apply to anyone, cyber security experts were asked for recommendations for the general public, rather than for journalists specifically, because it was important to ensure that expert responses did not overlook basic protections and mitigations that would affect everyone. However, not specifically asking expert respondents about IoT threats to the free press may have influenced their responses towards underestimation of risk, which is a limitation of the chosen approach.

3.2.3.2 Questionnaires for validation of framework content

In order to populate the prototype framework to help members of the media assess and manage the journalism-specific risks associated with the IoT, four surveys were developed to solicit responses from experts in three topics: the media, cyber security, and states' technological and legal capabilities of exploitation. Each survey included different question types (e.g. open-ended questions, closed yes/no, scale and rank questions). This variety provided both thick and more easily statistically analysable material, to enable assessment of areas of potential improvement to the conceptual models and framework. See all four full questionnaires in Appendices H, I, J, and K.

The media survey asked experts to match each countermeasure to: (1) the overarching phase(s) of the journalistic workflow to which the countermeasure is most relevant (per the top-level workflow designated by the Association for International Broadcasting, AIB), (2) the category of media roles that is most likely to be responsible for implementation of the countermeasure, (3) the beneficiary of the countermeasure, and (4) the feasibility of implementation of the countermeasure. The expertise needed for co-creation and validation of the cyber security sections of the framework was too substantial to use just one survey; the amount of time necessary was considered to be too much to ensure an adequate rate of completion. The necessary sections of the cyber security topic survey were thus split between two surveys: one on the topic of feasibility and function of the countermeasures, and another focused on matching the threats (from Chapter 5) to countermeasures, and determining the disadvantages for each countermeasure.

Finally, the states' capabilities survey asked experts to mark on a scale their perceptions regarding the current and anticipated realism of the IoT threats against journalistic and the utility of the assigned countermeasures. This was intended to validate the need for the framework's existence and for its potential future use in journalistic security trainings.

[298] Braun V, Clarke V, Boulton E, et al. (2021) The online survey as a qualitative research tool. *International Journal of Social Research Methodology* 24(6). Routledge: 641–654. DOI: 10.1080/13645579.2020.1805550.

The framework validation study (see Chapter 8) used questionnaire-style qualitative data collection.[299] Interactive methods of data collection were considered as an alternative, such as interviews, group interviews and focus groups. However, surveys were chosen as the methodology for this study because of the ease and speed with which they can be completed, as experts in these three topics may be resident anywhere in the world. They were also chosen because they could be structured to lead participants through questions on the content of the framework, without influencing their answers which is less possible with the other named methods, as they would necessitate interaction with participants.[300] To this end, a pilot study was conducted, in which two experts in each topic were asked to complete each survey and to provide feedback on the surveys themselves (see: section 3.4.3 of this chapter).

3.2.4 Country profiles

3.2.4.1 Comparative case study methodology rationale

This thesis' overarching research question is "How can members of the press in democratic countries improve their identification of, protection from, and resilience against threats from the Internet of Things?", so it was first essential to identify how the press in these countries are dealing with IoT threat models.

Comparative case studies act as an analytical tool for cross-national research by using interviews with relevant subject-matter experts to build upon literature-derived foundational evaluation of each profiled country with respect to clear themes.[301] Comparative case study-based research allows nuance and depth such that the resulting framework of journalism-specific IoT threat mitigation methods developed in Chapter 8 could be tailored to contextual needs and realities.[302] This makes the recommendations more likely to be feasibly implemented in each examined country.[303]

A case study method was chosen over statistical quantitative methods because, although there is merit to large-scale analyses, carefully chosen case studies of specific examples from different "classes of events" allow extrapolation of inferences to other cases within a broader, well-defined group.[304] Therefore, a case study approach to analysis highlights the chosen countries' many similarities, which can then be considered in subsequent analogous cases of nation-states desiring to update their laws and policies regarding the press and emerging technologies. Furthermore, there are recognised advantages to a case study methodology that are absent in other techniques. These include the "potential for achieving

[299] Bowling NA, Huang JL, Brower CK, et al. (2021) The Quick and the Careless: The Construct Validity of Page Time as a Measure of Insufficient Effort Responding to Surveys. *Organizational Research Methods*. SAGE Publications Inc: 10944281211056520. DOI: 10.1177/10944281211056520.

[300] Braun V, Clarke V, Boulton E, et al. (2021) The online survey as a qualitative research tool. *International Journal of Social Research Methodology* 24(6). Routledge: 641–654. DOI: 10.1080/13645579.2020.1805550.

[301] Kennett P (2001). *Comparative social policy*. Buckingham: Open University Press: p.144; Noguera J and Morcillo L (2012) The Future of Non-Metropolitan Regions in the European Union: A Member-State Comparative Report. European Development Opportunities for Rural Areas (EDORA). Spain: Universitat de València.

[302] Goodrick D. (2014). Comparative Case Studies: Methodological Briefs - Impact Evaluation No. 9, Methodological Briefs no. 9. UNICEF-IRC. Available at: https://www.unicef-irc.org/publications/754-comparative-case-studies-methodological-briefs-impact-evaluation-no-9.html

[303] Rio DDFD, Sovacool BK and Griffiths S (2021) Culture, energy and climate sustainability, and smart home technologies: A mixed methods comparison of four countries. *Energy and Climate Change*: 100035. DOI: 10.1016/j.egycc.2021.100035.

[304] George AL and Bennett A (2004) *Case Studies and Theory Development in the Social Sciences*. Belfer Center for Science and International Affairs. Cambridge, Massachusetts: MIT Press. Available at: https://pdfs.semanticscholar.org/94e9/eec015c650880356853533c4dc9b2dac42bb.pdf.

high conceptual validity"[305] and their utility in identifying and untangling complex causal influences in a given context.[306] Comparative case studies can also include both qualitative and quantitative elements, so there is no limit to the potential depth of analysis both within and between case studies.[307]

Interviews were semi-structured and focused on particular themes, enabling detailed investigation of the similarities and differences between a small number of examples in order to develop theories that can guide policy.[308] There are anticipated challenges to mixed research methods case studies, such as potentially conflicting interview responses.[309] However, these problems can be overcome with understanding of the environmental and experiential factors that affect participants. Tension due to varying contextual significance of privacy across societies is a facet of this research. Therefore, extensive preparation to understand each national interpretation and context-specific privacy considerations was undertaken prior to commencing interviews.[310]

3.2.4.2 Case selection

Case selection is another challenging aspect of research design. Rather than dictating specific criteria for the selection of case studies,[311] Kennett argued that "in studies of a small number of cases, random selection can be more likely to result in bias than intentional selection."[312] In order to avoid selection bias as much as possible, options for case studies were initially narrowed by only considering countries listed in the top 30% of V-Dem's 2018 Liberal Democracy Index.[313] This research focuses on "liberal democratic nation-states" as the class of political system exemplified by the country profiles, as they have a general cultural predilection for maintaining the values that underpin and support the free press to which this thesis can appeal. Although press freedom is, naturally, under great threat within and from authoritarian regimes, Reporters Without Borders has noted an increasing trend of regressive and restrictive behaviours

[305] George AL and Bennett A (2004) *Case Studies and Theory Development in the Social Sciences*. Belfer Center for Science and International Affairs. Cambridge, Massachusetts: MIT Press. Available at: https://pdfs.semanticscholar.org/94e9/eec015c650880356853533c4dc9b2dac42bb.pdf.

[306] Goodrick D. (2014). Comparative Case Studies: Methodological Briefs - Impact Evaluation No. 9, Methodological Briefs no. 9. UNICEF-IRC. Available at: https://www.unicef-irc.org/publications/754-comparative-case-studies-methodological-briefs-impact-evaluation-no-9.html

[307] *Encyclopedia of Case Study Research* (2010) Comparative Case Study. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. DOI: 10.4135/9781412957397.n64. Available at: https://methods.sagepub.com/reference/encyc-of-case-study-research/n64.xml

[308] George AL and Bennett A (2004) Case Studies and Theory Development in the Social Sciences. Belfer Center for Science and International Affairs. Cambridge, Massachusetts: MIT Press.

[309] Becker S, Bryman A and Ferguson H (eds) (2012) Understanding Research for Social Policy and Social Work. 2nd Revised edition edition. Bristol: Policy Press.

[310] See, for example: Ess C (2005) 'Lost in Translation'?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia). *Ethics and Information Technology*; Dordrecht 7(1): 1–6. DOI: http://dx.doi.org/10.1007/s10676-005-0454-0; Ho C (2019) Configuration of the Notion of Privacy as a Fundamental Right in Taiwan—A Comparative Study of International Treaties and EU Rules. In: Cohen JA, Alford WP, and Lo C (eds) *Taiwan and International Human Rights: A Story of Transformation. Economics, Law, and Institutions in Asia Pacific.* Singapore: Springer, pp. 423–436. DOI: 10.1007/978-981-13-0350-0_24.

[311] King G, Keohane RO and Verba S (1994) Determining What to Observe. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 115–149. Available at: https://www.jstor.org/stable/j.ctt7sfxj.7 (accessed 25 January 2020).

[312] Kennett P (2001). *Comparative social policy*. Buckingham: Open University Press: p.144.

[313] Varieties of Democracy (V-Dem) (2019) *V-DEM ANNUAL DEMOCRACY REPORT 2019: Democracy Facing Global Challenges*. V-DEM ANNUAL DEMOCRACY REPORT. V-Dem Institute at the University of Gothenburg, Sweden: Varieties of Democracy (V-Dem) Institute at the University of Gothenburg: 11 Available at: https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf (accessed 11 January 2020).

and practices in democratic nation-states around the world.[314] To ensure that cases could be seen as globally representative, they were sorted by continent. Due to language and potential access constraints, countries without English as one of their dominant languages were systematically filtered out. As there were time constraints associated with this research, four case studies were chosen, on four different continents.

This research is intended to establish the current and anticipated impact of the IoT on press freedom considerations in liberal democratic nation-states. Therefore, the chosen case study countries needed to be both representative of democracies and also not so divergent in culture and structure that the resulting recommendations lacked applicability across all profiled countries.[315] Using a Liberal Democracy index[316], the United Kingdom (UK), the United States of America (US), Taiwan and Australia were chosen to ensure representation across different continents and enable access to sufficient interviewees to provide necessary qualitative data. The UK, the US, Taiwan[317] and Australia are internationally influential liberal democracies[318] with English as a widely used media language,[319] policymaker interest in developing and/or regulating the IoT market,[320] and recent domestic data collection-related legislation.[321]

The inclusion of Taiwan seems to be an outlier among countries that are typically Western democracies. However, Taiwan represents a different but equally valid class of emerging democracies with a demonstrated dedication to the values that stereotypically characterise such countries, in an era where such values are depleting in other, more established democratic nation-states.

[314] Reporters Without Borders (2019) 2019 World Press Freedom Index | Reporters Without Borders. Available at: https://rsf.org/en/ranking (accessed 13 January 2020).
[315] Kennett P (2001). Comparative social policy. Buckingham: Open University Press: p.144.
[316] Varieties of Democracy (V-Dem) (2019) V-DEM ANNUAL DEMOCRACY REPORT 2019: Democracy Facing Global Challenges. V-DEM ANNUAL DEMOCRACY REPORT. V-Dem Institute at the University of Gothenburg, Sweden: Varieties of Democracy (V-Dem) Institute at the University of Gothenburg: 11 Available at: https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf (accessed 11 January 2020).
[317] Thompson L (2020) Why Taiwan Has Become The 'Geographical Pivot Of History' In The Pacific Age. Available at: https://www.forbes.com/sites/lorenthompson/2020/09/29/why-taiwan-has-become-the-geographical-pivot-of-history-in-the-pacific-age/ (accessed 31 December 2020).
[318] Wells AR (2020) Between Five Eyes: 50 Years of Intelligence Sharing. United Kingdom: Casemate.
[319] Tian S, Liu L and Christian CY (2004) Course-specific Corpora in the Classroom: A News Media English Class in Taiwan." The Journal of Asia TEFL 1(1): 267–290.
[320] US: Castro D and New J (2016) Everything the U.S. Government Is Doing to Help the Private Sector Build the Internet of Things. 12 December. USA: Center for Data Innovation. Available at: https://www2.datainnovation.org/2016-federal-support-iot.pdf (accessed 1 January 2021); UK: Gunashekar S, Spisak A, Dean K, et al. (2016) Accelerating the Internet of Things in the UK: Using policy to support practice. 4 October. Santa Monica, CA: RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR1492.html (accessed 31 December 2020); Taiwan: Department of Investment Service, Ministry of Economic Affairs (2019) Key Industries: The Internet of Things. Department of Investment Service, Ministry of Economic Affairs. Available at: https://www.contacttaiwan.tw/ (accessed 31 December 2020); Australia: Department of Home Affairs (2020) Voluntary Code of Practice: Securing the Internet of Things for Consumers. Available at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice (accessed 31 December 2020).
[321] US: DLA Piper (2019) Law in United States. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2= (accessed 26 January 2020); UK: Information Commissioner's Office (2019) Data Protection Act 2018: For Organisations. Available at: https://ico.org.uk/for-organisations/data-protection-act-2018/ (accessed 28 May 2019); Taiwan: DLA Piper (2019) Law in Taiwan, China. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=TW (accessed 26 January 2020); Australia: DLA Piper (2019) Law in Australia. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=AU&c2= (accessed 26 January 2020).

3.3 Participants

This subsection will first cover relevant ethical issues of this research, including harms and benefits of the data collection for this research, as well as efforts made to ensure participant privacy and confidentiality, and to secure ethical approval and informed consent. It will then discuss participant recruitment, for interviews and then questionnaires, before providing details of the Country Profiles interviewees to demonstrate expertise required for participation in this research.

3.3.1 Ethics

All interview guides and questionnaires (see: Appendices) began with standard questions regarding informed consent and pseudonymisation of responses, per the conditions of Oxford's ethical approval which was obtained separately for each study. The University of Oxford Central University Research Ethics Committee approval numbers are as follows for each study: CS_C1A_19_017-1 (exploratory study), CS_C1A_20_003 (country profile study), CS_C1A_021_027 (validation study). Institutional ethical approval was particularly important given the sensitive nature of cyber-threats against journalists and the possibility that participants might reveal sensitive personal information in their answers, such as their political affiliations.

The primary ethical consideration of this research concerned the conducting of interviews. Owing to geographical constraints (and those imposed by the COVID-19 pandemic), interviews took the form of voice or video calls. This was challenging for rapport-building, which was necessary to elicit truthful information from interviewees about the sensitive topic of cyber security knowledge and practices.

Every effort was undertaken to approach subjects appropriately and with full transparency in order for interviewees to feel as comfortable as possible in participating. This effort at transparency was intended to ensure that consent to participate was given with a clear understanding of potential risks, including psychological distress that might arise from revisiting traumatic events, such as data breaches, cyber-physical attacks, or legal threats. Prior to their interviews, participants read a detailed information sheet that included notes on data storage, withdrawal from the study, and information about how their identities and comments would be used in written outputs (see: Appendix E for an example participant information sheet). Furthermore, interviewees had the option to speak anonymously or with modified identification in order to assuage concerns about retribution. Interviewees then gave oral consent for their interviews to be recorded. In line with the parameters of this project's institutional ethics approval, audio recordings of interviews were deleted, while written transcripts and notes were preserved. All data has been protected according to UK law.

Following the write-up of interview-based chapters (e.g. Chapters 6 and 7), pseudonymised draft versions were sent to all interviewees for their review before submission for peer-review and publication. Interviewees were asked if they wished for a different job description, or to amend any pseudonymised details. Participants were informed that any future articles using the interview data would not deviate significantly from the use in the given chapter and were asked if they were happy for future work to be submitted for publication without seeking interviewee permission for each article. In the email to which the draft chapters were attached, interviewees were also given a deadline for response, and informed that if they did not respond by this date, their approval would be assumed.

3.3.2 Participant recruitment

3.3.2.1 Recruitment for interviews

This research required semi-structured interviews for the exploratory study (see: Chapter 4) and each country profile (see: Chapters 6 and 7). The niche and interdisciplinary nature of this research meant that all interviewees were necessarily specialists. Purposive sampling (a form of non-probability sampling in which existing networks are utilised to guarantee the inclusion of participants with relevant expertise or experience and therefore to ensure in-depth results)[322] was therefore undertaken in all interview-based studies, with some studies also employing snowball sampling.

3.3.2.1.1 Exploratory study interviewee recruitment

The exploratory study (see: Chapter 4) research questions were premised on the belief that having a heightened awareness of the risks attached to researching high profile topics is likely to cause journalists to adopt defensive strategies. For the exploratory study, potential interviewees were originally selected based on their published work that demonstrated an interest in, or understanding of, cyber security or other high-risk topics that could make them targets of cyber-attacks by well-resourced adversaries.

After selection, these individuals were contacted and asked if they would be interested in participating in the exploratory study. As this study had strict time constraints, only 36 people were contacted, of which 11 positively responded. Interviewees were chosen because of their relevant expertise, so they included journalists, experts in digital security, and executives at media organisations, in order to compare journalists' protective measures with expert protective advice. All interviewees were chosen for their likelihood of being among those who should be best versed in the dangers of the Internet of Things that are specific to journalism, with the objective, if possible, of recording and proliferating their protective procedures to guide other journalists. Section 3.3.2.3 provides demographic information of interviewees.

For the exploratory study, it was necessary to establish the extent to which journalists perceive IoT threats and the protective tools and methods that they feel are currently effective in increasing their cyber security against all perceived cyber-threats (including any from the IoT). Therefore, an interview guide for journalist participants was formulated, with questions phrased as neutrally as possible. 11 semi-structured interviews with members of the media industry were conducted, each lasting on average 45 minutes.

3.3.2.1.2 Country profile interviewee recruitment

For the country profiles, 63 interviews with experts (in the media, relevant legislation, emerging technologies, etc.) were used to supplement a country-specific literature review. Access to a pool of relevant professional contacts enabled purposive sampling of industry experts, threat intelligence experts, and members of the media who have specialisms relevant to each country. To reduce selection bias, approximately 280 experts were contacted. The focus on participants' niche expertise prevented study inclusion criteria from controlling for all potential variables, such as political affiliation. However, the participant pool was supplemented through snowball sampling, by asking interviewees to name other people who are experts in their niche, both who agree and disagree with them. While potential participants from law enforcement and intelligence backgrounds were contacted, the necessity of a low profile in these fields limited the number of relevant participants recruited and precluded some of those

[322] Bourgeault I, Dingwall R and Vries R de (2010) The SAGE Handbook of Qualitative Methods in Health Research. London, UK: SAGE Publications Ltd; Campbell S, Greenwood M, Prior S, et al. (2020) Purposive sampling: complex or simple? Research case examples. Journal of Research in Nursing 25(8). SAGE Publications Ltd: 652–661. DOI: 10.1177/1744987120927206.

contacted from agreeing to be interviewed. Breakdown of interviewees' areas of expertise can be found in section 3.3.2.3.

The inclusion criteria for participation were simply that prospective interviewees were over the age of 18 and had self-professed subject-matter expertise, whether this was relevant to their domestic IoT market, the cyber security of news institutions, or the legal and political threats to journalists and the news industry in one or more of the countries. These criteria were decided because a major aim of these interviews was to discover any cyber security strategies and policies within the press in each country, and to determine their approach to overcoming or mitigating any country-specific legal threats related to the IoT.

Given the novelty of the IoT, the length of someone's time in a specific professional role was not considered to be an indicator of their specialist knowledge of peripheral subjects. Rather, expertise was judged qualitatively. This is because even if an interviewee had only worked in their current role for a year, they either had academic or professional experience in other relevant roles or it was deemed that their current role was so intensive and required such a high level of expertise they are uniquely qualified to speak on the topic.

3.3.2.2 Recruitment for questionnaires

3.3.2.2.1 Exploratory study questionnaires recruitment

For the cyber security expert questionnaire part of the exploratory study (see: Chapter 4), all cyber security expert respondents were either invited via academic mailing lists or via social media posts, which requested participants who were "involved in cyber security."

The online media expert survey that supplemented the exploratory study interviews was sent by the AIB to a number of their journalist contacts, regardless of demonstrated interest in cyber security or the Internet of Things. This is because the prevalence of the IoT and its massive generation of data that are made accessible to law enforcement agencies under national security justifications, mean that all journalists are likely to be impacted by these technologies, even if they are not aware of it.[323]

3.3.2.2.2 Validation study survey recruitment

Inclusion criteria for survey respondents for the validation study were that they were above the age of 18 years old, could give informed consent, and were experts (i.e. had worked in some capacity for over one year) in the spheres of: (1) journalism, (2) IoT and cyber security, (3) state capabilities, whether these are legal, political, or technological powers. The breadth of each category was due to the variety of ways in which a particular person may have expertise or experience in relevant security issues.

To minimise selection bias, a greater number of experts were contacted for recruitment than were estimated to be necessary for each survey. Experts were recruited through purposive sampling, based on institutional affiliations (e.g. to journalism departments), relevant publications, and a pool of contacts found through professional and social-media-based networks. Participants were recruited through a variety of ways: anyone who had previously participated in this thesis research and agreed to be contacted

[323] Swinford S (2013) Leveson could have 'chilling effect' on journalism, Information Commissioner warns. *The Telegraph*, 7 January. Available at: https://www.telegraph.co.uk/news/uknews/leveson-inquiry/9786404/Leveson-could-have-chilling-effect-on-journalism-Information-Commissioner-warns.html (accessed 9 September 2019); Lowenthal T (2015) Surveillance forces journalists to think and act like spies. Available at: https://cpj.org/2015/04/attacks-on-the-press-surveillance-forces-journalists-to-think-act-like-spies.php (accessed 9 September 2019).

again was asked to complete any of the surveys and to distribute them to their relevant networks. Additionally, pre-existing networks that were tailored to each expert group were tapped (e.g. the AIB and the Journalist's Resource newsletters for media experts, the Security Queens newsletter and PETRAS networks for the cyber security surveys). Further, recruitment utilised personal professional networks, both directly and via social media (e.g. LinkedIn and Twitter), to maximise their reach. The pool of participants was further expanded through snowball sampling.

Due to the secretive nature of experience in states' capabilities, it was more difficult to recruit experts for this survey. Participant recruitment started by leveraging three types of contact: previous colleagues with this expertise, attendees of Harvard Kennedy School's Executive Education Cyber Security programme, and threat intelligence experts who were sponsors of the cyber security doctoral programme at the University of Oxford.

3.3.2.3 Breakdown of Country Profiles interviewees' areas of expertise

Tables 1 and 2 summarise the interviewees' jobs and expertise, whilst Table 3 provides a full list of the country and subject expertise of each interviewee.

Job categories	**Countries**				
	Taiwan	UK	US	Australia	**Total interviewees who cover these categories**
Lawyer	1	5	3	2	11
Academic	4	10	14	7	35
Journalist	4	3	0	4	11
NGO	1	1	5	0	7
Independent researcher	1	1	1	1	4
Consultant	1	5	3	3	12
Total interviewees with expertise in each country	11	22	24	14	-

Table 1: Job categories for Country Profile interviewees

Expertise categories	**Countries**				
	Taiwan	UK	US	Australia	**Total interviewees who cover these categories**
Journalist security	1	2	4	5	12

IoT threats and/or mitigations	0	8	9	4	21
Cyber policy and regulation	3	6	4	8	21
Politics & law related to press freedom	8	12	13	8	41
Total interviewees with expertise in each country	11	22	24	14	-

Table 2: Expertise categories for Country Profile interviewees

Interviewee subject matter expertise and years of experience:

Interviewee pseudonym	**Countries covered**	**Expertise category**	**Years of experience**
P1	UK	Politics & law related to press freedom	25
P2	UK	IoT threats and/or mitigations	20
P3	Australia	IoT threats and/or mitigations; Cyber policy and regulation	2
P4	UK	Politics & law related to press freedom	6
P5	Taiwan	Politics & law related to press freedom	25
P6	US	IoT threats and/or mitigations	8
P7	US	Cyber policy and regulation	17
P8	US	IoT threats and/or mitigations	10
P9	US	Journalist security; Politics & law related to press freedom	20
P10	UK	IoT threats and/or mitigations	10
P11	UK	Politics & law related to press freedom	45
P12	UK, US, Taiwan	Journalist security	7
P13	US	Journalist security; Politics & law related to press freedom	5
P14	Australia	Cyber policy and regulation	13
P15	UK	Politics & law related to press freedom	11
P16	UK	Journalist security	25
P17	UK, US	Cyber policy and regulation; IoT threats and/or mitigations	21
P18	UK	IoT threats and/or mitigations; Cyber policy and regulation	7
P19	US, Taiwan	Cyber policy and regulation	25
P20	UK	IoT threats and/or mitigations; Cyber policy and regulation	11

P21	US	Politics & law related to press freedom	4
P22	UK, Taiwan	Politics & law related to press freedom	24
P23	UK, US	Politics & law related to press freedom	25
P24	US	Politics & law related to press freedom	15
P25	Taiwan	Politics & law related to press freedom; Cyber policy and regulation	10
P26	UK	Politics & law related to press freedom	14
P27	Australia	Politics & law related to press freedom; Journalist security	26
P28	Australia	Politics & law related to press freedom; Cyber policy and regulation	8
P29	Taiwan	Politics & law related to press freedom	25
P30	Australia, UK	Cyber policy and regulation; Politics & law related to press freedom	6
P31	UK	IoT threats and/or mitigations; Cyber policy and regulation	4
P32	US	Politics & law related to press freedom	6
P33	Australia	Cyber policy and regulation; IoT threats and/or mitigations; Journalist security	16
P34	US	Politics & law related to press freedom	16
P35	US	Politics & law related to press freedom	4
P36	Australia	Cyber policy and regulation; IoT threats and/or mitigations	14
P37	US	IoT threats and/or mitigations	20
P38	Taiwan	Politics & law related to press freedom	4
P39	Taiwan	Politics & law related to press freedom	12
P40	Australia	Politics & law related to press freedom; Journalist security	8
P41	UK	IoT threats and/or mitigations; Cyber policy and regulation	38
P42	Australia	Politics & law related to press freedom	30
P43	UK	Politics & law related to press freedom	8
P44	UK, US	Politics & law related to press freedom	15
P45	UK	Politics & law related to press freedom	21
P46	US	IoT threats and/or mitigations; Politics & law related to press freedom; Journalist security	9
P47	US	Politics & law related to press freedom	15

P48	Australia	Cyber policy and regulation	15
P49	Taiwan	Cyber policy and regulation	5
P50	UK	IoT threats and/or mitigations	10
P51	US	IoT threats and/or mitigations	26
P52	Australia	Politics & law related to press freedom; Journalist security	6
P53	UK	Politics & law related to press freedom	8
P54	US	Politics & law related to press freedom; IoT threats and/or mitigations	3
P55	Australia	Politics & law related to press freedom; Journalist security	13
P56	Australia	Politics & law related to press freedom	8
P57	US	Cyber policy and regulation	20
P58	Taiwan	Politics & law related to press freedom	25
P59	US	IoT threats and/or mitigations	10
P60	Australia	IoT threats and/or mitigations; Cyber policy and regulation	5
P61	US	Politics & law related to press freedom	42
P62	US	IoT threats and/or mitigations	10
P63	Taiwan	Politics & law related to press freedom	3

Table 3: Country Profile interviewees' subject matter expertise and years of experience

3.3.2.4 Breakdown of Validation Study respondent expertise

Survey respondents for Chapter 8's validation study were not assigned participant identifiers, as the surveys did not request enough qualitative responses to require discussion of individual responses. Further, responses were quantitatively analysed and used to populate and refine the contents of the framework of countermeasures.

Tables 4, 5, and 7 outline the self-stated expertise and experience of the participants of the cyber security and states' capabilities surveys, whilst Table 6 refers to the media survey and includes the category of media experience of each respondent.

Cyber security (threats-countermeasures matching) survey respondents' expertise:

Self-stated expertise	**Years of experience**
I currently work in cyber security as a penetration tester. I also have an undergraduate degree in cyber security.	2
Worked with multinationals and governmental organisations to secure their networks against internal and external threats. Actively worked to compromise the digital accounts of various individuals and companies in order to discern the weaknesses in their security.	11.5

Offensive cyber	10
I help develop standards for IoT and IoMT security and manage security standards	20

Table 4: Cyber security (threats-countermeasures matching) survey respondents' expertise

Cyber security (function and feasibility) survey respondents' expertise:

Self-stated expertise/experience	**Years of experience**
Employed for over a decade as a penetration tester providing external cyber security expertise to multinational companies and various public sector bodies. Long-serving member on Hunted, with experience compromising IoT devices for surveillance and sensitive information retrieval purposes.	~12
I work in cyber security as a penetration tester. I also have a degree in cyber security	2
Offensive cyber	10
Cyber policy	6

Table 5: Cyber security (function and feasibility) survey respondents' expertise

Media survey respondents' expertise:

Media role umbrella (category of media experience)	**Years of experience**
Business/Corporate/Commercial/Organisational Stakeholders	45
Editorial/Narrative Producers (inc. Programme Editors)	20
Editorial/Narrative Producers (inc. Programme Editors)	40
Editorial/Narrative Producers (inc. Programme Editors)	10
Editorial/Narrative Producers (inc. Programme Editors)	9
Editorial/Narrative Producers (inc. Programme Editors)	7
Editorial/Narrative Producers (inc. Programme Editors)	18

Table 6: Media survey respondents' expertise

States' capabilities survey respondents' expertise:

Self-stated expertise/experience	**Years of experience**
I have worked with a number of state agencies both in an education and operational capacity	10+
I run a cyber intelligence business that looks into these areas	10
Worked in National Criminal and Military Intelligence Roles	20
I worked as a cyber investigator and intelligence lead for UK law enforcement	15
I do not have direct practical knowledge of state interception/exploitation capabilities. My understanding is based	7

on c.5 years covering state intelligence activity in an analytical/editorial role on a UK-based magazine and two years of PhD study on cyber security.	

Table 7: States' capabilities survey respondents' expertise

3.4 Data collection

3.4.1 Exploratory study interview procedure

For the exploratory study, it was necessary to establish the extent to which journalists perceive IoT threats and the protective tools and methods that they felt were currently effective in increasing their cyber security against all perceived cyber-threats (including any from the IoT). 11 semi-structured interviews with members of the media industry were conducted, each lasting on average 45 minutes. As this was an exploratory study, the scope of the IoT technologies covered was not narrowed beyond specifying to participants that the study was not concerned with established devices – i.e. smart phones, desktop computers, laptops, and tablets. If participants mentioned aspects of "smart cities" (i.e. systematic use of IoT technologies to make an urban environment more "sustainable, livable, secure, […] green or connected,")[324] the interviewer did not shift their focus to commercially available IoT technologies.

Additionally, the interview technique was adapted to prevent confusion in participants who may not be familiar with the concept of the IoT. This was done in line with guidance published by researchers at University College London (UCL), which included a list created by UCL researchers to outline kinds of new internet-enabled smart devices that would expand the attack surface of vulnerable groups that was presented to participants, if participants indicated unfamiliarity with the definition of IoT.[325] This meant that the interviewer often used the more colloquially accepted word "smart" when asking about IoT devices, because pre-study discussions held with members of the media industry found that journalists are likely to see the phrase "Internet of Things" as a marketing gimmick, rather than it furthering their awareness of the sociological issues associated with new internet-enabled devices. The UCL source was chosen because it is not a biased definition, while still capturing the analytical capabilities and interconnected nature of IoT devices in a way that has been designed to be understandable to vulnerable groups of lay people.

Once participants confirmed that they understood the given definition of IoT, questions turned to what, if any, concerns they have about these sorts of devices and whether they feel that their attitudes and behaviours regarding these devices are typical of journalists that they know. Then, interviewees were asked about their knowledge of examples of any cyber-attacks conducted against journalists and potential perpetrators and motivations of these threats, as well as focusing on interviewees' beliefs regarding exploitation of IoT devices to threaten journalists' work, wellbeing, and sources. For comparison, interviewees were then questioned about their experience of non-cyber threats and whether they see IoT threats as comparable, given the increased potential for attacks to jump from the cyber realm into the physical world. Following this section, interviewees were asked about their personal cyber security strategies and whether they have any relevance to perceived IoT threats.

[324] Arroub A, Zahi B, Sabir E, Sadik M (2016) A literature review on Smart Cities: Paradigms, opportunities and open problems. In: 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), October 2016, pp. 180–186. DOI: 10.1109/WINCOM.2016.7777211.

[325] UCL STEaPP (2018) Tech Abuse: How Internet-connected Devices Can Affect Victims of Gender-based Domestic and Sexual Violence and Abuse. July. London: UCL. Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/gender-iot-tech-abuse.pdf (accessed 9 September 2019).

The penultimate section of the interview guide acknowledged the many examples of journalists being subject to surveillance, censorship and intimidation by governments and law enforcement agencies, including in democratic states. It questioned participants about their personal encounters with governments and law enforcement agencies' Internet of Things exploitative capabilities as they relate to participants and their work, but it was reiterated that participants were under no obligation to answer any questions with which they did not feel comfortable. Finally, to end the interview with a more positive outlook and to avoid causing participants stress, they were asked about their expectations for the future of journalists' cyber security and whether they had any suggestions for whose responsibility it might be to improve journalists' understanding of threats through IoT devices in practice. Interviews were ended by asking for any additional questions or comments, or aspects of journalists' cyber security that participants feel are disproportionately overlooked.

3.4.2 Country Profile interview procedure

For the country profiles, the objective was to ascertain the current state of affairs regarding the IoT and press freedom and security, including state capabilities, in the United Kingdom, the United States, Taiwan and Australia (see: section 3.2.4.1 for justification of the case study method as part of this research). Depending on interviewees' specialisms, the discussion covered at least three subtopics (detailed below); interviewees were notified of which ones in advance via their Participant Information Sheet. All 63 semi-structured interviews were held remotely and lasted on average one hour.

For media experts, subtopics were threat intelligence sharing methods between news organisations and/or journalists, geopolitical pressures and national security tensions regarding the media, and any other threats to the maintenance of a free press in these countries. For experts in state capabilities, subtopics discussed relevant data protection/retention or cyber security legislation, laws regarding ambient/targeted surveillance, and the technical capabilities of law enforcement, security, and intelligence agencies. Interviewees discussing the IoT in each country were asked about the domestic market for emerging technologies (particularly the IoT), IoT security and privacy norms and standards, and IoT regulation, both proposed and enacted (including perspectives in government oversight in this regard).

Prior to initiating interviews, a flexible interview guide was designed to elicit longform answers for analysis to create analytically powerful "thick data."[326] Using the funnel technique, questions became more specific as the interview went on.[327] The interview guide was split into three sections: (1) The IoT, (2) press freedom and security, and (3) legal and technical surveillance capabilities of the state. These three topics were further used to develop four different surveys that informed the content of the framework in Chapter 8: two cyber security surveys, a media survey, and a survey on state capabilities. A full list of interview questions can be found in Appendices H, I, J, and K. As with the exploratory study interviews,

[326] Smets A and Lievens B (2018) Human Sensemaking in the Smart City: A Research Approach Merging Big and Thick Data. *Ethnographic Praxis in Industry Conference Proceedings* 2018(1): 179–194. DOI: 10.1111/1559-8918.2018.01203.
[327] Cannell CF, Miller PV and Oksenberg L (1981) Research on Interviewing Techniques. Sociological Methodology 12. [American Sociological Association, Wiley, Sage Publications, Inc.]: 389–437. DOI: 10.2307/270748.

for country profile interviewees who were unfamiliar with the IoT, the UCL definition was provided,[328] and participants were directed to the published exploratory study paper for this thesis.[329]

3.4.3 Piloting the questionnaires for validation of framework content

Given the depth of the surveys needed to create the framework, a pilot study was important to understand whether their length would be overwhelming to respondents, and whether they were framed correctly to get useful answers. This pilot study, conducted in February 2022, involved using purposive sampling to recruit two people for each questionnaire, requesting that they complete their assigned questionnaire, and then having a call with each of them to debrief and enable understanding of their thoughts and feedback. Each respondent was asked (1) how long it took them to complete the survey, (2) whether they had any edits regarding question phrasing or formatting, (3) what, if anything, they thought should be added or removed from the survey, and (4) if they anticipated any limitations or challenges to getting survey responses.

All four surveys were designed to first gain the participants' informed consent, then establish professional experience and expertise. Further, they all included a section explaining the framework, in that it suggests 20 countermeasures that were found through 70+ interviews with experts, as well as reviewing academic literature and news articles. These countermeasures cover behaviours, actions and long-term goals that are likely to protect against and mitigate threats to the media from the Internet of Things. Each survey set out what participants needed to do in the following pages. In their final sections, all surveys asked open-ended questions regarding participants' thoughts on the content of the survey, and were thanked for their responses.

The online questionnaires included various different question types (e.g. open-ended questions, closed yes/no, scale and rank questions). This variety provided both thick and more easily statistically analysable material, to enable assessment of areas of potential improvements to the framework. Where possible, the surveys relied on multiple choice questions, in order to maximise the completion rate. Questions were designed to avoid soliciting personal information, other than an initial section requesting basic biographical information to demonstrate that participants were experts whose opinions would constitute useful validation of the framework. To further provide incentive, IP addresses were not recorded, which was disclosed in the informed consent portion of the survey. The surveys were hosted by 'Bristol Online Surveys,' which is compliant with all UK data protection laws and university policy.

The function and feasibility survey, and the states' capabilities survey were comprised of matrices, to minimise the amount of time needed to complete them, while eliciting unambiguous responses that could be compared. In contrast, the media expert survey and the threats-countermeasures matching survey included open-ended questions, to gather qualitative data.

For the Media Expert survey, it took the first respondent 35 minutes because some of the questions were not formatted as "optional" and so the respondent had to fill out every box, even when they had no additional thoughts. They recommended that all "What, if anything, would you change about the phrasing

[328] UCL STEaPP (2018) Tech Abuse: How Internet-connected Devices Can Affect Victims of Gender-based Domestic and Sexual Violence and Abuse. July. London: UCL. Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/gender-iot-tech-abuse.pdf (accessed 9 September 2019).

[329] Shere ARK, Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.

of this countermeasure? Why? [text answer]" questions be made optional, a suggestion that was accepted for the official survey roll-out. The second respondent took 45 minutes to complete the survey, and had several suggestions, most of which were implemented. These were intended to make the survey more accessible to non-academic media experts, and included recommendations to: remind participants what is included in the definition of the IoT used for this research (a note was added to every survey page); remove any academic jargon and break sections of information down to make the survey framing easier to read (this was done); and elaborate on why this research is necessary so that participants feel invested in the cause and are more likely to complete all questions (this was done both in the survey introduction and in the participant recruitment email template).

Regarding the Feasibility and Function (cyber security) survey, one participant noted that the "stronger passwords" countermeasure was explicitly both individual and collective and so there are multiple potential answers for feasibility. Unfortunately, the survey platform did not allow a multiple-choice-single-answer question to be converted to a multiple-choice-multiple-answers question. It was therefore necessary to weigh up the benefits of remaking the survey to just change the type of feasibility question, which would have increased the time-taken to complete the survey and so lowered the rate of response. It was decided to keep the current survey structure and to instead take this limitation regarding nuance into account when putting the data into the framework itself, and in future research. This respondent noticed some spelling errors, which were removed before the official survey roll-out. Notably, the first participant also thought the function of countermeasure categories could be limiting, but agreed that it would be useful to have clearly stratified countermeasures, so more information was included in their framing to clarify the different labels and how they might apply. This respondent took an hour to complete the survey, while the second respondent took under 30 minutes and had no additional concerns.

For the Threats Matching (cyber security) survey, the first participant felt it would be important to emphasise that questions were asking for the "most" relevant countermeasures for each threat, which was done. They further suggested that the options for countermeasure disadvantages were vast, so it would be important to decide if they should relate to individual end-users or to organisations, which was a consideration that was deferred until all responses were received, and to parse during the analysis phase of the study, so that it would not affect answers collected, but rather the data input in the framework. The first respondent took roughly 90 minutes to complete the survey, although they acknowledged that they had taken a break while filling out the questions. The second participant took an hour to submit their responses and had no further edits to suggest. As a result, the introduction of the survey was amended regarding the time-taken to complete all questions.

The States' Capabilities survey was divisive, with one pilot participant claiming that they could not answer the whole questionnaire as questions covered too many topic areas, which led to refining the list of possible participants and networks to use for recruitment. The second participant finished the survey in 40 minutes and found it very comprehensive, offering to help distribute the survey to their professional contacts.

3.5 Data processing

3.5.1 Thematic analysis of qualitative data

Chapters that included qualitative data collection through participant studies (see: Chapters 4, 5, 6, 7 and 8) involved thematic analysis of study data. By identifying any recurring responses and positions from the interviews and qualitative survey responses, themes were established that could be compared and contrasted. This was done by transcribing interviews and long-form survey responses, before employing

Erlingsson and Brysiewicz's qualitative content analysis techniques.[330] Their article describes a 5-step process for consolidating themes by abstracting qualitative data: (1) identifying direct quotes, (2) rephrasing them, (3) creating a relevant and brief "code" to label the chosen quotes, (4) grouping similar codes into the same category based on shared context, and (5) clustering categories under any overarching themes that were relevant to each chapter's objectives. These themes would then form the basis for the primary analysis and discussions in this research.

3.5.1.1 Comparative case study analysis for the Country Profiles

In total, 63 interviews were conducted for the country profiles, with some individuals participating in relation to their expertise in more than one of the countries. This resulted in 11 expert interviews that covered Taiwan, 14 for Australia, 22 for the UK, and 24 for the US. These transcripts were coded using NVivo and thematically analysed in accordance with grounded theory.[331]

First, each transcript where the interviewee discussed multiple countries was manually input (coded) into a different 'case' per country, so that when searching for themes for country 1, country 2's details could not skew the results. Second, every interviewee was manually assigned one or two job categories from the following list of options: lawyer, academic, journalist, NGO, independent researcher, or consultant. This list of options was created from the self-reported interviewee data. They were manually assigned a category summarising their area of expertise, demonstrating a mix of topics covered for each country: (1) Journalist security, (2) IoT threats and/or mitigations, (3) cyber policy and regulation, and (4) politics and law related to press freedom. These categories were developed from interviewees' self-reports when choosing which expertises to speak on.

Following these categorisations, the 'cases' were searched and manually coded using NVivo to find content relating to each country; the full codebook can be found in section 3.5.3. These codes were then manually grouped (axial coded) into themes.[332] The overarching themes that interview questions explored in each country are the following: press freedom, the IoT market (including regulation and supply chain considerations), IoT implications for journalists, and any existing cyber protections and mitigations undertaken by journalists and news organisations (see: Appendix F).

These were the thematic categories that guided the semi-structured interviews. New themes were then developed from the results of these interviews to understand the threats interviewees were most concerned about from the IoT, according to an overall assessment of the priority given to each risk factor by interviewees collectively, along with the three axes specified in Bartlett and Vavrus' system for comparative case studies.[333] The dominant theme was legal threats, which therefore became the focus of Chapter 6. The additional themes identified of threats from the geopolitical landscape and threats from lack of current protective mechanism are discussed in Chapter 7.

Aligning with Hesse-Biber, Yin and Eisenhardt's thoughts on writing up mixed methods results, the presentation of Chapters 6 and 7 integrates results and discussion, combining secondary literature into

[330] Erlingsson C and Brysiewicz P (2017) A hands-on guide to doing content analysis. *African Journal of Emergency Medicine* 7(3): 93–99. DOI: 10.1016/j.afjem.2017.08.001.
[331] Braun V and Clarke V (2013) Successful Qualitative Research: A Practical Guide for Beginners. London, UK: SAGE Publications Ltd.
[332] Braun V and Clarke V (2013) Successful Qualitative Research: A Practical Guide for Beginners. London, UK: SAGE Publications Ltd.
[333] Bartlett L and Vavrus F (2016) Rethinking Case Study Research: A Comparative Approach. New York: Routledge. p.35.

the analysis of primary research, i.e. interview responses.[334] This provides context supporting interviewee responses and demonstrates that they are not just anecdotal, enabling readers to understand how this data underpins the range of countermeasures to IoT threats to the media presented in Chapter 8.[335]

As the majority of media interviewees considered legal threats to be their most urgent concern, Chapter 6 focuses on challenges associated with legislation and regulation, documenting the ways in which they facilitate some of the threats described in Chapter 5. Within this theme, Chapter 6 highlights the specific categories of law that increase IoT risk to the press: carve-outs in laws, surveillance laws, bulk data collection, insufficient journalist legal protections, unfit IoT regulation, incompetent data protection, and cyber-physical criminal threats exacerbated by poor IoT regulation. This correlates with Barlett and Vavrus' first axis, "horizontally" contrasting the impact of subnational actors (such as law enforcement agencies and media organisations) on IoT threats to press freedom. The chapter groups those legal and regulatory threats stemming from domestic government overreach and those arising from domestic government inadequacy, to provide context for their origins that will be considered in the creation of Chapter 8's countermeasures.

Chapter 7 used the second axis of Barlett and Vavrus' method to "vertically" compare non-governmental factors that influence IoT threats to the press, primarily geopolitical supply chain considerations (at the international level) and media organisational politics (at the organisational level). Finally, across both chapters, "a transversal comparison" per the third axis discusses the evolution of the "political, economic, social, and cultural context" in each country to determine areas of generalisability and context-specific detail. The use of these methods therefore enabled these chapters to comparatively analyse the context of press freedom and IoT uptake and threats across countries. This enables the framework for journalist protections against IoT threats (see: Chapter 8) to be applicable across the four democracies.

3.5.2 Conceptual models

3.5.2.1 Compiling the Environmental IoT Model

Chapter 5 includes a conceptual model organising the consumer IoT according to environmental categories in which journalists may interact with devices. Having a tool to categorise components of the IoT allows identification of both assets and vulnerabilities, as recommended by NIST.[336] The objective of this model is therefore not to be an exhaustive taxonomy of all IoT devices available on the market, but rather to demonstrate that the IoT is ubiquitous, not idiosyncratic to a specific locale, and common enough to merit subsequent research into their threats to journalists.

The four overarching categories that were chosen for the conceptual model organising the consumer IoT are: (1) *private homes*, (2) *public spaces*, (3) *workplace*, and (4) *wearable*. These categories were created by coding thematically the consumer IoT devices and situations mentioned by over 70 interviewees (see: Chapters 4, 6 and 7) using NVIVO. These categories were then further refined through secondary source

[334] Hesse-Biber, SN, & Johnson, RB (eds) 2015, The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry, Oxford University Press, Incorporated, Oxford. Available from: ProQuest Ebook Central: pp. 84, 198-200.; Yin RK (2009) Case Study Research: Design and Methods. Fourth. Applied Social Research Methods Series. California, USA: SAGE Publications, Inc; Eisenhardt KM (1989) Building Theories from Case Study Research. *The Academy of Management Review* 14(4). Academy of Management: 532–550. DOI: 10.2307/258557.

[335] Ezzy D (2002) Chapter 6: Writing about qualitative data. In: Qualitative Analysis: Practice and Innovation. London, UK: Routledge, pp. 138–163; Hartley J (2004) Case Study Research. In: Cassell C and Symon G (eds) *Essential Guide to Qualitative Methods in Organizational Research*. London: SAGE Publications Ltd., pp. 323–333. DOI: 10.4135/9781446280119.

[336] Keller, N.: Identify: NIST Cybersecurity Framework, https://www.nist.gov/cyberframework/identify, last accessed 2020/09/11.

analysis of existing IoT taxonomies (see sources mentioned throughout this chapter). They were subsequently augmented through news and other secondary sources that describe specific examples of IoT functionalities and situations.

Categories were chosen to be as broad and clear as possible. This allows cross-referencing, such as to enable a journalist to check both the *private homes* and *workplace* categories to give them an idea of which devices have been accumulated by members of their household if they are working from home or, for example, if the journalist is working from a hotel room or a college bedroom. Further, the *wearable* category is intended to always be viewed in addition to location-specific environments. As in the rest of this thesis, the scope of the IoT does not include legacy devices such as routers, phones, laptops, tablets, or desktop computers, all of which are excluded from this model.

The decision to use environment as the primary basis for grouping devices was taken to demonstrate to journalists with no previous knowledge of the IoT both the scale and prevalence of devices. The global consumer IoT market is growing and diversifying at such a rate that categorising all existing devices would be both futile and unhelpful. As one interviewee, a managing security consultant in the private sector, said, "in a few years, for example, there will probably be as many medical devices as there are conditions to treat."[337] However, the motivation behind the creation of this model was to give readers an idea of where a journalist might be most likely to encounter a device and therefore of how much control they may have over devices, depending on the location. The benefit of classifying devices by environments is that, even as technologies change, they will occupy the same environments. Thus, this model may be used for on-going identification of devices, on both individual and organisational levels. This function can be combined with the threats categorisation (see: Chapter 5) to evaluate immediate threat landscapes.

Regarding definitions of each of the main themes: *Private homes* include a journalist's own residence, as well as any other abodes that they may visit. Within the *private homes* category, there are three subcategories: (1) *household management/utilities*, (2) *leisure*, and (3) *security*. This subcategorisation by device purpose is intended to allow for variation in home environment as, for example, an individual residing in a flat-share is likely to have access to different facilities to someone living in a mansion, but they may have similar patterns of life.

The inclusion criteria for the *private homes* category are that the devices are used within a private residence for the purposes embodied by the subcategories: *household management/ utilities, leisure,* or *security*. Such devices may overlap with those that fall under the *public spaces* or *workplace* categories. However, they must not qualify for the *wearable* category, or they should be included there.

Public spaces range from *outdoor public areas*, e.g. parks, where one might find lighting systems and CCTV cameras, to *indoor public areas*, e.g. shops, where one might encounter smart television screens and speakers. This category includes transient areas, such as *transport*, where one might encounter both fixed sensors and those hosted on other people (and animals) who are passing through, on public transport (underground lines, trains, etc.), semi-public transport (ride-sharing services, commercial aeroplanes, etc.), and private transport (personal cars, bicycles, etc.). Challenging areas within this theme included elements like ride-sharing services, which are private vehicles that are not owned by the people in the backseat and are subject to claims by the company through which the rides are arranged. Additionally, regarding different parts of *indoor public areas* for example, restaurants may have smart White Goods, but these may not be located in consumer areas. Still, this potential has been included in order to err on

[337] Interviewee: Participant10

the side of transparency so that users are aware of the ubiquity of such devices and their integration into different places.

The inclusion criteria for the *public spaces* category are that the devices are used within its environmental subcategories: *transport, outdoor public areas,* and *indoor public areas*. Such devices may overlap with those that fall under the *private homes* or *workplace* categories. However, they must not qualify for the *wearable* category, or they should be included there.

The *workplace* is designed to encompass specific types of devices for professional and academic environments, the latter of which includes universities, as well as schools for minors that journalists may encounter if they have caring responsibilities. These types of technologies may be present in home offices as well, but are most probably found in large buildings built for these specific purposes, especially infrastructural embedded devices like smart whiteboards.

The inclusion criteria for the *workplace* category are that the devices are used within academic or office-based professional environments for the purposes embodied by the subcategories: *waiting/meeting room entertainment, utilities,* or *security*. Such devices may overlap with those that fall under the *private homes* or *public spaces* categories. However, they must not qualify for the *wearable* category, or they should be included there.

Areas that presented a challenge to subcategorisation included devices containing access tokens or portable devices with GPS trackers, both of which could fall into all subcategories. For example, a gym used by residents of an apartment complex might require a digital access key, hosted on a smartwatch that tracks location. This issue was resolved by the *wearable* category.

The inclusion criteria for the *wearable* category are that the devices are ingested, implanted, or otherwise worn on an individual. Devices that are portable but that are not designed to be used while being carried on a single person's body are excluded from this category.

3.5.2.1.2 Presentation of the Environmental IoT Model

The tables used to structure and determine the contents of the model each have three columns, with increasing levels of detail (see: Chapter 5). First, categorising devices according to environment; second: subcategories classified according to device purpose; and a third column noting generalised device capabilities. The aim of this structure was to make the model useful to journalists, media lawyers and journalistic security teams, who may all need to know different information to conduct relevant risk assessments. To provide this overview, device capabilities used were chosen from Sturgess *et al.,* although app capabilities have not been included.[338] The global consumer IoT market is growing and diversifying at such a great rate that categorising all existing devices would be both futile and unhelpful.

To present the model in a way that was clear to lay viewers, simplified Venn diagrams were designed to demonstrate the ubiquity of the IoT and illustrate the overlaps between the devices that exist in different environments in an easily understood way.[339] To create a Venn diagram, as many details of devices as

[338] Sturgess J, Nurse JRC, Zhao J. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In: 2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018 [Internet]. London, UK: Institution of Engineering and Technology; 2018 [cited 2020 Sep 11]. p. 37 (8 pp.)-37 (8 pp.). Available from: https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0037.

[339] Barstow BA, Vice J, Bowman S, et al. (2019) Examining perceptions of existing and newly created accessibility symbols. *Disability and Health Journal* 12(2): 180–186. DOI: 10.1016/j.dhjo.2018.11.012.

possible were collected, to reach "a critical mass of material."[340] These were then thematically grouped by considering the potential for their interaction with journalists. Both tables and Venn diagrams were used to ensure that information could be conveyed either as extensively or as concisely as possible. This allows journalists and other members of the news media to choose which resource to use, depending on the time available.

3.5.2.2 Creating and compiling threat models for the threat categorisation

The threats categorisation (see: Chapter 5) involves modelling IoT-related threats to journalists, informed by a variety of sources. These include news articles, grey literature such as commercial and NGO reports, interviews with experts on both the IoT and journalist security, and academic literature on the capabilities of consumer IoT devices. All categories were created by compiling information on potential vulnerabilities and associated exploitation opportunities from academic studies into IoT threats and news sources discussing cyber-attacks on the press. The key inclusion criterion was that current feasibility of the threats must have been evidenced in academic and news materials. The categories were subsequently refined using thematic analysis and by eliminating any threats that were insufficiently relevant to the consumer IoT, then by grouping the remaining nineteen threats into overarching categories.

3.5.2.2.1 Threat modelling approach

A threat model categorisation system is useful for demonstrating the interlinked nature of different threats from the same system, and as a conceptual foundation for organising emerging threats within an existing framework.[341] The categorisation discussed in this section builds on the IoT device model presented earlier. It begins with an understanding of the different environments in which journalists interact with the IoT, and establishing ways in which the devices found in those environments could pose threats to journalists. This is in line with the Electronic Frontier Foundation's description that "coming up with a set of possible threats you plan to protect against is called threat modelling or assessing your risks."[342]

This thesis views threat modelling as a process with the objective of systematically organising threats from a given technology and the impacts they would have against a specific population. This builds on Torr's foundational article on threat modelling describes it as the creation of a "living document both to describe the component's security-relevant design points and record the findings of the threat-modelling process."[343] This approach utilises the work of Xiong and Lagerström who undertook a systematic review of cyber security threat modelling literature, cited Uzunov and Fernandez: "threat modelling is a process that can be used to analyse potential attacks or threats, and can also be supported by threat libraries or attack taxonomies."[344]

[340] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. p. 131.

[341] Fruhlinger J. Threat modeling explained: A process for anticipating cyber attacks [Internet]. CSO Online. 2020 [cited 2020 Sep 11]. Available from: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html

[342] Electronic Frontier Foundation. Threat model [Internet]. Surveillance Self-Defense. 2020 [cited 2020 Sep 11]. Available from: https://ssd.eff.org/en/glossary/threat-model

[343] Torr P. Demystifying the threat modeling process. IEEE Secur Priv. 2005 Sep;3(5): p. 66.

[344] Uzunov AV, Fernandez EB. An extensible pattern-based library and taxonomy of security threats for distributed systems. Comput Stand Interfaces. 2014 Jun 1;36(4): pp. 734-747; Xiong W, Lagerström R. Threat modeling – A systematic literature review. Comput Secur. 2019 Jul 1;84: p. 56.

Xiong and Lagerström note that threat modelling can be used in three different ways.[345] This categorisation aims to do the first of these, i.e. to make a contribution to threat modelling by introducing a new method of threat model that is specific to threats to journalists. As with most existing threat models in cyber security, this was coded manually, given the novel nature of focusing on journalists as the subject population.

There are already established methods for threat modelling in cyber security, such as the MITRE ATT&CK framework and STRIDE, which was used by Hoffman for her IoT threat modelling.[346] Given the interdisciplinary nature of this project, such information-security-centric methods were deemed to be too restrictive and not accessible enough to people with limited security experience. Both named examples focus on attacker actions and, while STRIDE touches upon consequences of its component threats, it does not emphasise potential physical repercussions, which are relevant to the IoT. Like STRIDE, the method of threat categorisation in Chapter 5 is not designed to be as exhaustive as a taxonomy; rather, it is intended to be an interactive aid for journalist security training, built upon as members of the media engage with this threat modelling exercise, so that more subcategories and hypothetical consequences can be added over time. However, journalists process information in more linear and narrative forms, making technically-focused methods less helpful for explaining the ways in which IoT threats could manifest specifically against journalists.[347]

The threat modelling method used in Chapter 5 therefore relies on the creation of scenarios, similarly to those listed by the Australian organisation, 'Privacy for Journalists.' Their threat modelling system for conventional cyber threats to information includes noting who the likely adversary is and what their objective is, how they can achieve this and, building on those points, how journalists can defend themselves.[348] Additionally, an oft-cited blogpost resource entitled "Why every journalist should have a threat model (with cats,)"[349] which aims to inform journalists of the realistic risks associated with their work, including legal threats and some limited physical threats also helped contextualise the methodology used. Another resource also recommends threat modelling to journalists as the first stage of their security analysis when working on a given story.[350] All three of these materials are excellent starting points for journalists with no previous experience of technological risk assessments. However, although the pieces touch upon physical and legal threats, examining them is beyond their scope. Further, none of them take into account the expanded threat landscape as a result of the increasing prevalence of the IoT (see: Chapter 2).

[345] Xiong W, Lagerström R. Threat modeling – A systematic literature review. Comput Secur. 2019 Jul 1;84: pp. 53-69.
[346] Freund J. Threat-Modeling Basics Using MITRE ATT&CK [Internet]. Dark Reading. 2020 [cited 2020 Sep 11]. Available from: https://www.darkreading.com/risk/threat-modeling-basics-using-mitre-attandck/a/d-id/133772; Hoffmann S. IoT Security Architecture and Policy for the Home - a Hub Based Approach [Internet]. Oxford, United Kingdom: IoT Security Foundation; 2018 Nov [cited 2020 Aug 12] p. 40. Available from: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf.
[347] *The True Story of Using Fiction to Enhance Risk Intelligence* (2021) The Association of International Risk Intelligence Professionals (AIRIP). Available at: https://www.youtube.com/watch?v=qP_i94eP2Ho (accessed 18 January 2023).
[348] Szathmari G. Threats | Threat Modeling | Privacy for Journalists [Internet]. Privacy for Journalists. 2017 [cited 2020 Sep 11]. Available from: https://privacyforjournalists.org.au/threat-modeling-for-journalists
[349] Bradshaw P. Why every journalist should have a threat model (with cats) [Internet]. Online Journalism Blog. 2014 [cited 2020 Sep 11]. Available from: https://onlinejournalismblog.com/2014/07/16/why-every-journalist-should-have-a-threat-model-with-cats/
[350] Stray J. Security for Journalists, Part Two: Threat Modeling [Internet]. OpenNews: Source. 2014 [cited 2020 Sep 11]. Available from: https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/

Any threat model categorisation needs to be both relevant to contemporary threats and cognisant of potential future threats (called here anticipatory).[351] Thus, review of literature relating to IoT device capabilities and examples of misuse or of the potential for misuse was first undertaken (see: section 3.2.1 of this chapter). This was then followed by 70+ detailed interviews with journalists, media and security experts, and relevant academics (see: Chapters 4, 6 and 7). These interviews were key to understanding the real-world needs that this categorisation hopes to address.[352] The ways in which journalists may be targeted through the IoT were systematically evaluated and categorised. These are predominantly threats that are unlikely to manifest against less high-value civilians to the same extent, either in terms of probability, prevalence, or intensity, due to the level of technical skill or the time and resources necessary to implement such threats.

3.5.2.2.2 Organisation of the threat categorisation

The threats categorisation was created inductively,[353] by compiling information on different potential vulnerabilities and associated exploitation opportunities from various sources, including academic studies into IoT threats as well as news sources discussing cyber-attacks on the press. This culminated in a knowledge map in the form of a list, split into clusters of threats relating to specific threats against the free press relating to consumer IoT devices. As with the conceptual model of IoT devices, the IoT threats in this categorisation were classified through thematic coding of both consumer and smart city-related IoT devices and situations referred to by over 70 interviewees (see: Chapters 4, 6 and 7) using NVIVO. Following this, categories and their contents were then updated through secondary source analysis of existing IoT threat taxonomies (see sources mentioned throughout Chapter 5 and in section 3.5.2.2.1).

The organisational use of a list visually classifies threats to information and their "chained" relationships to secondary consequences.[354] Further, each item in the list is presented as a threat description, and a hypothetical consequence scenario that affects journalists, news organisations and the press more generally. The decision to use threat modelling scenarios was taken because they familiarise subjects with vectors and consequences by framing them as short, well-defined contingencies.[355] This also enables the later mapping of such threats to countermeasures in an overarching framework of mitigations (see: Chapter 8).

Delineation of the clusters of threats was iterative, to capture emergent threats and predictively include them in the mapping process.[356] Another consideration in the creation of each of the categories, rather than use existing categories from published cyber-harms papers, was that they must build on the real needs and work of journalists, rather than being dictated by those outside the stakeholder industry such as technical computer science experts. Each new category - *Regulatory gaps, Legal threats, Profiling threats, Tracking threats, Data and device modification threats, and Networked devices threats* - was

[351] Kazansky B (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society 8(1). SAGE Publications Ltd: 2053951720985557. DOI: 10.1177/2053951720985557.
[352] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. p. 151.
[353] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. p. 73.
[354] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. pp. 14, 42.
[355] Kazansky B (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society 8(1). SAGE Publications Ltd: 2053951720985557. DOI: 10.1177/2053951720985557.
[356] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. Pp. 73, 131, 143.

designed with consideration of journalists' typical vocabularies and priorities.[357] The goal was to design the categories to be sustainable, robust, and able to include future technologies.

Initially, the threats categorisation was an attempted taxonomy that categorised IoT threats with the potential to harm journalists' work and wellbeing, first relating to information, and then how those threats to information may burgeon into legal and physical threats. The threats to information were as follows: *Stealing information*, *tracking journalists and sources*, *altering information*, *assuming control over intended device functionality to discredit or physically harm journalists*, and *limiting device functionality* (see: Appendix D). This early form of the threats organisational model was revamped per reviewer feedback that highlighted the difficulty of future-proofing a taxonomy of emerging technologies. Once the threats categorisation was altered into the version shown in Chapter 5, it was presented at the Cyber Science 2022 conference and published by Springer in the Proceedings.[358] One feature of the draft threats "taxonomy" that was kept when it was revised into a threats categorisation is that all categories of threat offered examples to illustrate the ways in which they would harm press freedom.

3.5.3 Codebook for Country Profile interview development and analysis

Table 8 lists the individual codes used to manually code in NVivo, arranged by theme used to structure the interviews conducted for Chapters 6 and 7.

Journalism	***IoT Landscape***	***Legal threats (either relating to the press or the IoT)***	***Pandemic impacts***
Source	Smart city	Law	COVID
Press	Security by Design	Law enforcement	Covid-19
Press freedom	Privacy by Design	Police	Coronavirus
Journalist	Internet of Things	Intelligence	Pandemic
Media	IoT	Intelligence agency	Geofencing
	Design	Security service	Emergency powers
Country	IoT landscape	Security agency	Contact tracing
United States	Market	Legal threat	Virus
United States of America	Supply chain	Legal	Spread
USA	Geopolitics	Legislation	Disease
US	Geopolitical	Legislative	Rona
America	Data centre	Politics	Tracking
American	Manufacture	Data protection	
United Kingdom	Sold	Decrypt	*(To ensure the thesis remained useful post-pandemic, this theme was largely excluded from Chapters 6 and 7. However, it was the basis of a 2023*
UK		Data retention	
Britain	***Media cyber protections***	Government	
British	Media organisation	Policy	
England	News outlet	Data collection	
English	News organisation	Data aggregation	
Northern Ireland	Cyber security	Surveillance	
Northern Irish	Cyber protection	Profiling	
Scotland	Mitigation		

[357] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. p. 151.

[358] Shere ARK, Nurse JRC and Martin AP (2023) Threats to journalists from the consumer Internet of Things. In: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Springer Nature. Wales, UK: Springer, p. 230. Available at: https://link.springer.com/book/9789811964138.

Scottish Wales Welsh Taiwan Taiwanese Australia Australian ***Regulation (either relating to the press or the IoT)*** Regulate Regulation Standards Standardise Code of Practice CoP Governance	Resilience Cyber Security Privacy Threat Physical threat Cyber-physical threat Psychological threat Ambient Bystander Botnet Cyber-attack Threat intelligence Threat intelligence sharing Threat model Threat assessment Risk Assessment Strategy Encryption Encrypt Cryptographic	Analysis Warrant Warrantry Sourcing Restriction Reporting restriction Intimidation Reporting Legislation Computer Network Exploitation CNE	*commentary article written for the Shorenstein Center).*[359]

Table 8: Codebook for Country Profile interview development and analysis

3.5.4 Analysing validation survey results

To explore how to structure the framework, four steps were taken: First, surveying the field to find the gap in the literature (see: Chapter 2). Second, designing a solution, i.e. deciding on a filterable spreadsheet that takes into account multiple factors related to IoT risks to journalists (see: Chapter 8). Third, defining the individual columns of the framework, i.e. identifying the key criteria relating to inclusion and exclusion of information in the framework, thus ensuring that the solution proposed matches what is needed to fill said gap (see: section 3.2.3.2 of this chapter, and the discussion regarding defining framework columns in Chapter 8). Fourth, piloting and soliciting expert feedback to refine the content of the framework (see: sections 3.2.3.2, 3.3.2.2.2 and 3.4.3 of this chapter).

Regarding this final step, for each of the four expert surveys, raw results were exported from the JISC survey platform in the form of an Excel spreadsheet. Data within each spreadsheet was then sorted and restructured to make it easier to read, understand, compare, and analyse. The first tab was always dedicated to demonstrating participant information (e.g. number of years of experience), with subsequent tabs relating to information specific to a given framework column.

Open-ended question responses were thematically coded to identify any recurring themes to establish which framework improvements must be made, by popular demand. The closed-ended question responses were statistically analysed and used to assess the content of each section of the framework. Any responses that were more relevant to the framework discussion, rather than its contents, were moved to a Word document to be included in Chapters 8 and 9. See Chapter 8 for more information on

[359] Shere ARK (2023) Threats To Press Freedom In The COVID-19 Era. In: *Shorenstein Center*. Available at: https://shorensteincenter.org/commentary/threats-press-freedom-covid-19-era/ (accessed 19 June 2023).

how the validation survey results were analysed to populate the framework columns, and details of the framework's finalised content.

3.6 Conclusion

This chapter has detailed the mixed methodologies of the research studies that support this thesis. These were developed to address the needs identified from a literature review and synthesis on the factors affecting consumer IoT threats to the press (see: Chapter 2). Mixed methods of data collection and analysis were chosen to integrate both qualitative and quantitative findings, across disciplines that relate to the research question that underpins this work. The result is a rich and rigorous thesis that solicits contributions from experts in, for example, journalism, law, cyber security, press freedom, and privacy, applies these perspectives to four different countries, and uses them to present a toolkit of resources designed to support members of the press in incorporating IoT considerations in their risk assessment and management strategies.

Chapter 4: Exploratory Study: Investigating How Journalists Perceive and Respond to Risks from the Internet of Things

4.1 Introduction

To investigate the overall research question of "How can members of the press in democratic countries improve their identification of, protection from, and resilience against threats from the Internet of Things?," an exploratory study was needed. This chapter presents the exploratory study, a version of which was peer-reviewed and published at the 2020 IEEE European Symposium on Security and Privacy Workshops.[360] The goal of this chapter is to evaluate the extent to which journalists understand the risks present in the IoT.

Practitioner-focused reports such as those from Reporters Without Borders highlight the rise in attacks against journalists worldwide and yet contain a total lack of protective information about the potential threats posed by IoT devices.[361] There is, however, no academic research into this emerging human-computer interaction domain. As the IoT grows as a popular feature in journalists' daily lives (both at home and work), researching the implications of this is imperative. Therefore, although the results of this exploratory study should in no way be taken as generalisable, they are intended to contribute to the sparse academic environment relating to the impact of the IoT on the free press. Later chapters use this exploratory study as the baseline from which to increase journalistic awareness of (see: Chapter 5) and protection against IoT threats (see: Chapters 8 and 9).

Many news stories report on manipulation of journalists' legacy devices for surveillance or disruption purposes. However, there appear to be no articles online about novel IoT devices that belong to journalists being hacked. This may be because of the heterogeneous nature of the consumer IoT and the potential for even individual devices to be manipulated to several different ends, thereby allowing less overt exploitation like surveillance efforts to be more clandestine.

While journalists may be aware of established risks, such as being tracked via the GPS on a mobile phone, guidance documents by well-known supporting organisations such as the Rory Peck Trust and Reporters without Borders overlook the potential for smartwatches and fitness trackers to be used to collect (for example) scheduling, messages, geolocation and biometric data.[362]

Already, instances of more novel attacks on the free press include those conducted through "botnets" (multiple insecure IoT devices that have been hacked and harnessed to attack more secure targets). These have not garnered much attention, as well as not being explicitly linked in news articles to the IoT. Examples include the use of botnets to launch Distributed Denial of Service (DDoS) attacks on news

[360] Shere ARK, Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.

[361] Reporters without borders (2018) Worldwide round-up of journalists killed, detained, held hostage, or missing in 2018. 1 December. Available at: https://rsf.org/sites/default/files/worldwilde_round-up.pdf (accessed 9 September 2019). Reporters without borders (2019) Only nine percent of humankind lives in a country where press freedom is good. Available at: https://rsf.org/en/news/only-nine-percent-humankind-lives-country-where-press-freedom-good (accessed 9 September 2019).

[362] Rory Peck Trust (2019) Digital Risk Assessment. Available at: https://rorypecktrust.org/resources/Digital-Security-Guide/Digital-Risk-Assessment?cu=en-GB (accessed 9 September 2019); UNESCO and Reporters without borders (2015) *SAFETY GUIDE FOR JOURNALISTS: A handbook for reporters in high-risk environments*. Reporters without borders. Available at: https://rsf.org/sites/default/files/guide_journaliste_rsf_2015_en_0.pdf (accessed 9 September 2019).

organisations and the National Union of Journalists in the Philippines, intended to censor the press by limiting the availability and accessibility of their work.[363]

Multiple studies have assessed how best to protect journalists from conventional cyber-threats to phones, laptops and communications channels including two from McGregor *et al*. and McGregor *et al*.[364] These provide an exemplary overview of much of the preceding academic work regarding journalists' computer security and the importance of secure communications channels, while recognising the crucial need to verify source identities or risk proliferating false information. This research builds upon seminal work in the area of journalist cyber security, for example papers by McGregor, Watkins and Henrichsen, which did not consider newer IoT threats to the free press. This is a clear literature gap that this exploratory study (described in this chapter) seeks to address by exploring the risks facing journalists from newer technologies.

This chapter presents the exploratory study conducted early in this research process. It was designed as a self-contained study to briefly assess the extent to which members of the media and cyber security experts aligned in their expectations of how journalists can protect themselves from IoT. This was designed and published as a standalone study, [365] so it can best be understood presented as a unified chapter, to demonstrate the success of this exploration and its relevance to the rest of this thesis.

Given the three research questions that underpin this chapter (explored in the next section), the objectives of this pilot research were threefold: First, interviewing and surveying a total of 16 members of the media industry to examine the extent to which journalists understand the risks inherent in the IoT (including how the IoT might exacerbate pre-existing threats, such as security issues regarding remote communications methods) and to collect information on how they attempt to combat perceived IoT-related threats. Second, 34 cyber security experts were surveyed to confirm how, if at all, lay-people ("the general public") can protect their privacy and security against threats through the IoT. Third, this chapter sought to compare and contrast the self-disclosed security behaviours of the journalists with the expert recommendations, in order to find out whether the journalists should maintain or could improve their security strategies to protect against both immediate and long-term IoT threats. This is intended to provide a unique insight into an understudied area of work and motivate future research on the topic.

4.2 Research Questions

This chapter focuses on the following research questions:

1. To what extent do journalists perceive threats from the Internet of Things (IoT)?
2. What protective tools and methods do journalists feel are currently effective in increasing their cyber security against all perceived cyber-threats (including any from the IoT)?

[363] Ellao JAJ (2019) What you need to know about the ongoing cyber-attacks vs. alternative news Bulatlat. In: *Bulatlat*. Available at: https://www.bulatlat.com/2019/02/07/what-you-need-to-know-about-the-ongoing-cyber-attacks-vs-alternative-news-bulatlat/ (accessed 4 March 2020); Minda News (2019) STATEMENT: DDoS attacks on NUJP, alternative media continue. *MindaNews*, 11 February. Available at: https://www.mindanews.com/statements/2019/02/statement-ddos-attacks-on-nujp-alternative-media-continue/ (accessed 4 March 2020).

[364] McGregor SE, Charters P, Holliday T, et al. (2015) Investigating the Computer Security Practices and Needs of Journalists. In: *Proceedings of the 24th USENIX Security Symposium*, Washington, D.C., 12 August 2015, p. 17. USENIX Association; McGregor S, Roesner F and Caine K (2016) Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proceedings on Privacy Enhancing Technologies* 2016. DOI: 10.1515/popets-2016-0048.

[365] Shere ARK, Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.

3. Are the protective measures reported as in use by journalists actually effective, when compared to the known recommendations from contemporary literature and experts in cyber security?

4.3 Results

4.3.1 Participants

Journalist interviewees reported having the following specialisms: markets and financial technology, cyber security, local investigative reporting, domestic politics, economics, drug trafficking, the economy, agriculture, current affairs, investigative reporting, finance and business, wire services, conflicts and defence, technology, digital security, human rights, civil society and activism, East/West relations in Europe, international relations, transnational organised crime, and the impact of history on contemporary politics. All of these specialisms could be considered high-risk in terms of targeting by state and criminal actors.

In the following sections, journalist participants will be referred to with pseudonymised identifiers beginning with I (interviewees, i.e. I1-I11) and S (journalists surveyed through the questionnaire disseminated by the AIB, i.e. S1-S5), per Tables 9 and 10.

Interviewee	**Role(s) held in the media sector**	**Years working as a journalist/with journalists**
I1	Journalist	6
I2	Journalist	~15
I3	Journalist	20
I4	Journalist	10
I5	Journalist/ media executive	40+
I6	Journalist/ foreign correspondent	21
I7	Journalist/ academic researcher	25
I8	Journalist/ foreign correspondent	4
I9	Journalist/ academic researcher/ cyber security advisor and trainer	25+
I10	Cyber security advisor (I10 is not a journalist, but works closely with journalists and news organisations on cyber security training and responses)	5+
I11	Journalist/ foreign correspondent/ consultant	~37

Table 9: Details of Interviewees

Respondent	Journalistic specialism	Whether cyber security is a subject element of their work	Whether they are aware that they have been the target of any digital attacks	Years working as a journalist
S1	Live reporting	Yes	Yes	38
S2	Technology	Yes	Yes	29
S3	None	Yes	Yes	25
S4	International refugee crisis	No	No	Almost 10
S5	Broadcast journalism	No	No	10

Table 10: Details of AIB Survey Respondents. Respondents to the AIB survey were all journalists.

Due to the high-risk nature of participants' work, more demographic information cannot be divulged. Additionally, in the following analysis of the results, the gender-neutral pronoun "they" has been used to further obfuscate identities.

A total of 34 cyber security expert respondents were recruited in this study. 29/34 respondents (85.3%) claimed to have conducted academic research in the field of cyber security.

4.3.2 Media industry participants' responses

Figure 2 below displays the number of media industry respondents (both interviewees and AIB survey respondents) who disclosed using different types of consumer IoT devices, compared to their use of conventional devices (laptops, desktops, tablets, and smart phones).

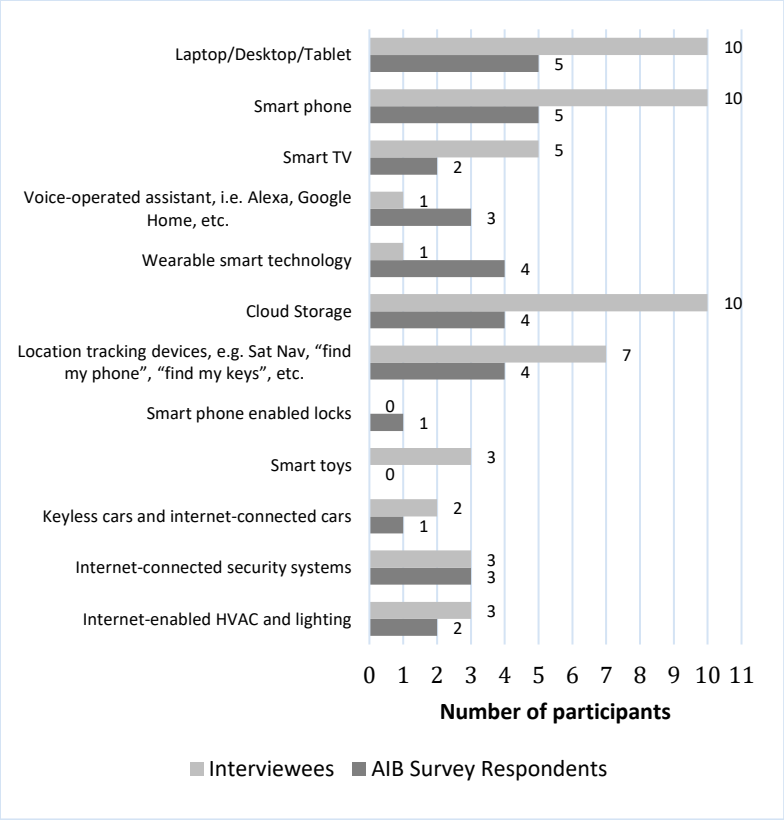


Figure 2: Technology used by media industry respondents

Most of the interviewees, all of whom were journalists, made it clear that they perceive IoT threats to their work and well-being. These were categorised into three broad and overlapping types of censorship-related threat: those to information, legal threats, and threats to physical well-being. Each will be mentioned below and further explored in this chapter's Discussion section.

Other results that will then be documented in this section include media participants' responses regarding protective tools and methods that journalists use to increase their cyber security, physical protection strategies for journalists, and allocation of responsibility for journalists' cyber security.

4.3.2.1 Threats to Information

IoT-related danger can manifest in different ways, from the unique cyber-physical capacity for threats to jump from the virtual realm to the material world, to an exacerbation of longstanding threats to information. This means threats to the confidentiality, integrity, and availability of both raw and analysed data.[366]

Two interviewees, both of whom advise and train journalists on security,[367] stated that their experience indicated that most journalists with whom they interact are unaware of IoT-related threat models. This is despite the fact that these threats are becoming more targeted as global press freedom decreases and attacker sophistication increases. I10, a cyber security advisor, responded that journalists and their

[366] Poremba S (2018) Data Privacy Must Evolve Beyond Confidentiality. In: *Security Intelligence*. Available at: https://securityintelligence.com/data-privacy-must-evolve-beyond-confidentiality/ (accessed 14 April 2020).
[367] Interviewees: I9, I10.

organisations were reactionary and tended to seek help only after being attacked. I10 also stated that many journalists "don't understand the risks of their basic devices so don't see how adding more internet-connected devices expands the attack surface" and that the threat was not just to information, but in some cases safety. By two interviewees' own admission,[368] additional risk emanated from reckless behaviour. Even though aware of the importance of using hardened professional networks and sanitised devices, they confessed to taking work calls near unsecured smart-home entertainment systems.

4.3.2.2 Legal Threats

Legal threats to journalists occur when states implement legislation that grants them intrusive or sweeping powers. Regarding the IoT and the free press, these often manifest as data retention laws, national security loopholes in data protection regulations, the criminalisation of whistleblower and journalistic activities, or bans on security provisions such as strong encryption.

Ten interviewees admitted or intimated that they are concerned that IoT devices amass data that can be accessed by authoritarian or overreaching democratic governments with a track record of coercing companies into divulging this data in the name of national security.[369] Some of these interviewees mentioned concerns about the risks inherent in IoT devices because of the likelihood of state surveillance of journalists and a history of attempts to use "overreaching" legal mechanisms to conduct leak enquiries.[370]

A perception that most standard IoT devices lack end-to-end encryption was also the subject of four responses regarding legal threats to journalists.[371] Further, three journalist participants expressed fears regarding the lack of accountability employed by governments to justify data retention and anti-encryption laws (such as those in Australia),[372] [373] and six indicated concern about legal loopholes in data protection laws (such as the "legitimate interest" justification in the GDPR).[374] [375]

I7 noted that their research has unearthed clear worries in the journalistic communities in countries such as Australia. This is because of the clear lack of adequate threat modelling demonstrated by the country's ban on strong encryption, meaning that access to the huge quantities of IoT data and metadata can allow governments to retroactively build cases against a targeted individual that lead to their prosecution, incarceration, or social alienation such that they cannot continue to operate as a journalist or a citizen.

4.3.2.3 Physical Threats

Given the cyber-physical nature of the IoT, IoT threats could be escalated to threats to the physical security and safety of journalists and sources. I3, who consented to being identified as a Mexican journalist with experience covering drug trafficking stories, stated that this interview was the first time that they had

[368] Interviewees: I4, I7.
[369] Interviewees: I2, I3, I4, I5, I6, I7, I8, I9, I10, I11.
[370] E.g. Interviewees: I3, I4, I6.
[371] Interviewees: I2, I4, I5, I10.
[372] Interviewees: I2, I7, I8.
[373] Taylor J (2019) Australia's anti-encryption laws being used to bypass journalist protections, expert says. *The Guardian*, 8 July. Available at: https://www.theguardian.com/australia-news/2019/jul/08/australias-anti-encryption-laws-being-used-to-bypass-journalist-protections-expert-says (accessed 9 September 2019).
[374] Interviewees: I2, I3, I5, I6, I7, I8.
[375] Information Commissioner's Office (2019) Guide to the General Data Protection Regulation (GDPR): Lawful basis for processing: Legitimate interests. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (accessed 9 September 2019).

discussed cyber security because "it's not linked enough in countries like mine to survival." Their answer elucidated that, traditionally, the perception of cyber-threats is focused on information, rather than being linked to potential physical attacks.

While it is true that technologies like smart phones, laptops and tablets are most at risk of loss of data that comprises the content of a news story, novel IoT devices (such as smart fridges, smart light bulbs and internet-connected vehicles) represent a new kind of cyber-physical system that could have more urgent implications for both the data and physical well-being of targets.[376] I7, who has conducted academic research into the interface of cyber security and journalism, referred to the belief of free speech and regulation expert, Dr. Katherine Gelber, that the prevalence of the IoT comes with global dependence on the IoT for "production, dissemination, the basic tenets of our jobs, so there's no way to separate the kinds of attacks that affect information from those that affect us physically." The interviews conducted made it clear that, for more journalists to be able to understand IoT threats, they must be conceptually detached from the typical perception of cyber-threats as just to data and thus irrelevant to personal physical security.

As will be explored in the Discussion section, respondents noted that manipulation of the physical properties and outputs of IoT devices and networks have psychological effects that "chill" their drive to do journalistic work. I7, a journalist and academic researcher, argued that appeals to national security frameworks to allow states to access IoT contents and metadata could initiate a slippery slope towards "sedition and treason," for which the ramifications may be physical and life-threatening. I10, whose primary role is as a cyber security advisor, noted that "in our work it's very crucial that we understand that digital security is just one component. There are also physical and legal threats and other kinds of attack. It's pretty common in our work that we see these be interconnected. Even with the best protections in the world, if the weakest link in the chain is physical or legal security, the threat model is too weak."

I11, who has roughly 37 years of experience as a journalist, including as a foreign correspondent and media consultant, disagreed with Rid's argument that "cyber war will not take place,"[377] saying that their "concern is that there are so many unpredictables within the expanding network, specifically because of IoT, that there is an elevated risk of something happening in the cyber sphere having a very significant impact in the real world." I9, who has worked for over 25 years as a journalist, academic researcher, and cyber security advisor and trainer, also pointed out that the normalisation of an increased prevalence of IoT devices could lead to populations becoming dependent on their continued function. This would give a zero-day attack the power to destabilise societies and the global order in both kinetic and non-kinetic ways. I10, who assists journalists with cyber-attack recovery, stated that "there are a lot of differences between the capabilities of the adversaries and the journalists being attacked [and] for someone who doesn't have a network to support them, it's very hard to fight those battles."

On a smaller scale, I4 noted that they had fears, as both a consumer and a journalist, about the physical effects of the market for basic appliances (e.g. TVs and fridges) being flooded by IoT devices, thereby making non-internet-connected devices more expensive and less accessible and forcing IoT devices to be

[376] Privacy International (2019) Case Study: Connected Cars and the Future of Car Travel in the Digital Age. Available at: http://privacyinternational.org/case-studies/769/case-study-connected-cars-and-future-car-travel-digital-age (accessed 9 September 2019).
[377] Rid T (2013) *Cyber War Will Not Take Place*. London: C Hurst & Co Publishers Ltd.

the new standard. They were concerned that an attack on their internet access and/or power supply would affect the functionality of critical devices.

4.3.2.4 Protective tools and methods that journalists use to increase their cyber security

When asked about the tools and techniques they employ to defend against IoT exploitation, every interviewee confirmed that their primary approach to risk mitigation was to minimise interactions with IoT devices and return to analogue methods of data collection, communication, and storage. Above all, this recurrence of traditional journalistic habits was noted as being a crucial component of source protection, but I7, a journalist and journalism researcher, acknowledged that it was regressive for newsgathering, as IoT technologies "would make the job easier and give us access to sources who were further away or evidence that is harder to find."

Worryingly, perhaps because of a feeling of futility regarding the security of and protection from IoT devices, some journalist respondents admitted that they did not have coherent or relevant cyber security strategies.[378] Participants I5 and I10, whose work involves managing or cyber security training numerous journalists, noted that their organisational risk assessment procedures do not take into account IoT threats.

4.3.2.5 Physical protection strategies for journalists

All ten journalist interviewees were concerned that the spread of casual-use IoT devices could remove the confidentiality of source-journalist interactions,[379] with I10 being more attuned to journalists' vulnerabilities owing to their work as a civil society cyber security trainer. Respondents' techniques for minimising threats through the IoT can be classified as attempting to limit their access to the internet, and they focused on disconnecting devices and disabling applications when not in use. Interviewee I9 admitted to taking Faraday cage bags to meet sources so that, if batteries cannot be removed, sources' devices can be switched off, allowing unintentional audio-recordings to be muffled and any signals to be blocked.

Ways of physically limiting the functionality of IoT devices that were mentioned by respondents included the use of covers over cameras. However, all disclosed strategies were acknowledged to be temporary because of the dangers of remote access when internet-connection is built into the functionality of essential devices such as home security systems. All 11 interviewees recognised that the main issue with physical strategies was the same as with all IoT threats, namely that journalists cannot always control IoT presence in the environment where they meet with sources.

Resultantly, some journalists rely on remote communications methods. However, as mentioned, interviewees admitted to communicating important information in the presence of insecure IoT devices.[380] This may render any effort to use secure remote communications channels redundant, a problem that will be exacerbated as the prevalence of ambient IoT technologies grows. Still, the following participant responses were included to emphasise the IoT's capacity to reinforce and heighten existing security issues, not just to create new ones. Nine interviewees discussed the challenges of finding and exclusively using secure channels for communication with sources. Two interviewees detailed their use of

[378] Interviewees: I1, I3, I4.
[379] Interviewees: I1, I2, I3, I4, I5, I6, I7, I8, I9, I11.
[380] Interviewees: I4, I7.

specific encrypted messaging platforms, such as Signal and hardened emails, like ProtonMail.[381] Others mentioned PGP encryption or that they try to use encrypted communication mechanisms in general.

However, I5, who has over 40 years of experience as a journalist and media executive, suggested that it was hard to verify whether these methods of securing remote communications were sufficient, and thus discussed attempts not to put any source-identifying information into a digital format. I5 noted though, that this "has made it more difficult to communicate". Acknowledging the same challenges, I8, who is a foreign correspondent, was nevertheless aware that avoiding all remote communications channels is unrealistic even if encryption methods are not guaranteed to be secure.

Many IoT devices now have inbuilt email functionality, providing an additional pivot-point for attackers to access email correspondence, thereby further lowering confidence in email security, confidentiality, and integrity. Interviewees differed in their approaches to email security. I11, who has been a journalist (including working as a foreign correspondent) and consultant for roughly 37 years, claimed that the core of their security regime is to "assume that what you're doing is public communications," while I1's sources only communicate with them using burner accounts and then the emails are bounced through multiple accounts "so the [audit] trail is muddled. Additionally, much of the reliance on or avoidance of emails depends on source location and context. For example, I2 preferred not to communicate via email if the story is sensitive while, at organisations for which I7 has worked, "some stories have been shut down completely if there have been emails" because the channel is "not considered hygienic and that's often enough to end a source-relationship or to kill a story altogether, so it's a form of self-censorship."

4.3.2.6 Allocation of responsibility for journalists' cyber security

Repeated themes from interview respondents included that "the responsibility to educate journalists about IoT threats lies with news organisations" and that often "the threats come from governments so we wouldn't have incentive to listen to their advice".[382] Multiple respondents (most of whom preferred to not have their responses even attributed post-pseudonymisation) also believed that states and state-affiliated agencies could not be trusted to inform journalists about IoT threats, as they were responsible for most instances of targeted exploitation of journalists' devices. As a result, proposed regulation of the IoT industry or reforms of data-related legislation could be met with scepticism by any journalists who understand technological threats.

Instead, news organisations, journalists' unions and NGOs were the suggested parties for education and training of journalists against IoT threats.

4.3.3 Comparing expert recommendations with media members' risk mitigations to determine their efficacy

Of 34 expert respondents, 20 (58.8%) felt that members of the public could not opt out of the use of the IoT in 2019, and 26 (76.5%) felt that by 2024 the public – including journalists – would find it almost impossible to opt out of having their information vulnerable to IoT devices, even if they avoided personal ownership of them. This invalidates the responses given by all interviewees, that the core of their (often informal) IoT-related security strategies is to avoid ownership of and restrict contact with IoT devices.

[381] Interviewees: I2, I11.
[382] Interviewee: I7.

Experts suggested few solutions: In the short-term individuals could focus on efforts to avoid, subvert, or limit the ability of IoT devices to collect personal information. These include changing default settings to make passwords stronger, activating device firewalls, avoiding public Wi-Fi, segmenting networks so that critical and non-critical IoT devices could not interact, and purposefully inputting incorrect user information in order to impede accurate data collection. One expert said that "physical and digital controls of such devices might offer some protection against privacy/security threats," which supports the utility of mitigations implemented by journalist respondents, such as the use of camera covers and mechanisms to obstruct microphones like Faraday bags.

In the longer-term, expert respondents recommended better education about the potential threats of IoT devices (30.8% of respondents), lobbying governments and private companies to create industry standards around consumer safety related to IoT devices (26.9%), and a focus on the need for united public activism in order to push for protective legislation and education (11.5%) was viewed as vital. This links to the pivotal point touched upon by I10: the free press is staving off near-constant attacks from well-resourced and skilled adversaries, so how can society expect individual journalists to implement both fundamental technical and high-level cyber security measures against evolving emerging threats like the IoT? As mentioned, when asked who should be responsible for journalistic cyber security, media participants largely endorsed an institutional approach. This suggests that they understand, at least in part, the theme of most experts' responses: that IoT threats are systemic and can only be combatted long-term through structural shifts that require coordinated activist efforts.

4.4 Discussion

This section discusses the different kinds of threats perceived by journalists from IoT devices as well as potential protection strategies and their drawbacks.

It is important not to draw general findings from the anecdotal information disclosed by 11 interviewees and five additional surveyed journalists. Thus, as mentioned, when recruiting for this exploratory study a purposive sample of participants were recruited, and then snowball sampling was conducted. Those considered were all members of the press who work on an assortment of topics that could be considered to be "high-risk," from a variety of countries, whose work (either in terms of journalism, news organisation management or cyber security training) exposes them to the experiences of other journalists.

Additionally, some of the yielded results seem in line with findings from previous studies on similar topics. For example, McGregor and Watkins investigated journalists' and editors' conceptualisations of their own digital security demonstrated that "experience with a system does not necessarily translate to an accurate system *or* mental model of it" as their interviewees lacked understanding of the risks associated with communications technologies.[383] Although McGregor and Watkins' findings are not IoT-specific, they are corroborated by this chapter's findings, with clear parallels between both their and this study's participants' responses regarding threat perceptions and resultant attitudes and behaviours.

Similarly, although Williams *et al.*'s research does not focus on journalists, it shows that the users of only older technologies are much less likely than IoT device users to display a "privacy paradox," i.e. to assert

[383] McGregor SE and Watkins EA (2016) "Security by Obscurity": Journalists' Mental Models of Information Security. *#ISOJ* 6(1). The Multimedia Edition of the Official Research Journal of the International Symposium on Online Journalism. Available at: https://isojjournal.wordpress.com/2016/04/14/security-by-obscurity-journalists-mental-models-of-information-security/ (accessed 15 February 2020).

their desire for privacy while displaying contradictory behaviours, such as buying insecure IoT devices.[384] This is another finding that was corroborated by evidence from these interviews, notably with interviewee I7, who has 25 years of experience working in and researching journalism.

As mentioned in the Results section, many of the interviewees for this chapter were able to articulate that they perceive substantial threats from the IoT. These could be categorised into three broad and overlapping types of threat that could lead to censorship: those to information, legal threats, and threats to physical well-being. Together, these kinds of threats represent the following three sections of analysis, after which respondents' allocation of responsibility for journalists' cyber security will be discussed.

Then, cyber security expert responses regarding the IoT threat vectors mentioned by all the participants will be incorporated and structured according to whether they facilitate privacy-related threats or access control-related threats. They will be used to compare expert assessments of IoT threats and possible mitigations and solutions with the journalists' practices.

4.4.1 Threats to Information

IoT utility often relies on the same function that poses a threat to journalists, such as the need for voice-activated devices to be constantly listening.[385] Only two journalist interviewees mentioned or alluded to the knowledge that IoT cloud databases were points of vulnerability, either for information loss, or because they could divulge locational metadata from self-tracking services.[386] This was interesting when one also considers that it may well be impossible for journalists to always remain vigilant against ambient IoT surveillance.

One AIB survey respondent, S1, who works in live reporting, stated that they have a strategy of "keeping sensitive data away from the devices and if necessary, away from the 'cloud.'" Their answer infers a mental separation of IoT devices and the cloud, signifying a lack of awareness of how IoT devices often work. It was common for interviewees to emphasise their awareness that newer IoT devices are often less secure and do not use strong encryption, while neglecting the technical details of other IoT-specific vulnerabilities, such as cloud-reliant architectures.

Three AIB survey respondents explicitly expressed their concern that IoT devices pose a threat to anonymity of sources.[387] However, S5, a broadcast journalist, also noted that their work is reliant on "these internet-enabled mediums," indicating the complexity of the choice to limit their access to such technologies.

4.4.2 Legal Threats

Legal provisions can be used by government agencies and state-affiliated organisations to unmask sources and monitor the whereabouts of journalists without the need to explain their actions and analysis to the public. There is a disparity between states' almost-unfettered access to data and the amount of information that journalists can glean from governments, demonstrated by the 42% UK government

[384] Williams M, Nurse J and Creese S (2017) 'Privacy is the Boring Bit': User Perceptions and Behaviour in the Internet-of-Things. In: *15th International Conference on Privacy, Security and Trust (PST)*, 28 August 2017. DOI: 10.1109/PST.2017.00029.
[385] Williams M, Nurse J and Creese S (2017) 'Privacy is the Boring Bit': User Perceptions and Behaviour in the Internet-of-Things. In: *15th International Conference on Privacy, Security and Trust (PST)*, 28 August 2017. DOI: 10.1109/PST.2017.00029.
[386] Interviewees: I1, I4.
[387] AIB survey respondents: S2, S4, S5.

approval rate of Freedom of Interest requests in 2018.[388] Access to the vast amounts of data collected and conveyed by IoT networks could allow corrupt government bodies and law enforcement agencies to manipulate information to incriminate journalists and censor news stories. I4 also acknowledged that there could be a lack of accountability in the event that state surveillance is uncovered.

4.4.3 Physical Threats

The asymmetrical nature of the threat means that it is difficult to anticipate threat levels and to know how to prioritise different defence and source protection strategies. Furthermore, interviewee I9, who has a role as a cyber security trainer for journalists, spoke of the prevalent belief that cyber-threats against journalists come primarily from states. Their work has revealed that this is often the case, but that journalists are often subject to cyber-attacks from the private sector, particularly from banks, which are underestimated in terms of the time and money they spend hunting whistleblowers through surveillance of journalists. Due to the potent global influence of these public and private institutions, the interviewee argued that there is a higher likelihood of targeted cyber-physical attacks on journalists through the IoT that result in clandestine consequences. I2 also noted that attribution is difficult for this reason.

Fear of consequences for their work can cause journalists to self-censor as IoT sensors are integrated into almost all environments, creating a panopticon that can identify, track, record and analyse personal data on a global scale. This is the well-documented "chilling effect" of constant surveillance on free speech, enabled by technological advancement and an erosion of legislative safeguards for protection of individual privacy and a free press.[389] Indeed, I3 noted experiences that had concerned them, disclosing that "sometimes the TV switches on by itself and that's not normal," and going on to express that "everyone is watching you, the web is like Big Brother". This is an example of a scenario in which manipulation of the physical features of an IoT device stimulates a psychological reaction (fear and stress) in a journalist, potentially causing subsequent physical issues – from health responses to erratic or antisocial behaviour that further isolate journalists.

Potential scenarios in which IoT devices are hijacked in this way are difficult to corroborate, as Conti *et al.*'s research has demonstrated that digital forensics is difficult in many IoT devices, stating that "detecting presence of IoT systems is quite a challenge considering these devices are designed to work passively and autonomously […] in most cases when an IoT device is identified there is no documented method or a reliable tool to collect residual evidences from the device in a forensically sound manner."[390]

The cyber-physical nature of the IoT has facilitated a myriad of novel targeted virtual-to-physical anticipatory threat models, which are underexplored because of an academic focus on common threats. These include innovative vectors such as attacking an HVAC system and causing someone's pipes to freeze in winter, which could cause intimidation or distraction of a journalist, thus leading to censorship of their work through a seemingly accidental problem. Other journalists interviewed were also hyper-aware that "the attack surface has astronomically widened"[391] on both an individual and wider scale. Further, they were aware of kinetic threats through the IoT and potential escalation strategies to give targeted cyber-

[388] The Economist: Daily Chart (2019) Britain is rejecting an ever greater share of freedom-of-information requests - Daily chart. *The Economist*, 5 January. Available at: https://www.economist.com/graphic-detail/2019/05/01/britain-is-rejecting-an-ever-greater-share-of-freedom-of-information-requests (accessed 9 September 2019).
[389] Mills A and Sarikakis K (2016) Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism. *Big Data & Society* 3(2): 2053951716669381. DOI: 10.1177/2053951716669381.
[390] Conti M, Dehghantanha A, Franke K, et al. (2018) Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems* 78(2). Elsevier Ltd.: 544–546. DOI: 10.1016/j.future.2017.07.060.
[391] Interviewee: I2.

threats physical impacts.

Regarding targeted attacks on individual journalists, I2 acknowledged that the proliferation of IoT sensors in urban spaces, creating so-called 'smart cities,' would aid adversaries in tracking and locating journalists, thereby facilitating planned opportunities for physical attacks.

In terms of conducting massive disruption or destruction operations through IoT exploitation, the respondents with the most acute understanding of potential physical threats to journalists through IoT devices (who all had experience in both journalism and academic research into journalists' security) were best able to envision threat models for large-scale kinetic attacks that could have a generalised effect or could target all people likely to be in a specific place at a specific time, which could be used against multiple members of the media at once.

Specific examples of this kind of attack that were given by interviewees include compromising a traffic grid and "entering a city's network through various IoT devices and disrupting the ability to summon the emergency services." Cyber-attacks on the Ukrainian power grid in December 2015 are clear evidence of international efforts against critical national infrastructure and demonstrated the potential for abuse of Supervisory Control and Data Acquisition (SCADA) systems which, while centralised, share similarities with the IoT and can be integrated into the IoT if airgaps are removed or breached.

There is the danger of normalisation of reliance on the remote-access functionality of many IoT technologies, such as the ability to use one's phone to confirm that smart locks are engaged, which could then be exploited or malfunction. This could cause property to be less secure, as well as affecting users' mental and emotional well-being by removing a safety blanket upon which they had been dependent. I4 gave the example of video game consoles to illustrate their lived experience of manufacturers being motivated by profits and so abandoning devices (i.e. not releasing patches and updates or making additional features incompatible with previous models) and thus making the devices redundant because of a loss of functionality that is built-in to the devices themselves.

Additionally, the concept of "a porous border between the internet and the tangible world" frightened I4, as they likened IoT devices to windows in a house: "My assumption is always that the more devices you have, the more entry-points for attackers, just like if there are more windows in your house there are more entry-points for burglars." This signals an awareness of how the increased prevalence of IoT devices expands the attack surface of an individual and their environment.

4.4.4 Allocation of responsibility for journalists' cyber security

As detailed in the Results section, most respondents (many of whom preferred to not have their responses even attributed post-pseudonymisation) were openly scathing about the possibility of relying on governments to improve IoT security and protect journalists from related threats. Additionally, many interviewees were sceptical about involving technology companies in this responsibility as they felt that the technology industry tended to be more aligned with state interests. However, others, such as cyber security advisor I10, felt that "the first line should be security experts, developers, making guidelines so the consumer knows that their device has basic security settings embedded." They pointed out that "the real question is whether it's reasonable to ask a journalist in distress in an oppressive regime to do all these checks. Security should be there by default." The implication here is that there is a need for the development and legislation of standards for the IoT industry, which would require the involvement of governments.

Some states, such as the UK and French governments have already attempted a push to legislate for security by default and design in these devices.[392] Although it was suggested that journalists would find it difficult to accept assistance from states, I7 was clear about why external help must be enlisted: the resources available to help journalists from within the media industry "are strained because of the costs of maintaining legal counsel and training programmes that are current."

Increasingly, journalists are freelancing or working for underfunded fledgling organisations that depend on the savvy of individual employees or on the advice of NGOs. Even I5, a media executive, said "I try to follow good and balanced advice from professional organisations for journalists, like the Electronic Frontier Foundation."

I2 and I6 both mentioned that the information that informs how they maximise their own security or brief sources on potential threats was collated by the security teams of organisations for which they work. I10 argued that it is "a challenge to update the risk assessment [used by their organisation, which deals specifically with advising actors such as journalists on cyber-threats] because every day more IoT devices are coming out and even the ones you think you should trust have stories of being a risk." They noted that because of the huge increase in internet-connected devices released, even in communities that should be more conscious of IoT threats, risk assessments are lagging behind.

Unfortunately, there is extensive evidence that adversaries are outsourcing attacks on journalists to covert security companies that specialise in finding innovative, effective and sometimes clandestine ways to subvert their targets, such as the NSO Group and BlackCube.[393] Per the intention of this chapter, I11 noted that looking to journalists who have successfully avoided having a monumental story leaked or smothered, such as those who collaborated on the Panama Papers,[394] may be key to having hope about overcoming the asymmetry in cyber skills and resources between journalists and adversaries. Clearly, while a top-down approach to IoT security measures is desirable, in practice journalists seem to be learning from their peers and employing individual protections.

4.4.5 Threat vectors

Media participants (both interviewees and AIB survey respondents) touched upon their understanding of IoT threat vectors, naming a variety of aspects of the IoT that are susceptible to exploitation. These were compared to the answers from 34 cyber security expert respondents and the following two subsections were compiled based on all participants' responses.

Cyber security expert survey respondents mentioned several potential attack vectors for IoT devices, most of which relate to inadequate security considerations of manufacturers and vendors. These included

[392] GOV.UK (2019) Consumer Protection: Secure by Design. Available at: https://www.gov.uk/government/collections/secure-by-design (accessed 10 September 2019); ETSI (2019) *CYBER; Cyber Security for Consumer Internet of Things*. CYBER ETSI TS 103 645 V1.1.1 (2019-02), February. Sophia-Antipolis, France: European Telecommunications Standards Institute (ETSI). Available at: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (accessed 10 September 2019).

[393] Kenyon M (2019) Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes. *The Citizen Lab*, 1 April. Available at: https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/ (accessed 9 September 2019); Bergman R and Shane S (2019) The Case of the Bumbling Spy: A Watchdog Group Gets Him on Camera. *The New York Times*, 28 January. Available at: https://www.nytimes.com/2019/01/28/world/black-cube-nso-citizen-lab-intelligence.html (accessed 9 September 2019).

[394] ICIJ (2016) The Panama Papers: Exposing the Rogue Offshore Finance Industry - ICIJ. Available at: https://www.icij.org/investigations/panama-papers/ (accessed 9 September 2019).

"reuse of code libraries" by developers, an inability to alter passwords, insecure communication protocols between devices and servers, a lack of patches and "missing/delayed/inadequate firmware updates" post-release of products. These are all evidenced in current research.[395]

These experts' responses regarding digital threats could be divided into two broad classes: privacy and access control, the latter of which could be further broken down into reduction of data integrity, denial of service, and creation of botnets. Their responses regarding physical threats could be classed as illicit access to information that indirectly facilitates physical harm, or altering the output of an IoT device so that it facilitates or obfuscates physical harm to its environment and to its user.

Both of these classes of threat could have destructive consequences if enacted against journalists, whose role relies on trust – both that they can ensure source confidentiality, and that they can verify that their published work is truthful. Despite these considerations, when their answers were compared to those from cyber security expert respondents, the media participants did not appear to have in-depth knowledge or understanding of specific threats. While all their concerns were realistic, it was assessed that at least five of them lacked detail and were limited in scope.[396] This indicates that journalists may not have sufficient understanding of the multitude of potential threats that can be amplified because of the networked nature of the IoT.

4.4.5.1 Privacy-related threats

Many interviewees expanded on two recurrent themes: that IoT devices are compromised as a result of (1) the financial incentive for manufacturers to externalise costs and insufficient industry standards and regulations,[397] and (2) systemic subscription to data capitalism.[398] These points were corroborated by expert survey responses, which noted that both the insecurity of IoT devices and their intentional data collection present threats to the public. One expert summed up both themes, saying "there is a commercial incentive to build a badly set up panoptican *[sic].*"

Another privacy-related issue that was raised by three respondents is linked to the masses of data accumulated and transferred by IoT devices: information leakage and theft resulting from weak or non-existent encryption and other poor data protection mechanisms, such as inadequate cloud or application security.[399] Three AIB respondents also explicitly mentioned encryption,[400] while S1's answers did not mention data transfer and instead seemed to indicate that they try to physically and virtually isolate their data.

Regarding strategies for the preservation of sources' integrity and confidentiality in light of the ever-expanding IoT market, S2, who is a technology journalist, said "individual journalists do not have viable solutions for this." For journalists, unwanted disclosure of data could endanger their relationships with sources. Notably, I7 mentioned the "chilling effect" on news reporters as a potential outcome of increased awareness of the data collection and analytics resulting from expansion of the IoT.

---

[395] Bertino E (2016) Data Security and Privacy in the IoT. In: *Proceedings of the 19th International Conference on Extending Database Technology (EDBT 16)*, Bordeaux, France, 15 March 2016, p. 3. Series ISSN: 2367-2005. Open Proceedings. DOI: 10.5441/002/edbt.2016.02.

[396] Interviewees: I1, I3, I4, I6, I7.

[397] Interviewees: I1, I2, I4, I5, I9, I10, I11.

[398] Interviewees: I1, I2, I4, I5.

[399] Interviewees: I1, I5, I8.

[400] AIB survey respondents: S3, S4, S5.

4.4.5.2 Access Control-related threats

Access control threats can have implications both in the cyber and physical realms. With respect to the latter, altering the output of an IoT device can cause physical harm to its environment and users and, one expert respondent noted, "new emerging physical attack models [...] are likely to not be known to end users of these systems." This study demonstrated that this is true of members of the media industry.

A lack of investment in IoT security means that users cannot anticipate or control device behaviour, including data collection and sharing. Crucially for journalists, whose jobs rely on public trust, this threatens to call into question data integrity as there is a risk that data could be tampered with, both on a device and while in transit, which would threaten the ability to trust that source material is unedited.[401]

Additionally, the availability of data held by multiple devices can be compromised through Denial of Service attacks targeting even one IoT node in the network. This could mean active censorship, with journalists being locked out of laptops and denied access to information. Potentially most significantly, unauthorised access to IoT devices can result in host takeovers and their co-option into a botnet, which could then be used to enact Distributed Denial of Service (DDoS) attacks against other, better secured targets, such as entire media organisations. Three expert responses mentioned botnets as IoT-specific digital threats, and cyber security advisor I10 noted that botnet attacks against journalists and news organisations are already occurring, and the IoT market boom would exacerbate this threat.

Use of IoT devices to indirectly facilitate or obfuscate physical harm can take many forms. The networked nature of the IoT means that gaining unauthorised access to one device can allow an attacker to control an entire smart home. This could be through remote access, with victims targeted in such a way that attribution is unlikely, as the physical effects could be seen as unintentional. An example of this could be the manipulation of CCTV footage to falsify crime scene evidence. [402] One expert respondent mentioned that attacks on health trackers could lead to inappropriate diagnoses and prescriptions if subject to tampering. Both of these scenarios could spur a chilling effect on the press if journalists are aware of the possibility that any investigations may lead to potentially fatal legal or physical threats.

Cyber security advisor I10 stated that often attribution is unnecessary after cyber-attacks on journalists, from the target's perspective, because they can logically link the attack to the subject of a particular story that they are planning to publish. Additionally, the constant presence of IoT technologies and the opacity of their settings would allow the creation of a dangerous environment even when the attacker is not physically present. Technology could become even more complicit in abuse if attackers are skilled enough to utilise and subvert the consequences of features such as Amazon's facial recognition software, which can now detect fear.[403] Participants suggested that there are also scenarios in which cyber and physical attacks could be concurrent, such as "people using photos of valid users' faces to gain access to their smart

[401] Benjakob O (2022) This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure - National Security & Cyber - Haaretz.com. Haaretz, 26 December. Available at: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000 (accessed 12 January 2023).

[402] Benjakob O (2022) This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure - National Security & Cyber - Haaretz.com. Haaretz, 26 December. Available at: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000 (accessed 12 January 2023).

[403] Choudhury SR (2019) Amazon says its facial recognition can now identify fear. *CNBC*, 14 August. Available at: https://www.cnbc.com/2019/08/14/amazon-says-its-facial-recognition-can-now-identify-fear.html (accessed 9 September 2019).

locks" or tampering with burglar alarms, which could then lead to the purely physical threat of theft. These scenarios demonstrate how attacks on the IoT could chill journalists' desire to work on stories involving well-resourced adversaries.

Smart fridges have social media platform access,[404] which could be abused with disproportionate effects for journalists if hackers were to publicly share false or inflammatory information that could cause them to be discredited and lead to physical violence.

Regarding altering the output of an IoT device so that the device directly causes physical harm to its environment and to its users, there are several threat models, both current and anticipatory. These range from crashing autonomous vehicles to taking over smart light bulbs. The latter could have a number of effects on the cyber and physical realms, from clandestine user data exfiltration, to their use to trigger epileptic attacks in photosensitive users.[405]

One cyber security expert survey respondent pointed out that there is the greatest threat of physical harm to a number of people "where there is a convergence between IoT and [Operational Technology]/SCADA/[and Industrial Control Systems], [which] can result in denial of critical services or physical damage." Dependence on such systems ranges from individual to societal. Examples of the former include infrastructure devices (e.g. thermostats, gas and water level detectors and smoke alarms, all of which rely on accurate and timely sensor reporting), and even the use of embedded medical devices (e.g. pacemakers, which one respondent said "can easily be hacked.")

Other cyber security expert survey participants considered targeted attacks with immediate and overt ramifications, saying that "any device which can catch fire, explode, emit whatever, etc. will be hacked to do so," and giving more specific examples, such as "a heater overheating and causing a fire (or similar) or turbines being sped up until they self-destruct."

As previously mentioned, research shows that forensic analysis of attacks through IoT devices is challenging because the IoT collects so much data that it makes "identification, collection, preservation and reporting of evidence" challenging.[406] It is clear that the prevalence of the IoT has the potential to facilitate massive targeting of individual journalists or suspected whistleblowers without likely attribution, which could have a rapid and effective chilling effect on the capabilities of the free press.

4.4.6 Who is responsible for IoT device vulnerabilities?

Media participants were not explicitly asked who they considered to be responsible for the vulnerabilities inherent in IoT devices, rather they were given questions on whose responsibility they considered it to be to improve journalists' understanding of threats through IoT devices, e.g. the journalists themselves, device suppliers, media organisations, etc., and whether participants believed that there was a need for better technical systems as well as knowledge.

---

[404] Paul K (2019) Teen claims to tweet from her smart fridge – but did she really? *The Guardian*, 13 August. Available at: https://www.theguardian.com/technology/2019/aug/13/teen-smart-fridge-twitter-grounded (accessed 9 September 2019).
[405] Maiti A and Jadliwala M (2018) *Light Ears: Information Leakage via Smart Lights*. 23 August. University of Texas at San Antonio: arXiv:1808.07814 [cs]. Available at: http://arxiv.org/abs/1808.07814 (accessed 9 September 2019); Doctorow C (2016) A lightbulb worm could take over every smart light in a city in minutes. In: *Boing Boing*. Available at: https://boingboing.net/2016/11/09/a-lightbulb-worm-could-take-ov.html (accessed 9 September 2019).
[406] Conti M, Dehghantanha A, Franke K, et al. (2018) Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems* 78(2). Elsevier Ltd.: 544–546. DOI: 10.1016/j.future.2017.07.060.

However, both the media industry respondents and cyber security experts mentioned two groups when discussing poor IoT security: (1) Developers, manufacturers, and vendors, for creating and disseminating products with minimal security, and (2) individual consumers, for not educating themselves on IoT security issues and possible mitigation tactics. These groups, the vulnerabilities they enable, and associated threats are all explored in the below table (Table 11).

Actor	**Potential vulnerability**	**Potential threat**
Developers, manufacturers, and vendors	Re-use of code libraries by developers	Reproduces existing weaknesses and illicit access.
	Inability to alter default passwords/settings	Enables further hacking by maintaining continuity of access credentials.
	Insecure communication protocols between devices and servers	Easier to use one compromised device to affect entire network.
	Lack of patches	Fails to address known mass IoT device vulnerabilities.
	Missing/delayed/insufficient updates	
	Displaying plaintext authentication details on devices	Only temporary physical access is needed to access digital information.
	Insufficient information passed on to consumers about how best to protect themselves, e.g. how to change default settings/passwords	Passes burden of security to consumers who may not have sufficient technical understanding and/or tools to protect themselves.
Individual consumers	Using legacy/proven problematic IoT devices	Maintains vulnerabilities of old/unsafe devices and can affect better protected devices that are within the same network.
	Lack of understanding of networked potential of IoT devices	One compromised device can make the whole network easily accessible to attackers.
	Lack of awareness about Wi-Fi security	

Table 11: Actors identified by study participants as being responsible for IoT vulnerabilities

Additionally, participants frequently referred to a more high-level influence on the quality of IoT security: state involvement. 26.9% of cyber security experts surveyed suggested that a potential solution to the long-term issues surrounding IoT security would be petitioning governments to improve relevant laws and policies. One cyber security expert respondent recommended that "the best defence is to educate, agitate and advocate for a legal solution to: Device ownership[,] Liability [and] Commercial surveillance." Here, there is the clear implication that outdated legislation and thus lax regulation are overarching factors regarding IoT security issues, and so governments are at least partially responsible for the current state of affairs.

As discussed, journalists preferred that non-governmental institutions be more involved in designing and implementing any journalism-centric IoT threat education and mitigation strategies, which is indicative of the perceived ineptitude or hostile nature of states' decision-makers. Given the fact that both groups from the above table (Table 11) are affected by state-driven actions, it felt relevant to investigate the national legislative and policy landscape, including aspects of the State-Industrial relationship, as part of the core context in each of the country profile chapters of this thesis (see: Chapters 6 and 7).

4.5 Conclusion

4.5.1 Relevance to this thesis

IoT proliferation across homes, workplaces and social spaces will expand the attack surface surrounding all individuals but will be particularly dangerous to communities that are already targeted. The first research question of this chapter asked, "To what extent do journalists perceive threats from the Internet of Things (IoT)?," to which the answer was that this community does not understand IoT-related threats.

Regarding the second research question of this chapter: "What protective tools and methods do journalists feel are currently effective in increasing their cyber security against all perceived cyber-threats (including any from the IoT)?," some journalist respondents acknowledged that they put in place protections, while others could name none that they felt were necessary. This meant that, when investigating the third research question, "Are the protective measures reported as in use by journalists actually effective, when compared to the known recommendations from contemporary literature and experts in cyber security?", it was determined that any countermeasures employed are either inconsistent or otherwise limited, so journalists do not have adequate protection against IoT threats.

This was done by first, interviewing and surveying a total of 16 members of the media regarding their perceptions of IoT threats to journalists; second, surveying 34 cyber security experts about their knowledge and predictions regarding whether lay-people can avoid or mitigate IoT threats and if so, how this can be achieved; and third, comparing journalists' perceived threat models and individual security behaviours against the expert descriptions of the IoT threat landscape at present and in future, to assess the current and anticipated efficacy of journalists' protective measures, as well as to determine any potential improvements.

Therefore, given the heightened risk that journalists and sources face from information threats, surveyed experts' responses suggest that most mitigation techniques for current and anticipated IoT threat models will only work in the short-term. The experts recommended that the public pursue large-scale structural responses to the predicted IoT market boom (this is explored in Chapters 6, 7, and 9).

Again, although the results of this exploratory study cannot be seen as generalisable, they have corroborated existing research, such as McGregor and Watkins' work which found that journalists'

conceptions of their own digital threat models are unrealistic.[407] There is therefore a clear need for future academic investigation into socio-technical and policy proposals to minimise IoT-related threats to the free press (see: Chapters 8 and 9). Additionally, a continued push by the Human-Computer Interaction Security academic community for design requirements to be shifted to incorporate better device security, so that the onus is not on users to be experts in managing ambient security is crucial (see: Chapter 8). This is especially true regarding investigative journalists, whose work can mean that they have to grapple with targeted physical and legal threats, in addition to the complex combination of emergent threat models presented by the IoT (see: Chapter 5).

4.5.2 Limitations of this exploratory study

In order to anonymise results, any mentions in transcripts of the nationality or location of journalist interviewees were redacted. For this exploratory study, not all media industry participants were based in democratic countries, although this later became the scope for the rest of the thesis. Still, variances in nationality or location did not seem to affect perceptions of threat actors, with journalists from both authoritarian and democratic countries registering their concern about state-affiliated attacks.

This research is focused on strengthening and reinforcing the cyber-physical security of the free press in democratic countries because there is a wealth of research being conducted and published on threats to the free press in authoritarian states, and authoritarian regimes pose a variety of different unchecked threats to journalists and sources, many of which are purely physical. In contrast, democratic states are considered to have checks and balances, such that the threats through the IoT may constitute a greater portion of journalists' threat landscape in those countries than they would to journalists in authoritarian states.

Additionally, as mentioned in this chapter, this study did not ask participants to apportion responsibility to stakeholders for the vulnerabilities in IoT devices. Still their references to the current and potential future impact of legislation and policy broadened the perspective of this chapter on the issue of IoT security, to include these factors in the research for this thesis. Each profiled country's legislative and policy landscape and the actions that governments are undertaking regarding consumer guidance and industry regulation will be explored in the relevant chapters (see: Chapters 6 and 7).

Responses to this exploratory study indicated that news organisations needed to be empowered to create and share threat intelligence, feasible solutions, and mitigation strategies for emerging technological threats. To this end, the next chapter is intended to clarify categories of commercially available IoT devices and to provide examples of many relevant novel threat models that the press can use as a basis for their cyber security strategies and policies in future.

[407] McGregor SE and Watkins EA (2016) "Security by Obscurity": Journalists' Mental Models of Information Security. *#ISOJ* 6(1). The Multimedia Edition of the Official Research Journal of the International Symposium on Online Journalism. Available at: https://isojjournal.wordpress.com/2016/04/14/security-by-obscurity-journalists-mental-models-of-information-security/ (accessed 15 February 2020).

Chapter 5: Conceptual Models

5.1 Introduction

The exploratory study (see: Chapter 4) showed that journalists had an abstract idea that the IoT posed threats to them and to their sources. However, it also surfaced that there was no clear or systematic way of identifying where these threats might occur, how they might be enacted, or what consequences were likely to arise. This is consistent with Oliver's findings that journalistic security training is insufficient and swiftly outdated.[408] This chapter therefore creates models of devices and threats to show the scope and scale of the issue and to demonstrate the need for countermeasures (presented in Chapter 8). This chapter's conceptual models are therefore intended to improve and update an aspect of this training by building a shared vocabulary for communication about the IoT and related threats. This will allow the journalistic community to negotiate priorities, develop communal habits and explicitly share these in order to coordinate collective actions successfully and promptly.[409]

Further, both models are designed to align with organisational objectives, i.e. to be relevant to and used by both facets of the machinery of news organisations: the newsroom and the business.[410] These models are purposefully conceptual and flexible to acknowledge that available IoT devices are heterogeneous in character, and constantly evolving so that no perfect model of either the IoT or its threats can exist.[411] For detailed information on how the conceptual models were created, and how the threat categorisation evolved, see Chapter 3. Within that chapter, section 3.5.2 explains the methodology used to create a review of the literature on IoT threats that underpin this chapter's conceptual models. Further, this chapter's models also draw on 63 interviews conducted with journalists and related experts (see: Chapter 3, section 3.3.2 for participant recruitment information). While the data from these interviews primarily informs Chapters 6 and 7, the models presented here in Chapter 5 also draw on them to ensure that all devices mentioned by interviewees are included in the models. This combination of data sources combines technical computer science and cyber security academic research (via systematic literature review, see Chapters 2 and 3) with the IoT risks perceived by the media industry, to demonstrate the relevance of the IoT to their threat landscape.

Accurate and extensive risk assessments are of particular importance to the media industry, as vulnerabilities are increasingly exploited by well-resourced attackers, primarily nation-states.[412] This is the

[408] Oliver J (2018) Journalism schools still behind on cybersecurity training, new survey finds. Available at: https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php (accessed 15 November 2020); Berdan, K. (2021). CLTC Report: An Evaluation of Online Security Guides for Journalists (p. 48). CLTC UC Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/2021/01/20/cltc-r

[409] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. p. 55.

[410] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. p. 59; Firesmith DG. Security Use Cases. J Object Technol. 2003 Jun;2(3):53–64. p. 53.

[411] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. pp. 49-50.

[412] Zorz Z. Government-backed cyber attackers increasingly targeting journalists [Internet]. Help Net Security. 2020 [cited 2020 Sep 11]. Available from: https://www.helpnetsecurity.com/2020/03/27/cyber-attackers-targeting-journalists/; Reporters Without Borders. RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders [Internet]. RSF. 2020 [cited 2020 Sep 11]. Available from: https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators; Perlroth, N.: Washington Post Joins List of News Media Hacked by the Chinese, https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html, (2013); Huntley, S., Marquis-Boire, M.: Tomorrow's news is today's intel: Journalists as targets and compromise vectors. Black Hat Asia 2014., Singapore (2014); Wagstaff, J.: Journalists, media under attack from hackers: Google researchers, https://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328, (2014).

motivation for primarily discussing state attackers in this thesis, as well as the fact that there is no higher authority in the global arena than the state. States have the ability to pass laws, create and control both physical and social boundaries, and pressure corporations and individuals. This final point is particularly relevant to this thesis because states dictate what qualifies as a public or private space, and legal threats are exclusively set by states. Chapter 6 expands further on the specific ways in which journalists interviewed for this thesis considered the governments of the US, UK, Australia, and Taiwan to threaten their work.

Non-state actors may attack journalists through the IoT for similar reasons to states acting within their own limits, e.g. to identify confidential sources, and may even include states that are exerting their powers transnationally or through proxies.[413] These adversaries are often unable to enact legal restraints against journalists, but, especially when acting criminally, are unfettered in terms of enacting physical threats. Using this chapter's novel conceptual models to become aware of the reach and capabilities of the most powerful threat actors means that journalists will begin to understand the potential for media-specific threats from these emerging technologies. This should allow them to decide the extent to which they want to invest in protections and mitigation strategies (see: Chapter 8) against these state and non-state actors.

This chapter is divided into the two conceptual models, first exploring the IoT devices by environment organisational model, then the IoT threat categorisation system. For each, it will give a rationale for the needs and structure of the model, then it will present the model itself, before going into more detail when discussing the ramifications and limitations of the model.

5.2 Conceptual model 1: IoT devices by environment

The consumer IoT includes technologies from autonomous vehicles[414] to children's and pets' toys,[415] all of which either regularly or constantly collect and convey sensor data and have physical functionalities. Such devices have been viewed as potential novel platforms for audience interaction.[416] However, the omnipresence of IoT devices means that journalists may continually, unknowingly, interact with them.[417] This is an especially likely scenario for journalists whose workflow can span different locations, which can make it difficult for them to recognise the differences in security risks as their environment changes.[418]

[413] Rauta V (2020) Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. *Cambridge Review of International Affairs* 33(6). Routledge: 868–887. DOI: 10.1080/09557571.2019.1656600.
[414] Bryans JW (2017) The Internet of Automotive Things: vulnerabilities, risks and policy implications. Journal of Cyber Policy 2(2). Routledge: 185–194. DOI: 10.1080/23738871.2017.1360926.
[415] Keymolen E and Hof SV der (2019) Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. Journal of Cyber Policy 4(2): 143–159. DOI: 10.1080/23738871.2019.1586970; WESNET Australia (Women's Services Network, Australian Government) (2020) Smart toys & location tracking: privacy & safety concerns with children & pets. In: *TechSafety*. Available at: https://techsafety.org.au/resources/resources-women/toys/ (accessed 6 December 2022).
[416] Mills J, Pellanda E and Pase A (2017) New Interactions. *Journalism Practice* 11(8). Routledge: 980–999. DOI: 10.1080/17512786.2016.1224679.
[417] Maple C (2017) Security and privacy in the internet of things. Journal of Cyber Policy 2(2): 155–184. DOI: 10.1080/23738871.2017.1366536; Constance E (2017) The Internet of Things: preparing for the revolution. *Journal of Cyber Policy* 2(2). Routledge: 152–154. DOI: 10.1080/23738871.2017.1361890.
[418] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.

These unknowing interactions could therefore bypass existing security and privacy measures and present more opportunities and vectors for attacks.[419] Consequently, it is important to establish in which contexts – and therefore how often – a journalist engages IoT devices in their daily life, and to increase awareness among the press of the capabilities of these devices. For this reason, while this conceptual model is not directly included in Chapter 8's framework, an abstracted journalistic workflow is a component of the framework. This is underscored by the NIST CSF function 'Identify,' which recommends identifying both assets and vulnerabilities.[420]

The problem of IoT threats to the free press relates to risk management. This model enables journalists and readers to visualise and conceptualise how IoT devices in different environments may create risks. Further, its user-focused language and organisation empower journalists to begin to use this organisational model for awareness, mitigation, and protective purposes.

This section presents a novel conceptual model to codify and organise IoT devices present in different environments, with examples of how journalists and their work could be impacted, both passively (i.e. via surveillance) or actively (i.e. via information theft). It also discusses how different environments that may contain IoT devices are often under the control of actors whom journalists cannot easily influence, nor protect themselves against. Especially as these devices continue to proliferate, journalistic risk from IoT devices in surrounding environments are growing. It is therefore important to address the contemporary and emerging risks to journalism that are associated with connected devices.

5.2.1 Conceptual model 1 - IoT Devices by Environment (visualisations)

Figure 3 shows the main categories of environments in which journalists may encounter the IoT. This is a visual representation of the tables discussed in section 5.2.3.1, where overlap between categories has also been addressed. Figures 4, 5 and 6 also depict the *private homes, public spaces,* and *workplace* categories. The *wearable* category is not depicted as a separate figure as it does not currently include subcategories. However, in Figure 3, *wearable* devices are portrayed within a ring, to demonstrate that the devices within the other categories cannot be classed as wearables, but that wearables can be found in any of these environments. Each section of the diagrams shows between one and three devices as an example, see section 5.2.2 for a full list of device types within each category.

The main takeaway of this model is that awareness of the ubiquity of IoT locations is likely to be key to enabling journalists to assess their options for protection. This is because many of the devices are beyond their abilities to avoid, for example those found in public transport and public spaces, thus confirming the expert predictions in the exploratory study (see: Chapter 4). This work is future-resistant because device environments and overall purposes are not likely to change, with the exception of more wearable devices being created. Therefore, any future updates to the model will likely involve simply adding new devices as they enter the market, as well as migrating any devices that become portable to the wearable category.

[419] Mohamad Noor M binti and Hassan WH (2019) Current research on Internet of Things (IoT) security: A survey. Computer Networks 148: 283–294. DOI: 10.1016/j.comnet.2018.11.025; Nurse JRC, Creese S and De Roure D (2017) Security Risk Assessment in Internet of Things Systems. IT Professional 19(5): 20–26. DOI: 10.1109/MITP.2017.3680959.
[420] Keller N. Identify: NIST Cybersecurity Framework [Internet]. NIST. 2018 [cited 2020 Sep 11]. Available from: https://www.nist.gov/cyberframework/identify

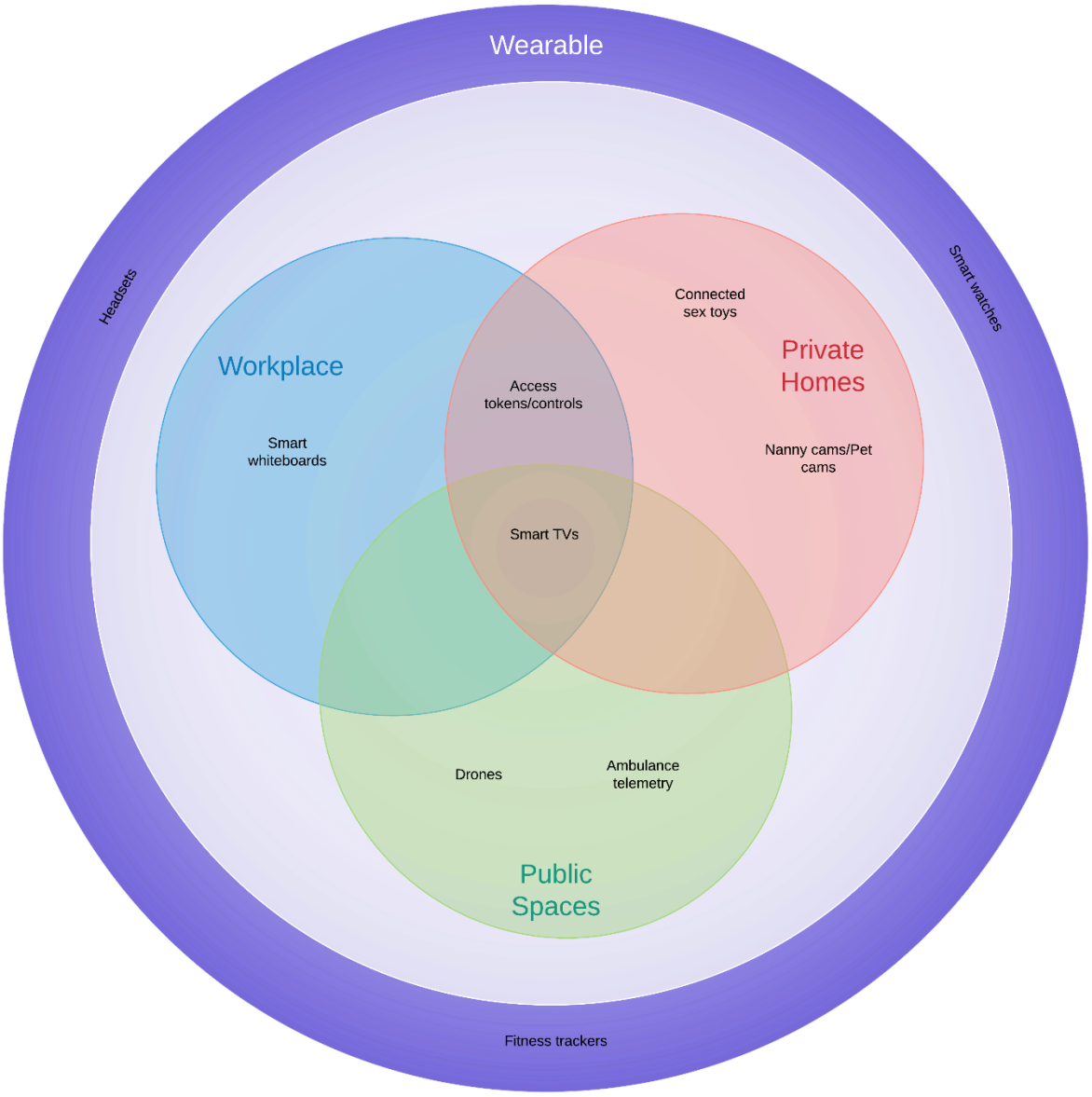


Figure 3: IoT devices organised by environment

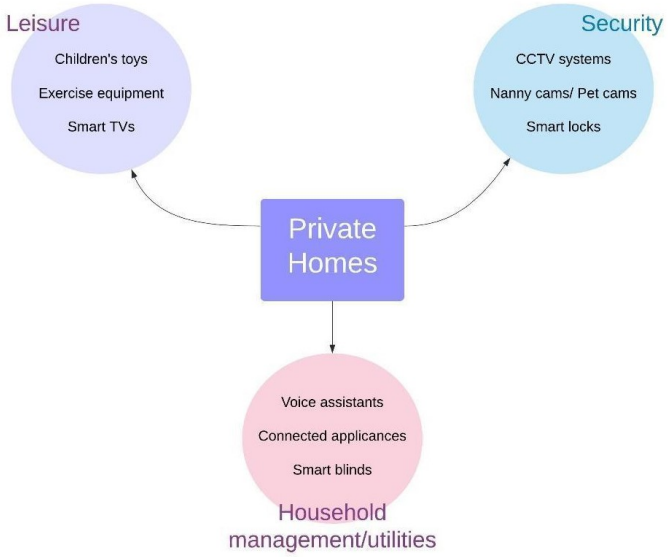


Figure 4: Private homes category

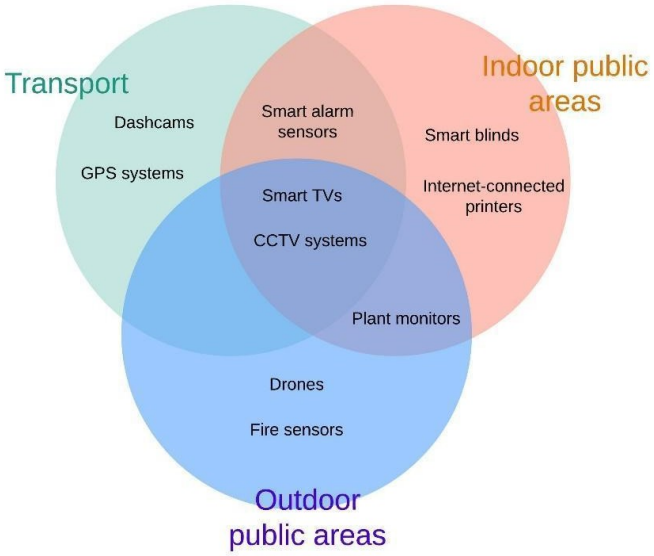


Figure 5: Public spaces category

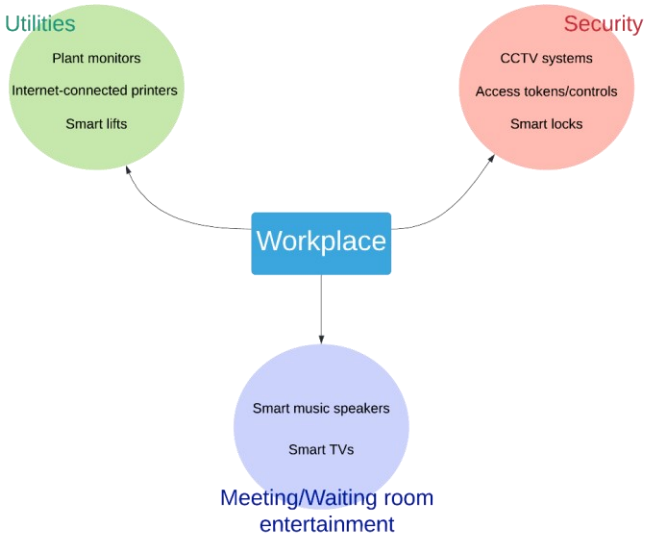


Figure 6: Workplace category

5.2.2 Conceptual model 1 - IoT Devices by Environment (tables with description)

The below table versions of the conceptual model (Tables 12, 13, 14, and 15) develop the visual representations above by providing more detail about the IoT devices that can be found in each category. Further, the inclusion of the "capability" column in this organisational model revealed that all environment categories may contain devices with any listed capability. More information on all categories can be found in Chapter 3, section 3.5.2.1.

Table 12 displays the *private homes* category in table form.

Private homes		
Purpose	**Item**	**Capability**
Household management/utilities	Voice assistants (e.g. Google Home, Amazon Echo, Siri, Xiao Ai)	Microphone/ Presence Sensor/ User Account
	Remote-access HVAC systems (e.g. thermostats)	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
	Remote-controlled lighting systems	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
	Internet-connected printers	Manual Activation/ User Account
	Internet-connected vacuum cleaners (e.g. Roombas)	Manual Activation/ Presence Sensor
	Smart blinds	Timed Activation/ Manual Activation/ Environment Sensor

	Connected appliances, White Goods (e.g. washing machines, fridges, cookers, toilets)[421]	Microphone/ Camera/ Environment Sensor/ Consumption Sensor/ Timed Activation/ Manual Activation/ Weather Display/ Integrated Web Browser/ Integrated Television/ User Account
	Smart electricity/ gas/ water meters	Consumption Sensor
	Smart lifts (in accessible housing)	Manual Activation/ Presence Sensor
	Plant monitoring and irrigation systems[422]	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
	Garage door-openers	Manual Activation/ Presence Sensor
	Access tokens/controls (e.g. RFID, near field communication devices)	Presence Sensor/ Manual Activation/ User Account
Leisure	Smart music speakers	Microphone/ Manual Activation/ Timed Activation/ Integrated Web Browser/ User Account
	Smart TVs	Microphone/ Camera/ Manual Activation/ Integrated Web Browser/ Integrated Television/ Weather Display/ User Account
	Children's toys[423]	Camera/ Microphone/ Presence Sensor/ Environment Sensor/ Medical/Health Reader/ Manual Activation/ User Account/ GPS/ Integrated Web Browser/ Integrated Television/ Weather Display/ Timed Activation
	Exercise equipment (e.g. Peloton standing bikes, which have an internet connection for live streaming of workouts)	Camera/ Microphone/ Presence Sensor/ Environment Sensor/ Medical/Health Reader/ Manual Activation/ User Account/ GPS/ Integrated Web Browser/ Integrated Television/ Weather Display/ Timed Activation
	Gaming equipment (e.g. Xbox consoles that allow access to Xbox Live)	Camera/ Microphone/ Presence Sensor/ Environment Sensor/ Medical/Health Reader/ Manual Activation/ User Account/ GPS/ Integrated Web Browser/ Integrated

[421] Park S, Won DD, Lee BJ, et al. (2020) A mountable toilet system for personalized health monitoring via the analysis of excreta. *Nature Biomedical Engineering* 4(6). 6. Nature Publishing Group: 624–635. DOI: 10.1038/s41551-020-0534-9.
[422] Carrión G, Huerta M and Barzallo B (2018) Monitoring and irrigation of an urban garden using IoT. In: 2018 IEEE Colombian Conference on Communications and Computing (COLCOM), Colombia, May 2018, pp. 1–6. IEEE. DOI: 10.1109/ColComCon.2018.8466722.
[423] Federal Bureau of Investigation (FBI) (2017) *Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*. Internet Crime Complaint Center (IC3) Alert Number I-071717 (Revised)-PSA, 17 July. USA: Federal Bureau of Investigation (FBI). Available at: https://www.ic3.gov/Media/Y2017/PSA170717 (accessed 7 January 2021).

		Television/ Weather Display/ Timed Activation
	Static connected health devices (e.g. connected sex toys and Wi-Fi-enabled weighing scales)	Camera/ Microphone/ Presence Sensor/ Environment Sensor/ Medical/Health Reader/ Manual Activation/ User Account/ GPS/ Timed Activation
Security	CCTV systems	Camera
	Smart doorbells (e.g. Ring or Nest)	Camera/ Microphone
	Smart locks	Presence Sensor/ Manual Activation/ User Account
	Nanny cams/Pet cams	Camera/ Microphone/ User Account/ Presence Sensor/ Manual Activation
	Smart alarm sensors	Camera/ Microphone/ User Account/ Presence Sensor/ Timed Activation/ Manual Activation
	Smart pet door/flap[424]	Presence Sensor/ Manual Activation/ User Account/ Environment Sensor

Table 12: Private homes category

Table 13 displays the *public spaces* category in table form.

Public spaces		
Purpose	**Item**	**Capability**
Transport (can be public, semi-public, or private)	Smart vehicles	Camera/ Microphone/ Presence Sensor/ Environment Sensor/ Consumption Sensor/ GPS/ Manual Activation/ Weather Display/ Integrated Web Browser/ Integrated Television/ User Account
	CCTV systems	Camera
	Smart TVs	Microphone/ Camera/ Manual Activation/ Integrated Web Browser/ Integrated Television/ Weather Display/ User Account
	GPS systems (e.g. Garmins/ TomToms, etc.)	GPS/ Weather display

[424] Zhang W, Abdulghani AM, Imran MA, et al. (2020) Internet of Things (IoT) enabled Smart Home Safety Barrier System. In: *Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things*, New York, NY, USA, 24 April 2020, pp. 82–88. CNIOT2020. Association for Computing Machinery. DOI: 10.1145/3398329.3398341.

	Dashcams	Camera/ Microphone/ User Account/ Manual Activation
	Parts of a car, e.g. wireless tire pressure sensors, engine monitors, speed accelerators	Camera/ Microphone/ Presence Sensor/ Environment Sensor/ Manual Activation/ User Account/ GPS/ Integrated Web Browser/ Integrated Television/ Weather Display/ Timed Activation
	Vehicle-enabled internet access or Bluetooth connection	Manual Activation/ Integrated Web Browser/ User Account
	Electric vehicle chargers	Consumption Sensor
	Ambulance telemetry	GPS/ Weather display
	Smart alarm sensors	Camera/ Microphone/ User Account/ Presence Sensor/ Timed Activation/ Manual Activation
	Self-driving vehicles	Camera/ Microphone/ Presence Sensor/ Environment Sensor/ Consumption Sensor/ GPS/ Manual Activation/ Weather Display/ Integrated Web Browser/ Integrated Television/ User Account
Outdoor public areas (e.g. parks, squares, carparks, skateparks, woods, industrial parks)	Smart TVs	Microphone/ Camera/ Manual Activation/ Integrated Web Browser/ Integrated Television/ Weather Display/ User Account
	CCTV systems	Camera
	Smart streetlights	Timed Activation
	Plant monitoring and irrigation systems[425]	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
	Pipeline leak detection	Environment Sensor
	Traffic control	Camera/ Presence Sensor/ Environment Sensor/ Timed Activation
	Fire sensors	Environment Sensor

[425] Carrión G, Huerta M and Barzallo B (2018) Monitoring and irrigation of an urban garden using IoT. In: 2018 IEEE Colombian Conference on Communications and Computing (COLCOM), Colombia, May 2018, pp. 1–6. IEEE. DOI: 10.1109/ColComCon.2018.8466722.

	Drones (e.g. camera-equipped)	Camera/ Presence Sensor/ Environment Sensor/ Consumption Sensor/ GPS/ Manual Activation/ Timed Activation/ User Account
Indoor public areas (e.g. medical facilities, banks, supermarkets, cafes/coffee shops, restaurants, bars, museums, shops, galleries, libraries, clubs, cinemas, gyms, pools, warehouses)	Remote-access HVAC systems (e.g. thermostats)	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
	Remote-controlled lighting systems	Environment Sensor/ Manual Activation/ User Account Sensor/ Timed Activation
	Smart TVs	Microphone/ Camera/ Manual Activation/ Integrated Web Browser/ Integrated Television/ Weather Display/ User Account
	Internet-connected printers	Manual Activation/ User Account
	Internet-connected vacuum cleaners (e.g. Roombas)	Manual Activation/ Presence Sensor
	Smart blinds	Timed Activation/ Manual Activation/ Environment Sensor
	Smart lifts	Manual Activation/ Presence Sensor
	CCTV systems	Camera
	Smart alarm sensors	Camera/ Microphone/ User Account/ Presence Sensor/ Timed Activation/ Manual Activation
	Plant monitoring and irrigation systems[426]	Environment Sensor/ Manual Activation/ User Account/ Timed Activation Sensor
	Smart electricity/ gas/ water meters	Consumption Sensor

Table 13: Public spaces category

Table 14 displays the *workplace* category in table form.

Workplace (e.g. office/ school)		
Purpose	**Item**	**Capability**

[426] Carrión G, Huerta M and Barzallo B (2018) Monitoring and irrigation of an urban garden using IoT. In: 2018 IEEE Colombian Conference on Communications and Computing (COLCOM), Colombia, May 2018, pp. 1–6. IEEE. DOI: 10.1109/ColComCon.2018.8466722.

Waiting/meeting room entertainment	Smart music speakers	Microphone/ Manual Activation/ Timed Activation/ Integrated Web Browser/ User Account
	Smart TVs	Microphone/ Camera/ Manual Activation/ Integrated Web Browser/ Integrated Television/ Weather Display/ User Account
Utilities	Internet-connected printers	Manual Activation/ User Account
	Remote-controlled lighting systems	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
	Remote-access HVAC systems (e.g. thermostats)	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
	Smart whiteboards	Microphone/ Camera/ Manual Activation/ Integrated Web Browser/ Integrated Television/ Weather Display/ User Account
	Internet-connected vacuum cleaners (e.g. Roombas)	Manual Activation/ Presence Sensor
	Smart blinds	Timed Activation/ Manual Activation/ Environment Sensor
	Smart electricity/ gas/ water meters	Consumption Sensor
	Smart lifts	Manual Activation/ Presence Sensor
	Connected appliances, White Goods (e.g. washing machines, fridges, cookers, toilets)	Microphone/ Camera/ Environment Sensor/ Consumption Sensor/ Timed Activation/ Manual Activation/ Weather Display/ Integrated Web Browser/ Integrated Television/ User Account
	Plant monitoring and irrigation systems[427]	Environment Sensor/ Manual Activation/ User Account/ Timed Activation
Security	Smart alarm sensors	Camera/ Microphone/ User Account/ Presence Sensor/ Timed Activation/ Manual Activation
	CCTV systems	Camera
	Smart locks	Presence Sensor/ Manual Activation/ User Account
	Access tokens/controls (e.g. RFID, near field communication devices)	Presence Sensor/ Manual Activation/ User Account
	Garage door-openers	Manual Activation/ Presence Sensor

Table 14: Workplace category

[427] Carrión G, Huerta M and Barzallo B (2018) Monitoring and irrigation of an urban garden using IoT. In: 2018 IEEE Colombian Conference on Communications and Computing (COLCOM), Colombia, May 2018, pp. 1–6. IEEE. DOI: 10.1109/ColComCon.2018.8466722.

Table 15 displays the *wearable* category in table form.

Wearable (NB: These can be found in any environment, so please always cross reference a specific environment with this category)		
Purpose	**Item**	**Capability**
Functionality	Smart watches (e.g. radio/Bluetooth-enabled Casio watches)	Microphone/ Presence Sensor/ Environment Sensor/ Medical/Health Reader/ GPS/ Timed Activation/ Manual Activation/ Weather Display/ Integrated Web Browser/ Integrated Television/ User Account
	Augmented reality headsets/ glasses (e.g. Google Glass)/ smart contact lenses	Camera/ Microphone/ User Account/ Integrated Web Browser/ GPS/ Weather Display/ Integrated Television/ Manual Activation
	Internet-connected clothes	Medical/Health Reader
	Pet wearables[428]	GPS/ Medical/Health Reader/ User Account/ Environment Sensor/ Presence Sensor
Security	Keychain finders with GPS beacons (e.g. Apple AirTags)	GPS/ Manual Activation
Health	Smart organs/ implants	Medical/Health Reader
	Smart pills	Medical/Health Reader
	Sleep monitoring devices (e.g. Oura Sleep Ring)	Medical/Health Reader/ User Account
	Portable connected medical devices (e.g. blood pressure meters, weight sensors in shoes, and blood sugar monitors)	Presence Sensor/ Environment Sensor/ Medical/Health Reader/ Manual Activation/ User Account/ GPS/ Timed Activation
	Fitness trackers (e.g. Fitbits)	Presence Sensor/ Environment Sensor/ Medical/Health Reader/ GPS/ Manual Activation/ User Account

Table 15: Wearable category

5.2.3 Discussion

5.2.3.1 Significant threats within each category

This categorisation system gives an insight into the risks to journalistic work in many environments, as well as raising awareness of the ubiquity of *wearable* devices. For example, within the *private homes* category, two devices (access tokens and GPS trackers) fit into the intersection of all four subcategories.

[428] van der Linden D, Edwards M, Hadar I, et al. (2020) Pets without PETs: on pet owners' under-estimation of privacy concerns in pet wearables. In: Proceedings on Privacy Enhancing Technologies 2020, Virtual, 1 January 2020, pp. 143–164. Sciendo. DOI: 10.2478/popets-2020-0009; Zhang W, Abdulghani AM, Imran MA, et al. (2020) Internet of Things (IoT) enabled Smart Home Safety Barrier System. In: *Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things*, New York, NY, USA, 24 April 2020, pp. 82–88. CNIOT2020. Association for Computing Machinery. DOI: 10.1145/3398329.3398341.

This may mean that the number of these devices present in private homes is particularly high and, given the likely portability and unobtrusiveness of such devices, they may increase the risk of a journalist being tracked or their pattern of life being identified.[429]

Similarly, regarding *public spaces*, smart TVs and CCTV systems exist in all subcategories. While *outdoor public areas* such as car parks might seem stark, they can contain less overt IoT devices, likely including CCTV systems that upload footage to the Cloud, which state and criminal actors might access to identify sources. In the *indoor public areas* category, the main risk may stem from the lack of control that individuals have over the devices with which they would interact. Often, the IoT devices in this category do not have interfaces that are accessible by lay people, and also have little inbuilt security. Therefore, if a technically-capable adversary identifies that a journalist interacts with such a device, they could exploit this knowledge without the target either realising that this is happening or being able to counter the threat.

In the *workplace* category, many of the devices are likely to be used to access or otherwise engage with a journalist's work. There are additional factors that threaten journalists' ability to actively recognise and avoid interaction with these devices, such as whether they have been absorbed into the culture of an office or into routines required by an editor or boss. Not only may these devices be difficult to observe in isolation when they are part of a chain of expected technological actions, but they may also have secondary functionalities that are likewise subversive (see: section 5.3.2.1 for an example). Devices in an office may also be both owned, installed and controlled by different actors (such as the news organisation's owner, the manufacturer, and the Head of IT)[430], which makes their threats tricky to include in risk assessments or even to communicate to journalists. All these factors pose a high risk to both intentionally unpublished material and unnamed sources who might be identifiable from the information that is (for example) retained by a smart printer.

Overall, smart televisions are present in all static (i.e. non-*wearable*) core categories and were mentioned by multiple interviewees (see: Chapters 6 and 7) as being concerning.[431] This is particularly significant because their additional IoT-relevant characteristics are designed to be unobtrusive. In fact, interviewees have mentioned that these are notably prevalent, poorly secured and easily manipulated by adversaries to harm journalists and sources, particularly when they incorporate additional data collection features such as cameras and microphones.[432] Further, there is ample evidence that some smart televisions track on-screen user activities, some of these devices incorporate microphones, and many of them have poor security and non-existent encryption.[433] It therefore seems probable that journalists would also not

[429] Bugeja J, Jacobsson A and Davidsson P (2020) Is Your Home Becoming a Spy? A Data-Centered Analysis and Classification of Smart Connected Home Systems. In: 2020, p. 8; Vetrivel S, van Harten V, Gañán CH, et al. (2023) Examining Consumer Reviews to Understand Security and Privacy Issues in the Market of Smart Home Devices. In: *Proceedings of the 32nd USENIX Security Symposium*, Anaheim, CA, USA, 9 August 2023, p. 18. USENIX Association. Available at: https://www.usenix.org/system/files/sec23summer_454-vetrivel-prepub.pdf; Nascimento DR, Ciano MP, Gumz J, et al. (2022) The acceptance process of smart homes by users: a statistical meta-analysis. *Behaviour & Information Technology* 0(0). Taylor & Francis: 1–18. DOI: 10.1080/0144929X.2022.2146534.

[430] Bugeja J, Jacobsson A and Davidsson P (2020) Is Your Home Becoming a Spy? A Data-Centered Analysis and Classification of Smart Connected Home Systems. In: 2020, p. 8.

[431] Interviewees: P24, P46, P6, P51, P44, P8, P34

[432] Interviewee: P6

[433] Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2017. 240 p; Varmarken J, Le H, Shuba A, et al. (2020) The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking. Proceedings on Privacy Enhancing Technologies 2020(2). Sciendo: 129–154. DOI: 10.2478/popets-2020-0021; Lawler R. Vizio IPO plan shows how its TVs track what you're watching [Internet]. Engadget. 2015 [cited 2020 Oct 26]. Available from: https://www.engadget.com/2015-07-24-vizio-ipo-inscape-acr.html; Constantin L. Smart TVs raise privacy concerns

recognise or consider that screens mounted in public places would also have these capabilities. However, the second categorisation system (of threat models) will provide more information about the threat level associated with various mentioned devices.

Although, as previously mentioned, there are currently no confirmed cases of journalists being targeted through novel IoT devices, there is evidence of this happening through coercive and controlling use of the IoT in Intimate Partner Violence situations.[434] Further, interviewees for Chapters 6 and 7 explicitly recognised similar IoT threats to journalists, including attacks on the confidentiality, integrity or availability of smart medical devices, which could be used to psychologically, financially and physically harm journalists and sources - as well as providing sensitive data to adversaries because of their use of the Cloud.[435] They also suggested media-specific IoT threats, such as retroactively editing published articles,[436] or otherwise psychologically injuring journalists and harming their reputation .[437]

There have also separately been instances of journalists attacked using other technologies, such as Marie Colvin, a foreign correspondent for The Sunday Times whose assassination occurred when the building she was in was identified due to signals from a satellite phone.[438] Given the increasing capabilities of IoT devices, it is important that journalists be made aware of their prevalence. Further, in countries where likely threat actors include states, organised criminal groups, corporations, and rogue adversaries, it is necessary for press security training to spark an understanding of the kinds of devices that exist and where they can be found.

5.2.3.2 Challenging areas and limitations

A limitation of this organisational model could be that it does not clearly exclude non-consumer IoT devices, despite the consumer IoT being the core focus of this thesis. However, the purpose of this specific model is not to distinguish between consumer and non-consumer IoT technologies, but rather to shine a spotlight on the omnipresence of internet-connected devices in most, if not all, of the spaces that journalists might visit on a regular, unthinking, basis. This thesis acknowledges that some consumer IoT devices can be found in public,[439] and refers to them as "informal" additions to state infrastructure, although some resources consider consumer IoT devices used to collect data to improve the operation of

[Internet]. Computerworld. 2015 [cited 2020 Oct 26]. Available from: https://www.computerworld.com/article/2881715/smart-tvs-raise-privacy-concerns.html; Goodin D. Man-in-the-middle attack on Vizio TVs coughs up owners' viewing habits [Internet]. Ars Technica. 2015 [cited 2020 Oct 26]. Available from: https://arstechnica.com/information-technology/2015/11/man-in-the-middle-attack-on-vizio-tvs-coughs-up-owners-viewing-habits/; Constantin L. Samsung smart TVs don't encrypt the voice data they collect [Internet]. Computerworld. 2015 [cited 2020 Oct 26]. Available from: https://www.computerworld.com/article/2885775/samsung-smart-tvs-dont-encrypt-the-voice-data-they-collect.html.

[434] Lopez-Neira I, Patel T, Parkin S, et al. (2019) 'Internet of Things': How Abuse is Getting Smarter. ID 3350615, SSRN Scholarly Paper, 11 March. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.3350615.

[435] Interviewees: P51, P62

[436] Interviewees: P51, P54

[437] Interviewee: P54

[438] RadioFreeEurope/RadioLiberty (2012) Marie Colvin's Death Raises Concerns About Use Of Satellite Phones. Available at: https://www.rferl.org/a/marie_colvin_death_concerns_about_safe_use_satelite_phones/24495230.html (accessed 19 November 2020).

[439] Department for Digital, Culture, Media & Sport and Lopez (MP) J (2022) Secure connected places (smart cities) guidance collection. Available at: https://www.gov.uk/government/publications/secure-connected-places-smart-cities-guidance-collection (accessed 5 December 2022).

services for civilians to be part of smart cities.[440] For the purpose of the IoT device organisational models, some elements of smart cities (e.g. public transport) were necessary to capture the full picture of the IoT with which journalists are likely to interact on a daily basis. However, scaling the IoT up to smart cities and other non-consumer technologies, such as industrial control systems, widened the scope of the DPhil too much to be included in other parts of the research.

Areas that presented a challenge to subcategorisation of the *workplace* category included devices containing access tokens or portable devices with GPS trackers, both of which could fall into all subcategories. For example, a gym used by residents of an entire apartment complex might require a digital access key, hosted on a smart watch that additionally tracks location. This issue was resolved through the creation of the *wearable* category.

The goal is for this conceptual model to be used by journalists, so it must have an easily understandable layout that can be updated in future both with new devices and new categories as needed. For example, for future, more complicated versions of this conceptual model, vertical and horizontal axes could be added, perhaps relating to physical functionality or number of sensors likely found in different devices, so that the more complex diagram could be used to both capture a wider range of features and also predict new elements based on more dimensions of analysis.[441] However, given that both a review of the literature and the exploratory study have demonstrated a lack of knowledge of the IoT among journalists, this simplified Venn diagram matrix should be easily comprehensible and navigable for lay people in media organisations to use as a starting point to design risk management practices, because it clearly shows how a variety of IoT devices overlap in scope and location, with facets designed based on perceptions of user needs[442].

5.2.4 Conceptual model 1 - Summary

Although conceptual models classifying and stratifying IoT devices already exist, these are largely aimed at readers with technical or computer science backgrounds and they assume a baseline understanding of protocols and processes.[443] Some individuals within the media industry have an understanding of which IoT devices exist and when, how, and where they might encounter IoT devices. However, this knowledge is neither prevalent, nor consistent, thereby ensuring that comprehensive risk assessments are impossible both individually and across the industry.[444]

---

[440] Arroub A, Zahi B, Sabir E, Sadik M (2016) A literature review on Smart Cities: Paradigms, opportunities and open problems. In: 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), October 2016, pp. 180–186. DOI: 10.1109/WINCOM.2016.7777211.

[441] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. p. 105.

[442] Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited; 2007. pp. 42, 68, 123-124.

[443] Weinberg, B.D., Milne, G.R., Andonova, Y.G., Hajjat, F.M.: Internet of Things: Convenience vs. privacy and secrecy. Business Horizons. 58, 615–624 (2015). https://doi.org/10.1016/j.bushor.2015.06.005; Alkhabbas, F., Spalazzese, R., Davidsson, P.: Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. Internet of Things. 7, 100084 (2019). https://doi.org/10.1016/j.iot.2019.100084; Mountrouidou, X., Billings, B., Mejia-Ricart, L.: Not just another Internet of Things taxonomy: A method for validation of taxonomies. Internet of Things. 6, 100049 (2019). https://doi.org/10.1016/j.iot.2019.03.003; Dorsemaine, B., Gaulier, J.-P., Wary, J.-P., Kheir, N., Urien, P.: Internet of Things: A Definition Taxonomy. In: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies. pp. 72–77. IEEE, Cambridge, UK (2015). https://doi.org/10.1109/NGMAST.2015.71.

[444] Shere, A.R.K., Nurse, J.R.C., Flechais, I.: "Security should be there by default": Investigating how journalists perceive and respond to risks from the Internet of Things. Presented at the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) September 1 (2020). https://doi.org/10.1109/EuroSPW51379.2020.00039.

Increasing the understanding of risks to non-technical journalists via this conceptual model can enable them to identify aspects of their life that may give rise to IoT threats. Journalists could then communicate these issues to security professionals, either at news organisations or at civil society organisations.[445] This allows the creation of meaningful risk assessments and threat mitigation methods through collaborative efforts, as it would encourage media threat intelligence sharing that includes IoT threats.

5.3 Conceptual model 2 - IoT threat categorisation system

The general security ramifications of the expansion of the consumer IoT have been widely discussed.[446] However, there are few user-specific assessments of privacy and security threats that can be enacted using IoT devices, and none relating to journalists. Chapter 4's exploratory study determined that this community is particularly vulnerable to IoT threats because of a lack of understanding of how these new technologies could increase risk to the work and wellbeing of members of the press and their sources, and of what can be done to mitigate these threats.[447] Further, journalists merit being the focus of research into IoT threats because of the public-facing nature of their job, which increases their risk level,[448] and also means that any consequences of successful attacks may extend far beyond an individual journalist and potentially destabilise other democratic infrastructure.[449]

[445] Tsui, L., Lee, F.: How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. Journalism. 00, 1–23 (2019). https://doi.org/10.1177/1464884919849418.

[446] Nurse, J., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S.: Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things. In: Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT). , Vienna, Austria (2015); Tanczer, L.M., Steenmans, I., Elsden, M., Blackstock, J., Carr, M.: Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? In: Living in the Internet of Things: Cybersecurity of the IoT - 2018. p. 33 (9 pp.)-33 (9 pp.). Institution of Engineering and Technology, London, UK (2018); Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., Qian, F.: Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 1381–1396. IEEE, Stockholm, Sweden (2019).

[447] McGregor, S.E., Charters, P., Holliday, T., Roesner, F.: Investigating the Computer Security Practices and Needs of Journalists. In: Proceedings of the 24th USENIX Security Symposium. p. 17. USENIX Association, Washington, D.C. (2015); McGregor, S.E., Watkins, E.A., Al-Ameen, M.N., Caine, K., Roesner, F.: When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. In: Proceedings of the 26th USENIX Security Symposium. p. 19. USENIX Association, Vancouver, BC, Canada (2017); McGregor, S.E., Watkins, E.A.: "Security by Obscurity": Journalists' Mental Models of Information Security. #ISOJ. 6, (2016); Shere, A.R.K., Nurse, J.R.C., Flechais, I.: 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. Presented at the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) September 1 (2020).

[448] Phillips, G.: How the free press worldwide is under threat, https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat, (2020); The Nobel Prize: The Nobel Peace Prize 2021, https://www.nobelprize.org/prizes/peace/2021/press-release/; Ball, J.: GCHQ captured emails of journalists from top international media, https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post, (2015); Pegg, D., Lewis, P., Safi, M., Lakhani, N.: FT editor among 180 journalists identified by clients of spyware firm, https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware, (2021); Woodhams, S.: Spyware: An Unregulated and Escalating Threat to Independent Media, https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/, (2021); Reporters Without Borders. RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders [Internet]. RSF. 2020 [cited 2020 Sep 11]. Available from: https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators

[449] Pickard, V.: Restructuring Democratic Infrastructures: A Policy Approach to the Journalism Crisis. Digital Journalism. 8, 704–719 (2020). https://doi.org/10.1080/21670811.2020.1733433; Stotzky, I.P.: The Role of a Free Press and Freedom of Expression in Developing Democracies. U. Miami L. Rev. 56, 255 (2001); Council of Europe: The 2019 Annual Report by the partner organisations of the Council of Europe's Platform for the Protection of Journalism and Safety of Journalists: 'Democracy at Risk: threats and attacks against media freedom in Europe'. Council of Europe, Council of Europe, Avenue de l'Europe F-67075 Strasbourg Cedex, France (2019).

Educating the press about such threats is crucial because the IoT is inherently and systemically insecure, demonstrated by a survey that showed both that "almost 70% of all IoT devices [are] prone to privacy threats" and "every IoT device is responsible for at least one piece of personal information collection."[450] As journalists are already highly targeted, any interaction that they may have with the consumer IoT creates a concerning expansion of their attack surface. Comprehensive risk assessments cannot be carried out without accurate threat modelling that facilitates prioritisation of security strategies and techniques.

As the IoT is an evolving and growing phenomenon, it is impossible to identify all associated risks and the threats from which they arise. Therefore, this chapter uses existing literature to propose a novel conceptualisation that explores ways in which these threats can manifest against the press, largely relating to surveillance.[451] Both section 3.5.2.2.2 of Chapter 3 and Appendix D discuss and demonstrate a previous iteration of the threats categorisation. These earlier versions were refined to produce the version in this chapter, which has been peer-reviewed and published.[452] These new IoT threat categories explore impacts and implications of IoT devices for the media, to increase understanding of the societal effects of surveillance and kinetic threats to journalists from these technologies. Interviews conducted by this author have shown that while general expectations consider IoT attacks against journalists as black swan events, attacks of this kind are realistic and increasingly likely.[453] This gap between expectation and reality is exactly what this conceptual model and, more broadly, the work of this DPhil hope to fill.

5.3.1 Conceptual model 2 - IoT Threat Models

This threat categorisation represents an initial exploratory step toward categorising and conceptualising threats in the context of a specific target population. It categorises nineteen IoT-specific threats that have the potential to harm journalists' work and wellbeing into six categories. The goal is not a complete or definitive threat taxonomy, but rather to present six clear and relevant categories of threats, described in detail in this section: (1) regulatory gaps, (2) legal threats, (3) profiling threats, (4) tracking threats, (5) data and device modification threats, and (6) networked devices threats. See Chapter 3 for more information on how the categories were created.

All six categories are technically possible and ranking them in order of likelihood of occurrence is difficult because the IoT is currently rapidly growing and expanding in scope, and likely threat actors against journalists (e.g. nation-states and organised criminal groups) are not hindered by the cost associated with prolonged or layered attacks. Some of these threats are less likely than those that simply require the journalist to have a phone, as there are well-established threats to journalists that have similar consequences, such as spyware.[454] However, for journalists who are engaging with the security advice that is media-focused and relates to traditional technologies, the IoT may be an overlooked area of risk. For example, journalists may be aware of overzealous data collection by IoT devices such as voice

[450] Gulzar, M., Abbas, G.: Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET). pp. 1–6. IEEE, Lahore, Pakistan (2019).
[451] Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L., Deibert, R.: The Information Security Cultures of Journalism. Digital Journalism. 0, 1–24 (2020). https://doi.org/10.1080/21670811.2020.1777882.
[452] Shere ARK, Nurse JRC and Martin AP (2022) Threats to journalists from the consumer Internet of Things. In: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Wales, UK, 20 June 2022, p. 230. Springer Nature. Springer. Available at: https://link.springer.com/book/9789811964138 (accessed 27 September 2022).
[453] Interviewees: P36, P50
[454] Kenyon, M.: Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes, https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/, (2019); Rueckert, P.: Pegasus: The new global weapon for silencing journalists, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/, (2021); Scott-Railton, J., Marczak, B., Razzak, B.A., Crete-Nishihata, M., Deibert, R.: Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware. University of Toronto, The Citizen Lab (2017).

assistants,[455] [456] but may not recognise the possibility of use of the voice recordings to activate other devices' functionalities without their knowledge (see category 6), nor consider the implications of biometric "voice-profiling" to derive inferences from voice indicators that enable microtargeting of news items and commercial adverts.[457]

The six categories of threat involve varying degrees of risk, with the severity of different threats depending on the individual circumstances and work of each journalist, their colleagues, and their sources. This is supported by McGregor's findings that there are many different attacks that may be executed against any member of the media because "there will always be entities interested in influencing, accessing, or restricting your coverage," and that the resources needed to execute each attack differ depending on the target.[458] Therefore, an attack on one journalist may be enacted in order for an adversary to access another person at the same news organisation. In fact, threats can occur in tandem; for example, a fitness tracker dataset of millions of users may allow easy isolation of a specific journalist's account data (category 4), which would potentially identify their home address and the locations where they meet sources if usernames are cross-referenced with information found on the public-facing social media page of a high-profile journalist (category 3). This could lead to threats to the journalist's specific device (categories 5 and 6). The complexity of multiple steps, as detailed in this example, may make such an attack less likely than a single example from one category, but the compounding potential of these threats is an important feature of networks such as the IoT.[459]

It is important to not to blame users of the IoT for the threats associated with such devices. That is why this threat categorisation includes regulatory gaps as a category to highlight the fact that the commodification of data is integral to the technology industry.[460] This is a theme underpinning all categories and their contents, as information collection – and, in some cases, leakage – is an intentional feature of IoT technologies, rather than a bug.[461] As a result, users are most likely to face risks not from incorrectly using the devices, but from the inherent properties of the devices that cannot be avoided.

Each category has its own description, threat titles, descriptions of some associated threats, and example consequences to illustrate how they would specifically harm press freedom. The chosen structure of method of categorisation is informed by the utility of communicating consequences as scenarios to a

[455] Seymour W, Zhan X, Cote M, et al. (2022) A Systematic Review of Ethical Concerns with Voice Assistants. arXiv:2211.04193. London, UK: arXiv. Available at: http://arxiv.org/abs/2211.04193 (accessed 6 December 2022).
[456] Ahmad I, Akter T, Buher Z, et al. (2022) Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW2): 364:1-364:31. DOI: 10.1145/3555089.
[457] Turow J (2021) Journalism and the Voice Intelligence Industry. *Digital Journalism* 9(7). Routledge: 1000–1006. DOI: 10.1080/21670811.2020.1829979.
[458] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[459] De Roure D, Hooper C, Page K, et al. (2015) Observing Social Machines Part 2: How to Observe? In: *Proceedings of the ACM Web Science Conference*, New York, NY, USA, 28 June 2015, pp. 1–5. WebSci '15. Association for Computing Machinery. DOI: 10.1145/2786451.2786475.
[460] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[461] Meteriz, Ü., Fazıl Yıldıran, N., Kim, J., Mohaisen, D.: Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In: 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). pp. 464–473 (2020); Hassan, W.U., Hussain, S., Bates, A.: Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide? Presented at the 27th USENIX Security Symposium (USENIX Security 18) (2018); Sadowski, J.: When data is capital: Datafication, accumulation, and extraction. Big Data & Society. 6, 2053951718820549 (2019). https://doi.org/10.1177/2053951718820549; Käll, J.: The Materiality of Data as Property. Harvard International Law Journal. 61, 1–11 (2020).

narrative driven audience such as the media.[462] Due to the difficulty of finding confirmed examples because IoT threats can be clandestine,[463] this threat categorisation extrapolates from existing IoT capabilities and evidence of the facilitation of malicious activities.[464] Specifically, the use of scenarios in Tanczer *et al.* influenced the presentation of Chapter 5's threat categorisation descriptions of hypothetical consequences for journalists, as did P. W. Singer's recommendation of FicInt as a way for readers to "experience" predicted threats so that they can strategise about how to counteract them.[465]

5.3.1.1 Regulatory Gaps

Poor inbuilt IoT security results from lax legal restrictions regarding security and privacy by design. Data is left vulnerable because, e.g. security settings are configured to an inadequately low default, and it is unclear how users can alter them.[466] A feature of this is that apps and the IoT devices on which they are hosted often have weak authorisation protocols that allow overreach, including downloading malware, which could facilitate data theft and manipulation via third party software or device layers, either in storage or in transit.[467] The resultant ambiguity as to whether a journalist is responsible for specific information, either through sharing or creation, could have ramifications for their credibility and public trust.

5.3.1.1.1 Third party supply chain actors accessing data

For reasons such as maintenance, IoT device manufacturers can legally ensure that devices continually upload data to, e.g. peer-to-peer networks that are coordinated by the manufacturer, regardless of the length of the chain of components and actors within these networks.[468] Data collected by consumer devices is therefore made accessible to an indeterminate number of parties, regardless of the knowledge or active consent of device owners.[469]

Hypothetical consequences: This supply chain risk means that journalists could have their technology and data compromised because they – necessarily or inadvertently – agreed to information sharing with third party actors in this chain.

---

[462] Rasmussen, L.B.: The narrative aspect of scenario building - How story telling may give people a memory of the future. AI & Soc. 19, 229–249 (2005). https://doi.org/10.1007/s00146-005-0337-2.

[463] Kebande, V.R., Karie, N.M., Michael, A., Malapane, S.M.G., Venter, H.S.: How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. In: 2017 IST-Africa Week Conference (IST-Africa). pp. 1–10 (2017).

[464] Blythe JM and Johnson SD (2019) A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*. DOI: 10.1057/s41284-019-00211-8; Heartfield R, Loukas G, Budimir S, et al. (2018) A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78: 398–428. DOI: 10.1016/j.cose.2018.07.011.

[465] Tanczer LM, Steenmans I, Elsden M, et al. (2018) Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? In: *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK, 2018, p. 33 (9 pp.)-33 (9 pp.). Institution of Engineering and Technology. DOI: 10.1049/cp.2018.0033; *The True Story of Using Fiction to Enhance Risk Intelligence* (2021) The Association of International Risk Intelligence Professionals (AIRIP). Available at: https://www.youtube.com/watch?v=qP_i94eP2Ho (accessed 18 January 2023).

[466] Michel MCK and King MC (2019) Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In: *2019 IEEE International Symposium on Technology and Society (ISTAS)*, Medford, MA, USA, 15 November 2019, pp. 1–7. IEEE. DOI: 10.1109/ISTAS48451.2019.8938009.

[467] Anell S, Grober L and Krombholz K (2020) End User and Expert Perceptions of Threats and Potential Countermeasures. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 10. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[468] Krebs B (2016) This is Why People Fear the 'Internet of Things'. In: *Krebs on Security*. Available at: https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/comment-page-1/#comments (accessed 31 December 2020).

[469] Tabassum M, Kosiński T and Lipford HR (2019) 'I don't own the data': end user perceptions of smart home device data practices and risks. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, USA, 12 August 2019, pp. 435–450. SOUPS'19. USENIX Association.

5.3.1.1.2 Data manipulation as a result of consent requirements

Some apps and IoT devices require users to consent to all manner of data acquisition, transfer, and processing, as well as allowing access to other device functionalities (such as cameras, microphones, and messaging systems) in order to function.[470] Similarly, with the evolution of deep fake technologies, the wealth of data created by IoT devices could be used to use an individual's likeness effectively and potentially legally.

Hypothetical consequences: These consent requirements allow the problematic potential for access and manipulation of journalists' data, possibly in ways that could dupe or reveal sources.[471]

5.3.1.1.3 Data harvesting from decommissioned devices

A situation in which adversarial physical access to devices would be problematic relates to individual journalists or news organisations disposing of defunct or decommissioned IoT devices without appropriately wiping them of their history. This could enable "dumpster divers" to fish out devices and recover confidential information stored either in the device's local memory or in the cloud, through the device. For many devices, there is no obvious reset button, and the physical device may be an easy entry-point to the user data still retained by the device's managing company.[472]

Hypothetical consequences: Adversaries viewing information on Internet of Things devices could leave journalists and news organisations exposed to data theft relating to finances, employees, security, etc. (i.e. anything that has been accessed via some devices, and anything mentioned in front of other devices), which could be devastating for both the newsroom and the organisation as a business.

5.3.1.1.4 Botnet creation

There is currently no legal or financial incentive for manufacturers to encrypt data or otherwise increase the security of purchased devices; this leaves endpoint management unsupported as devices have out of date firmware or software that can be exploited through well-known channels.[473] As a result, IoT devices, while potentially low-powered on their own, generally have such lax security that they can be easily co-opted into botnets, i.e. networks of (even unrelated and disparate) IoT devices that have been infected with malware.

Hypothetical consequences: Host takeover resulting in botnets can execute data breaches, Distributed Denial of Service (DDoS) attacks on well-secured networks or internet infrastructure,[474] and further

---

[470] Michel MCK and King MC (2019) Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In: *2019 IEEE International Symposium on Technology and Society (ISTAS)*, Medford, MA, USA, 15 November 2019, pp. 1–7. IEEE. DOI: 10.1109/ISTAS48451.2019.8938009.

[471] Michel MCK and King MC (2019) Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In: *2019 IEEE International Symposium on Technology and Society (ISTAS)*, Medford, MA, USA, 15 November 2019, pp. 1–7. IEEE. DOI: 10.1109/ISTAS48451.2019.8938009.

[472] Wright L (2017) Economic Espionage and Business Intelligence. In: Wright L (ed.) People, Risk, and Security: How to Prevent Your Greatest Asset from Becoming Your Greatest Liability. London: Palgrave Macmillan UK, pp. 91–105. DOI: 10.1057/978-1-349-95093-5_7.

[473] Hoffmann S (2018) *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. 15 November. Oxford, United Kingdom: IoT Security Foundation. Available at: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf (accessed 12 August 2020).

[474] Rizvi S, Kurtz A, Pfeffer J, et al. (2018) Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference*

malware delivery that can drastically affect services on which society relies, including news provision.[475] [476] [477] Any of these activities can be devastating for individual journalists and for news organisations, both of which might be at risk of losing access to vital devices or systems for indeterminate periods of time, as well as the potential that data held on those systems has been compromised.[478] Further, botnets could be used to launch large-scale online attacks on members of the press using troll armies.[479] [480]

5.3.1.2 Legal Threats

As was mentioned by participants for Chapter 4's exploratory study, and is discussed in more detail by interviewees for Chapters 6 and 7, legal threats are one of the most pressing types of risk perceived by journalists in democracies. This phrase refers to ways in which IoT data or actions might be used either in law enforcement investigations, or to embroil journalists in lawsuits.[481] The threat category presented here builds on Chapter 4; its real-world impact is explored in Chapter 6.

5.3.1.2.1 Abuse of data and privacy laws

There are a number of methods through which Internet of Things data can be accessed by governments, corporations, or even individuals, who know how to exploit ambiguous legal provisions. Journalistic data can therefore be too-easily accessed by third parties via these legal threats. These threats are due to technologically-neutral protections that do not sufficiently differentiate between types of data and devices, and negligent protections in data protection and privacy laws and regulations, all compounded by a requirement that certain kinds of data are retained for lengthy periods of time.

Hypothetical consequences: Data retention laws may be vague on whether they consider clearly identifiable data from IoT devices to constitute metadata, which further risks information because metadata is often allowed to be kept by governments for longer than other kinds of data. For example, Australian metadata retention laws require metadata storage for a minimum of two years. There is already evidence that these laws have chilled the Australian press, as well as counteracting some of the protections of pre-existing source shield laws.[482] Additionally, data protection laws intended to protect individuals' personal data from unwarranted collection or access and exploitation by third parties usually

On Big Data Science And Engineering (TrustCom/BigDataSE), August 2018, pp. 163–168. DOI: 10.1109/TrustCom/BigDataSE.2018.00034.

[475] Smith S (2017) *The Internet of Risky Things: Trusting the Devices That Surround Us*. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.

[476] Krebs B (2016) KrebsOnSecurity Hit With Record DDoS — Krebs on Security. Available at: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (accessed 23 October 2020).

[477] Cimpanu C (2016) A Massive Botnet of CCTV Cameras Involved in Ferocious DDoS Attacks. *softpedia*, 27 June. Available at: https://news.softpedia.com/news/a-massive-botnet-of-cctv-cameras-involved-in-ferocious-ddos-attacks-505722.shtml (accessed 23 October 2020).

[478] McGregor S (2016) Why DDoS attacks matter for journalists. Available at: https://www.cjr.org/tow_center/journalists_ddos_hack_passwords.php (accessed 15 November 2020).

[479] Agrafiotis I, Nurse JRC, Goldsmith M, et al. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1). Oxford Academic. DOI: 10.1093/cybsec/tyy006.

[480] Gulzar M, Abbas G. Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET) [Internet]. Lahore, Pakistan: IEEE; 2019. p. 1–6. Available from: https://ieeexplore.ieee.org/document/8711834. p. 2.

[481] Holcomb, J., Mitchell, A., Page, D.: Investigative journalists and digital security: Perceptions of vulnerability and changes in behavior. Pew Research Center in association with Columbia University's Tow Center for Digital Journalism, Columbia University, New York (2015).

[482] Brevini B (2017) Metadata Laws, Journalism and Resistance in Australia. *Media and Communication* 5(1). 1: 76–83. DOI: 10.17645/mac.v5i1.810.

include provisions for their negation for legitimate interest,[483] which governments and associated corporations use to justify their access to and use of data and metadata, including from the IoT.[484] Furthermore, the subject access ("Right to Access") requests enshrined in privacy laws and regulations, such as the GDPR, can also be ambiguous, leaving the data vulnerable to social engineering attempts that enable adversaries to impersonate journalists to access their information.[485]

5.3.1.2.2 Weaponisation of financial penalties

Criminal actors could exploit news organisations' notable lack of effective security protocols and the potential for IoT devices that are connected to a central Wi-Fi network. They may distribute ransomware that locks journalists and other media staff out of their work, thereby hindering the progress of a story and creating more financial and legal stressors for executives.[486] The financial repercussions of data breaches, on top of the ransom, are significant threats to the normal operation of media organisations and journalists.[487]

Hypothetical consequences: A media-industry-wide culture of under-prioritisation of security (often due to lack of funds) increases the likelihood of security breaches, especially from poorly secured IoT devices. This would likely trigger devastating financial pressures,[488] including regulatory fines, investigation costs and compensation payments that would force the news organisation to lay off some of its staff.[489]

5.3.1.2.3 Warrantless bulk data purchase

Government agencies and private companies can legally sidestep journalistic warrant requirements by purchasing bulk user data from service providers, including those that are involved in the maintenance of IoT devices.[490] This bulk data can include "incidental data" or "data exhaust," which are detailed chronological logs that automatically document the minutiae of IoT interactions regarding connection to other devices, users, and services (e.g. location, or search engine requests, etc.).[491]

---

[483] Information Commissioner's Office (2019) Data Protection Act 2018: For Organisations. Available at: https://ico.org.uk/for-organisations/data-protection-act-2018/ (accessed 28 May 2019).

[484] Shere A (2020) Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis. *The New Collection* 14: 3–21.

[485] Pavur, J., Knerr, C.: GDPArrrrr: Using Privacy Laws to Steal Identities. In: Blackhat USA 2019 Whitepaper. p. 10. Blackhat USA, Las Vegas (2019).

[486] Anell S, Grober L and Krombholz K (2020) End User and Expert Perceptions of Threats and Potential Countermeasures. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 10. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[487] Frost, J., Hamlin, A.: Ransomware - A Strategic Threat to Organizations. Mountain Plains Journal of Business and Technology. 21, (2020); Solove, D.J., Hartzog, W.: Breached!: Why Data Security Law Fails and How to Improve it. Oxford University Press, Oxford, New York (2022).

[488] Pavur, J., Knerr, C.: GDPArrrrr: Using Privacy Laws to Steal Identities. In: Blackhat USA 2019 Whitepaper. p. 10. Blackhat USA, Las Vegas (2019).

[489] Agrafiotis I, Nurse JRC, Goldsmith M, et al. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1). Oxford Academic. DOI: 10.1093/cybsec/tyy006.

[490] Anell S, Grober L and Krombholz K (2020) End User and Expert Perceptions of Threats and Potential Countermeasures. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 10. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf; Cox J (2020) Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal. Available at: https://www.vice.com/en_ca/article/k7qyv3/customs-border-protection-venntel-location-data-dhs (accessed 11 September 2020); Cox J (2020) The Loophole the DMV Uses to Sell Your Data to Private Investigators. *VICE*, 27 August. Available at: https://www.vice.com/en_us/article/ep47na/dmv-dppa-drivers-privacy-protection-act-buy-data-private-investigators (accessed 11 September 2020).

[491] Allam S (2018) An Exploratory Survey of Hadoop Log Analysis Tools. International Journal of Creative Research Thoughts 6(3): 801–804.

Hypothetical consequences. Even if a user can purge the logs held on an old device after years of ownership, they may never know how many times that data was transmitted, accessed, consolidated, or sold prior to the purge. Historical datasets are lucrative and there are already academic proposals for ways in which service providers can sell IoT datasets to advertisers and other third parties.[492] This creates a rich dataset from which adversaries may isolate key dates and events, in order to cross-reference these with information gathered on suspected journalistic sources, thereby definitively identifying a confidential source.

5.3.1.3 Profiling Threats

The timing of interaction with automated household and utility devices could allow "pattern of life" information (i.e. detailed daily routines) to be surmised and exploited.[493] In addition to the potential for behavioural manipulation via IoT "nudging",[494] predictive analysis can also be used to infer more sensitive data by devices or attackers with analytical capabilities, such as one's health status being recognised based on requests made to voice assistants,[495] or wearable devices.[496] The IoT-sourced data allows extrapolation to substantiate both true and false scenarios, which could also call into question journalists' professional integrity.

5.3.1.3.1 Continuous surveillance

Access level attacks on IoT systems target system availability and can be passive or active, including monitoring and eavesdropping, for example via microphones and/or cameras.[497] This ongoing access to information presents the dual issues of both identification of individuals and profiling, i.e. compiling and analysing data on the journalist and their identified sources.[498]

---

[492] Aksu, H., Babun, L., Conti, M., Tolomei, G., Uluagac, A.S.: Advertising in the IoT Era: Vision and Challenges. arXiv:1802.04102 [cs]. (2018).

[493] Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658; Burdon, M., Cohen, T.: Modulation Harms and The Google Home. Surveillance & Society. 19, 154–167 (2021). https://doi.org/10.24908/ss.v19i2.14299; McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.

[494] Rahaman, T.: Smart Things are Getting Smarter: An Introduction to the Internet of Behavior. Medical Reference Services Quarterly. 41, 110–116 (2022). https://doi.org/10.1080/02763869.2022.2021046; Owens K, Gunawan J, Choffnes D, et al. (2022) Exploring Deceptive Design Patterns in Voice Interfaces. In: *2022 European Symposium on Usable Security*, Karlsruhe Germany, 29 September 2022, pp. 64–78. ACM. DOI: 10.1145/3549015.3554213.

[495] Abdi, N., Ramokapane, K.M., Such, J.M.: More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security. pp. 451–466. USENIX Association, USA (2019).

[496] Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658; Gulzar M and Abbas G (2019) Internet of Things Security: A Survey and Taxonomy. In: *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, February 2019, pp. 1–6. IEEE. DOI: 10.1109/CEET1.2019.8711834; Alqhatani A and Lipford HR (2019) 'There is nothing that i need to keep secret': sharing practices and concerns of wearable fitness data. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, USA, 12 August 2019, pp. 421–434. SOUPS'19. USENIX Association.

[497] Gulzar M and Abbas G (2019) Internet of Things Security: A Survey and Taxonomy. In: *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, February 2019, pp. 1–6. IEEE. DOI: 10.1109/CEET1.2019.8711834; Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660; Benjakob O (2022) This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure - National Security & Cyber - Haaretz.com. Haaretz, 26 December. Available at: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000 (accessed 12 January 2023).

[498] Gulzar M and Abbas G (2019) Internet of Things Security: A Survey and Taxonomy. In: *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, February 2019, pp. 1–6. IEEE. DOI: 10.1109/CEET1.2019.8711834; Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things:

Hypothetical consequences: There is the possibility of devices with microphones picking up the sounds of nearby typing patterns, to allow reconstruction of messages sent, which could compromise confidential communications between journalists and their sources and editors, even when sent through secure channels.[499] Access to the huge amounts of personal information gathered by IoT devices, either historic data (such as location information from a fitness tracker or GPS keychain finder),[500] or live data (such as hacking the camera of a smart television, which may record both video and audio),[501] can facilitate the doxxing and stalking of journalists. In addition to the physical security, health, and safety consequences of doxxing and stalking, they could also result in financial and reputational damages that harm a journalist's credibility.[502]

5.3.1.3.2 Abusing health and biometric information

Journalists' devices to track personal health information may not have the inbuilt security to prevent leaks. Malicious actors may use this information to cause psychological or physical distress, thereby influencing a journalist's output, e.g. through blackmail.[503]

Hypothetical consequences: Insecurity of wearable fitness or medical devices, including those that collect health information, can contribute to inaccurate diagnoses and prescriptions, or even altered test results. These flaws could be fatal and could be used to put psychological, financial, or physical pressure on journalists.[504] A feasible but unlikely example is a diabetic journalist having a wearable blood sugar tracker that can be hacked, enabling adversaries to identify vulnerable moments.[505]

Perspectives and Challenges. *IEEE Internet of Things Journal* 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658; Edu JS, Such JM and Suarez-Tangil G (2019) Smart Home Personal Assistants: A Security and Privacy Review. *arXiv:1903.05593 [cs]*. Available at: http://arxiv.org/abs/1903.05593 (accessed 21 August 2020); Di Salvo P (2021) "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice* 0(0). Routledge: 1–18. DOI: 10.1080/17512786.2021.2014346.

[499] Liverpool L (2020) Voice assistant recordings could reveal what someone nearby is typing. *New Scientist*, 4 December. Available at: https://www.newscientist.com/article/2261844-voice-assistant-recordings-could-reveal-what-someone-nearby-is-typing/ (accessed 1 January 2021).

[500] Alqhatani A and Lipford HR (2019) 'There is nothing that i need to keep secret': sharing practices and concerns of wearable fitness data. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, USA, 12 August 2019, pp. 421–434. SOUPS'19. USENIX Association; Clayton J and Dyer J (2022) Apple AirTags - 'A perfect tool for stalking'. *BBC News*, 20 January. Available at: https://www.bbc.com/news/technology-60004257 (accessed 5 December 2022).

[501] Sturgess J, Nurse JRC and Zhao J (2018) A capability-oriented approach to assessing privacy risk in smart home ecosystems. In: *2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK, 2018, p. 37 (8 pp.)-37 (8 pp.). Institution of Engineering and Technology. DOI: 10.1049/cp.2018.0037.

[502] Anell S, Grober L and Krombholz K (2020) End User and Expert Perceptions of Threats and Potential Countermeasures. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 10. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[503] Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660; Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658.

[504] Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658; Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660.

[505] Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658; Agrafiotis I, Nurse JRC, Goldsmith M, et al. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1). Oxford Academic. DOI: 10.1093/cybsec/tyy006.

5.3.1.3.3 Data linkage and aggregation

The heterogeneity of IoT devices and their capabilities means that data linkage and data aggregation can reveal far more than was previously possible. Insufficient network and data segregation in smart home systems comprised of varied consumer IoT devices can enable profiling of both users and those with whom they interact, and can reveal this information to everyone within the environment.[506]

Hypothetical consequences: This could jeopardise source confidentiality if data and metadata from both ambient and wearable IoT devices is cross-referenced.[507] Further, this can cause identity theft and financial damage,[508] which could affect journalists by embroiling them in complex legal cases that leave little time available for them to focus on work and tie up resources.

5.3.1.4 Tracking Threats

A likely category of IoT threats is the use of devices' data collection capabilities for tracking purposes, generating either contemporary or retroactive movement patterns sold to private companies and government agencies.[509] Tracking journalists and sources poses a threat to confidentiality that could ultimately chill the press. Knowledge of their pattern of life may also facilitate physical attacks.

5.3.1.4.1 Informal additions to state surveillance networks

Consumer IoT networks can become informal features of smart cities, particularly when easily accessible by law enforcement and intelligence agencies.[510] Many IoT camera-equipped doorbells have built-in police access, effectively making them an extension of state surveillance networks.[511]

Hypothetical consequences: This centralisation of data could easily facilitate the tracking of journalists by governments without transparent oversight.

5.3.1.4.2 SOCMINT and IoT interrogation by law enforcement

Law enforcement's use of social media analysis may be cross-referenced with interrogation of portable IoT devices belonging to individuals who are suspected of attending protests.[512]

---

[506] Chhetri C and Genaro Motti V (2022) User-Centric Privacy Controls for Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW2): 349:1-349:36. DOI: 10.1145/3555769.

[507] Sturgess J, Nurse JRC, Zhao J. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In: 2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018 [Internet]. London, UK: Institution of Engineering and Technology; 2018 [cited 2020 Sep 11]. p. 37 (8 pp.)-37 (8 pp.). Available from: https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0037.

[508] Anell S, Grober L and Krombholz K (2020) End User and Expert Perceptions of Threats and Potential Countermeasures. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 10. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[509] Cox, J.: Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal, https://www.vice.com/en_ca/article/k7qyv3/customs-border-protection-venntel-location-data-dhs.

[510] Dooley B and Ueno H (2022) Where a Thousand Digital Eyes Keep Watch Over the Elderly. *The New York Times*, 2 February. Available at: https://www.nytimes.com/2022/02/02/business/japan-elderly-surveillance.html (accessed 5 December 2022).

[511] Wakefield J (2020) Ring doorbells to send live video to Mississippi police. *BBC News*, 5 November. Available at: https://www.bbc.com/news/technology-54809228 (accessed 7 November 2020); Guariglia JK and M (2022) Ring Reveals They Give Videos to Police Without User Consent or a Warrant. Available at: https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant (accessed 5 December 2022); Calacci D, Shen JJ and Pentland A (2022) The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW2): 400:1-400:47. DOI: 10.1145/3555125.

[512] Access Now (2020) New world disorder: digital attacks on freedom of assembly. In: *Access Now*. Available at: https://www.accessnow.org/new-world-disorder-digital-attacks-on-freedom-of-assembly/ (accessed 11 September 2020); Shere, A.R.K., Nurse, J.R.C.: Police surveillance of Black Lives Matter shows the danger technology poses to democracy,

Hypothetical consequences: This chills the press by creating a fear of identification and reprisals both among sources and journalists gathering information on the ground.[513]

5.3.1.4.3 Predictive analysis of location data to facilitate physical attacks

Tracking of a journalist or source by accessing the real-time geographic data gathered by and streamed from their car, fitness tracker or smart watch could also allow an adversary to infer previous routes and locations, or predict future ones.[514]

Hypothetical consequences: This location information could be capitalised on to facilitate a physical attack,[515] or to implicate the journalist in a crime.

5.3.1.5 Data and device modification threats

The continued existence of a free press depends on journalists' dissemination of accurate information. If this is threatened, such as through alteration of data held on or proliferated by journalists' devices or accounts, it could discredit the work of entire news organisations and lower public trust in the news media. Additionally, sometimes consumer IoT devices have sufficiently intrusive intended functionalities that an adversary can use existing capabilities in ways that the user may not have intended, endangering the psychological and physical safety and security of a journalist or source.

5.3.1.5.1 Sensor-level attacks on data confidentiality or integrity

Information can be changed via Information Damage Level attacks, which relate to the sensors in IoT devices. These attacks can take different forms, usually involving monitoring, intercepting, modifying, fabricating, or replicating data collected by these sensors and sent through a network. They particularly affect data confidentiality and integrity, as messages can be altered or recorded and replayed to the wrong people or at the wrong times.[516]

---

http://theconversation.com/police-surveillance-of-black-lives-matter-shows-the-danger-technology-poses-to-democracy-142194, (2020).

[513] Access Now (2020) New world disorder: digital attacks on freedom of assembly. In: *Access Now*. Available at: https://www.accessnow.org/new-world-disorder-digital-attacks-on-freedom-of-assembly/ (accessed 11 September 2020).

[514] @DFRLab (2018) Data and Defense: The Case of Strava. Available at: https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2 (accessed 9 August 2019); Alqhatani, A., Lipford, H.R.: 'There is nothing that i need to keep secret': sharing practices and concerns of wearable fitness data. In: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security. pp. 421–434. USENIX Association, USA (2019); National Security Agency (2020) *Limiting Location Data Exposure*. National Security Agency | Cybersecurity Information U/OO/155603-20 | PP-20-0535, August. USA: National Security Agency. Available at: https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF (accessed 11 September 2020); Levinson C (2021) Senior Israeli Security Official Reveals State Secrets as He Runs, Bikes. *Haaretz*, 17 December. Israel. Available at: https://www.haaretz.com/israel-news/2021-12-17/ty-article/shin-bet-bodyguard-broadcasts-state-secrets-as-he-runs-bikes-off-hours/0000017f-e389-d568-ad7f-f3ebb69e0000 (accessed 5 December 2022).

[515] National Security Agency (2020) *Limiting Location Data Exposure*. National Security Agency | Cybersecurity Information U/OO/155603-20 | PP-20-0535, August. USA: National Security Agency. Available at: https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF (accessed 11 September 2020); Cha, S.-C., Hsu, T.-Y., Xiang, Y., Yeh, K.-H.: Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. IEEE Internet of Things Journal. 6, 2159–2187 (2019). https://doi.org/10.1109/JIOT.2018.2878658.

[516] Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660; Benjakob O (2022) This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure - National Security & Cyber - Haaretz.com. Haaretz, 26 December. Available at: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-

Hypothetical consequences: These attacks could prevent journalists from feeling confident that they can effectively protect source information and that their work is founded in verifiable data.

5.3.1.5.2 Altering user-facing device and data attributes

Attacks used to alter user-facing information displayed on IoT devices could create psychological pressures that derail and undermine journalistic work, compromising journalists' reputations.

Hypothetical consequences: If an adversary overrides a photojournalist's authentication on a camera-equipped drone, this could prevent footage from being accessed and used. Spoofing data packets would cause devices to stop, start, or modify actions.[517] As a result, a journalist using a smart watch, for example, could be left unaware of messages that have been urgently sent to their phone by a source. Journalists often receive threatening messages,[518] which could also be delivered through their devices, such as a voice assistant. If these two events coincide, there is likely to be a chilling effect as they question the security of their professional systems and their own perceptions due to gaslighting.[519] Another example is clock skewing: if an adversary can control the pulse-accurate, synchronised clocks in a broadcast station, they can stop a live programme from going out. Further, falsification of time stamps could make journalists' task of verification of sources much more difficult, which may then allow their conclusions to be debunked and their reputations to suffer, for example if a faked timestamp is used to evidence a story that a politician knew about an action prior to its occurrence, the journalist breaking the story could appear biased. Finally, digital forensics, which is already notoriously unreliable regarding consumer IoT devices, may be made more challenging because, for example, monitoring when specific actions have been taken could be hindered if time stamps can be easily falsified by changing the time on the device's clock.[520]

5.3.1.5.3 Hijacking connected social media and communications accounts

Some smart White Goods have the ability to post from users' social media accounts or send emails,[521] and hacking into a journalist's fridge and accessing their social media accounts in order to imitate them could be used for a variety of nefarious purposes.[522]

---

article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000 (accessed 12 January 2023).

[517] Hoffmann S (2018) *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. 15 November. Oxford, United Kingdom: IoT Security Foundation. Available at: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf (accessed 12 August 2020).

[518] Binns A (2017) Fair game? Journalists' experiences of online abuse. *Journal of Applied Journalism & Media Studies* 6(2): 183–206. DOI: 10.1386/ajms.6.2.183_1.

[519] Middleton L (2020) Woman 'hacked into ex-boyfriend's Alexa and told his new girlfriend to leave'. *Metro*, 12 October. Available at: https://metro.co.uk/2020/10/12/woman-hacked-into-ex-boyfriends-alexa-and-told-his-new-girlfriend-to-leave-13407458/ (accessed 19 October 2020); Moody G (2020) The enemy within: welcome to the Internet of gaslighting. Available at: https://www.privateinternetaccess.com/blog/the-enemy-within-welcome-to-the-internet-of-gaslighting/ (accessed 11 September 2020).

[520] Gulzar M and Abbas G (2019) Internet of Things Security: A Survey and Taxonomy. In: *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, February 2019, pp. 1–6. IEEE. DOI: 10.1109/CEET1.2019.8711834.

[521] Agence France-Presse (AFP) (2014) Hackers use 'smart' refrigerator to send 750,000 virus-laced emails. *Raw Story*, 17 January. Available at: https://www.rawstory.com/2014/01/hackers-use-smart-refrigerator-to-send-750000-virus-laced-emails/ (accessed 23 October 2020).

[522] Greenberg, A.: Hackers Broke Into Real News Sites to Plant Fake Stories, https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/, (2020); Hamilton, E.: Eric Hamilton on Twitter: 'Here's a thing that happened today. I was recently -- and falsely -- linked to an article I didn't write, because the author who DID write it happens to share the same name/byline as I do. I'm not going to link to it because it's complete garbage.',

Hypothetical consequences: If a consumer IoT device that has access to a journalist's social media accounts is hacked and an adversary is able to publish disinformation under a journalist's name from their own account,[523] that would likely undermine the journalist's credibility. If this process repeats, the journalist's audience could shift or disappear to such an extent that the journalist no longer has a following of note or a sufficiently good reputation to have standing within the industry. The advent of global digital media platforms has created an environment with huge public influence and little regulation. Even democratic governments are using the disinformation crisis to pass more subversively restrictive laws on journalism with the pretext of inhibiting the spread of disinformation.[524] This could be used as evidence to invoke laws that would then result in the prosecution of the journalist.

5.3.1.5.4 Manipulation of devices' physical activities

Malware may change device settings and alter the behaviour or functionality of a device without the device owner's recognition. This can facilitate both clandestine surveillance and kinetic attacks in technologies from small consumer IoT devices to core national infrastructure, as happened with the Stuxnet hack.[525]

Hypothetical consequences: Examples range from large-scale kinetic attacks against IoT devices that control public goods in an urban area where lots of news organisations are concentrated,[526] to attacks on individual targets, such as remote takeovers of internet-connected vehicles resulting in adversaries gaining control of vital functions such as steering and braking, which could be used to physically harm journalists and sources.[527] This kind of manipulation of the settings of devices with physical functionalities upon which a journalist relies, can range from these more urgently relevant examples, to having an indefinite time frame, such as altering the temperature control function of a journalist's smart fridge so that it overcorrects, thereby spoiling the contents and poisoning the journalist.[528]

---

https://twitter.com/OnetheycallEric/status/1270857748092239872; Honeywell, L.: Leigh Honeywell @ 🏠 on Twitter: 'Btw this Eric Hamilton is _not_ the author of the shitty stalker article, just has the misfortune of the same name and profession', https://twitter.com/hypatiadotca/status/1270978645327110145.

[523] Schwedel, S., Palus, H.: A Ranking of the Weirdest Appliances That You Can Technically Tweet From, https://slate.com/technology/2019/08/twitter-electronics-ranked-list-which-is-best.html.

[524] Reporters Without Borders: RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders, https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators.

[525] Patel, C., Doshi, N.: Security Challenges in IoT Cyber World. In: Hassanien, A.E., Elhoseny, M., Ahmed, S.H., and Singh, A.K. (eds.) Security in Smart Cities: Models, Applications, and Challenges. pp. 171–191. Springer International Publishing, Cham (2019).

[526] Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660.

[527] National Security Agency (2020) *Limiting Location Data Exposure*. National Security Agency | Cybersecurity Information U/OO/155603-20 | PP-20-0535, August. USA: National Security Agency. Available at: https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF (accessed 11 September 2020); Agrafiotis I, Nurse JRC, Goldsmith M, et al. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1). Oxford Academic. DOI: 10.1093/cybsec/tyy006; Staff of Senator Ed Markey (2015) *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*. February. Massachusetts, USA: Office of the United States Senator for Massachusetts. Available at: https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (accessed 26 October 2020).

[528] Bhartiya S (2017) Your smart fridge may kill you: The dark side of IoT. Available at: https://www.infoworld.com/article/3176673/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html (accessed 18 November 2020).

5.3.1.6 Networked devices threats

The combination of multiple devices into IoT ecosystems presents unique challenges, meaning that Computer Network Exploitation (i.e. "hacking") of networks of Internet of Things devices can culminate in much greater harm than that posed by any single device.[529] Smart hubs that coordinate devices can be attacked in a variety of ways, and can be used for Elevation of Privilege attacks, therefore giving adversaries high-level access to and control of connected IoT devices.[530] Due to poor encryption and the networked nature of the Internet of Things, an entire network of journalists' devices could be compromised if an adversary has access to just one IoT device: even a smart lightbulb may reveal Wi-Fi passwords.[531] Representatives of intelligence agencies of democratic states have openly stated their intention to use poorly secured IoT devices to pivot into a network and gather data on users, including credentials that would give them access to more secure systems;[532] these systems could include those belonging to news organisations.

5.3.1.6.1 Voice stealing

The ability to identify IoT devices present in an individual's home through open-source investigations is the first step to many different attacks, including active access-level attacks that are specific to voice assistants, such as "voice squatting in which an attack skill carries a phonetically similar invocation name to that of its target skill" and "word squatting where the attack invocation name includes the target's name and some strategically selected additional words."[533] This was demonstrated when the UK's National Cyber Security Centre used a vulnerability in an IoT doll to unlock a smart door lock.[534]

Hypothetical consequences: Due to the poor inbuilt security of IoT devices, there have already been recorded instances of accidental malfunction, such as when voice assistants have recorded more audio data than intended and have sent this to members of the user's contacts list.[535] If this occurs in a space

---

[529] Nassi B, Bitton R, Masuoka R, et al. (2021) SoK: Security and Privacy in the Age of Commercial Drones. In: *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 73–90. IEEE Computer Society. DOI: 10.1109/SP40001.2021.00005; Kebande, V.R., Karie, N.M., Michael, A., Malapane, S.M.G., Venter, H.S.: How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. In: 2017 IST-Africa Week Conference (IST-Africa). pp. 1–10 (2017).

[530] Hoffmann S (2018) *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. 15 November. Oxford, United Kingdom: IoT Security Foundation. Available at: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf (accessed 12 August 2020).

[531] Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660; Doctorow C (2019) Discarded smart lightbulbs reveal your wifi passwords, stored in the clear. Available at: https://boingboing.net/2019/01/29/fiat-lux.html (accessed 5 December 2022).

[532] McLaughlin, J.: NSA Looking to Exploit Internet of Things, Including Biomedical Devices, Official Says, https://theintercept.com/2016/06/10/nsa-looking-to-exploit-internet-of-things-including-biomedical-devices-official-says/, (2016); Ackerman, S., Thielman, S.: US intelligence chief: we might use the internet of things to spy on you, https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper, (2016).

[533] Zhang N, Mi X, Feng X, et al. (2019) Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. In: *2019 IEEE Symposium on Security and Privacy (SP)*, Stockholm, Sweden, May 2019, pp. 1381–1396. IEEE. DOI: 10.1109/SP.2019.00016.

[534] Levy I (2017) Hacked doll 'could open front door'. *BBC News*, 14 February. Available at: https://www.bbc.co.uk/news/av/technology-38966285 (accessed 13 September 2020).

[535] Edu JS, Such JM and Suarez-Tangil G (2019) Smart Home Personal Assistants: A Security and Privacy Review. *arXiv:1903.05593 [cs]*. Available at: http://arxiv.org/abs/1903.05593 (accessed 21 August 2020); Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660; Shaban H (2018) An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says - The Washington Post. *The Washington Post*, 24 May. Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-

where an editorial team is discussing an as-yet unbroken story, the subject of the story could be directly or indirectly alerted. Further, intentional rerouting attacks such as voice stealing manipulate the data received by either end of a communications channel, and would be particularly problematic for journalist-source communication, or even for different members of a newsroom team discussing a sensitive story.[536] This could also be used to tell devices to activate functions that might endanger physical safety; for a journalist who has done public interviews, manipulation of the audio from those interviews to record a command that can then be played when an adversary calls the journalist's home phone, to activate a voice assistant, e.g. turning on ovens at night, to set fires in a journalist's home.

5.3.1.6.2 Denial of Service attacks

Denial of Service attacks can be effected against Internet of Things devices if a device's availability is maliciously overloaded through unnecessary data traffic.[537] This can be particularly damaging if the device has an essential function, such as monitoring blood sugar or pulse.[538] DoS could be achieved by exploiting vulnerabilities in the hub to disrupt the entire smart home ecosystem.[539] Being targeted by DoS attacks reduces a network's capacity and can disable it, which could occur if an adversary exhausts the resources of a specific IoT device or network by overloading communications or overusing a specific functionality. This could then cause the device to shut down due to low power, which would be particularly problematic if it is a device that centrally coordinates other IoT devices thus impacting the wider network.[540] Given the range of functionalities that consumer IoT devices can possess, users may come to rely on them, triggering detrimental physical and psychological effects if device functionality is unexpectedly limited.[541] Disruption of technological networks and denial of internet access are already features of governments' toolboxes, intended to prevent communication either to, by or among specific groups,[542] and so it stands to reason that this would be extended to situations involving IoT devices, making this a likely category of threats to be enacted.

---

recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/ (accessed 13 September 2020).

[536] Gulzar M, Abbas G. Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET) [Internet]. Lahore, Pakistan: IEEE; 2019. p. 1–6. Available from: https://ieeexplore.ieee.org/document/8711834. p. 2; Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660.

[537] Gulzar M, Abbas G. Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET) [Internet]. Lahore, Pakistan: IEEE; 2019. p. 1–6. Available from: https://ieeexplore.ieee.org/document/8711834. p. 2.

[538] Anell S, Grober L and Krombholz K (2020) End User and Expert Perceptions of Threats and Potential Countermeasures. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 10. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[539] Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660; Hoffmann S. IoT Security Architecture and Policy for the Home - a Hub Based Approach [Internet]. Oxford, United Kingdom: IoT Security Foundation; 2018 Nov [cited 2020 Aug 12] p. 40. Available from: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf; Gulzar M, Abbas G. Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET) [Internet]. Lahore, Pakistan: IEEE; 2019. p. 1–6. Available from: https://ieeexplore.ieee.org/document/8711834. p. 2.

[540] Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660.

[541] Finley, K.: Why Tech's Best Minds Are Very Worried About the Internet of Things, https://www.wired.com/2014/05/iot-report/, (2014); Anell, S., Grober, L., Krombholz, K.: End User and Expert Perceptions of Threats and Potential Countermeasures. In: The 5th European Workshop on Usable Security. p. 10. IEEE, Genova, Italy (2020).

[542] Mahase, E.: Kashmir communications blackout is putting patients at risk, doctors warn. BMJ. 366, l5204 (2019). https://doi.org/10.1136/bmj.l5204; Elliott, V.: Four ways governments disrupt internet access, https://restofworld.org/2021/four-ways-governments-disrupt-internet-access/.

Hypothetical consequences: If a journalist is reliant on the availability of a specific network or device that can be accessed through an insecure IoT device, DoS (e.g. through Information Damage Level attacks) could leave them vulnerable to extortion.[543] Similarly, restriction of internet access could have a particularly negative impact on journalists who are using such devices to report, such as camera-equipped drones. Internet-access denial tactics are also used to reinforce aggressive treatment of journalists covering protests by preventing them from using portable IoT devices to report on the ground.

5.3.2 Discussion

The literature review and synthesis conducted for this research determined that, although there is ample evidence that IoT devices are capable of these threats, this information is not communicated in journalist-facing publications. Rather, it remains siloed in two forms; in heavily technical academic papers, and in resources created by organisations that support survivors of Intimate Partner Violence (IPV).[544] In the latter case, while the information on IoT threats is conveyed in a way that is accessible to non-technical audiences, it is not presented to journalists as also relevant to them, nor is there much discussion of the potential for targeted exploitation outside IPV scenarios. This is likewise the case in the existing academic research on IPV threat models relating to the IoT.[545]

The specialist nature of these different research communities enables in-depth studies into the security and privacy flaws inherent in the consumer IoT. There are also interdisciplinary discussions and studies conducted that involve experts in topics such as privacy, surveillance, cyber security and the IoT. However, their segregation from non-specialist media means that not just the press, but also other highly targeted groups, are underserved. This is due to multiple challenges: First, the need to identify that the consumer IoT may facilitate threats. Second, the task of finding relevant information that is not rife with exclusionary academic, policy-related, or technical jargon, as well as the potential psychological pressures (e.g. imposter syndrome) associated with attempting to comprehend such sources. Third, the difficulty due to a lack of exposition linking technical vulnerabilities to real-life threats.

This new categorisation contributes to this area of research in two ways. First, it presents clear descriptions and examples of all threats, whether they're regulatory and legal, threats relating to both technical manipulation, or human threats such as profiling and tracking. Second, it brings the IoT into

[543] Hoffmann S. IoT Security Architecture and Policy for the Home - a Hub Based Approach [Internet]. Oxford, United Kingdom: IoT Security Foundation; 2018 Nov [cited 2020 Aug 12] p. 40. Available from: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf; Gulzar M, Abbas G. Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET) [Internet]. Lahore, Pakistan: IEEE; 2019. p. 1–6. Available from: https://ieeexplore.ieee.org/document/8711834. p. 2.

[544] Lopez-Neira I, Patel T, Parkin S, et al. (2019) 'Internet of Things': How Abuse is Getting Smarter. ID 3350615, SSRN Scholarly Paper, 11 March. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.3350615; Tanczer L (2020) Gender and the Internet of Things ('IoT'): Futureproofing Online Harms legislation. Tech Abuse, February. London, UK: UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP). Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/ucl_g-iot_online_harms_tech_abuse_one_pager_-_feb2020.pdf (accessed 1 January 2021).

[545] Slupska J and Tanczer LM (2021) Chapter 39: Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In: Bailey J, Flynn A, and Henry N (eds) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Studies In Digital Crime, Technology and Social Harms. London, UK: Emerald Publishing Limited, pp. 663–688. DOI: 10.1108/978-1-83982-848-520211049; Lopez-Neira I, Patel T, Parkin S, et al. (2019) *'Internet of Things': How Abuse is Getting Smarter*. ID 3350615, SSRN Scholarly Paper, 11 March. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.3350615.

journalism-specific cyber security considerations. These changes allow this article to be used to increase journalists' awareness of potential threats, regardless of their level of technical or legal knowledge.

5.3.2.1 Example threat scenarios

In addition to threats that fit into each of the detailed categories, there are vectors of attack that can give rise to multiple threat categories. For example, adversaries may attempt to gain remote access through different host-based attacks on the IoT, on hardware, against users, and on software. Example threats are demonstrated in more detail in this subsection via narrative vignettes. More examples that fit each of the individual threat categories can be found in an article for *The Journalist's Resource* that is based on this research, intended to clarify IoT threats for a readership of journalists.[546] The purpose of including these vignettes elaborating on the categories above is to demonstrate that although some IoT devices are not commonly considered to be problematic, their built-in functionalities can in fact become destructive. These narratives are based on academic research that evidences these IoT capabilities, and draw from real-world examples of such threats. However, as will be discussed in Chapter 8, it is difficult to find proof of IoT threats enacted in a covert way, which limits the number of past cases that can be cited.

For example, an adversary may find a hardware attack easy if a device has insufficient authentication mechanisms or easily accessed USB ports,[547] such as a smart television in the lobby of a news organisation's offices. The adversary could use malware on a USB stick to achieve diverse goals, for example relating to threat type 3.1.5.2 Altering user-facing device and data attributes, part of Data and device modification threats. This could involve hijacking the smart screen to force it to display material of their choosing, such as disinformation or programming that distresses and distracts those who view it,[548] making them more vulnerable to social engineering attacks, including those that might reveal source identities.[549]

A second possible outcome, relating to threat category 3.1.6 Networked devices threats, is that the adversary uses this entry point to pivot into the news organisation's Wi-Fi network which, if not properly segregated and secured, may allow access to sensitive information.[550] A third outcome, relating to threat type 3.1.3.1 Continuous surveillance, part of the Profiling Threats category, could be that the device, as with many smart televisions, has a camera. The adversary could subsequently access this camera for live remote surveillance of everyone who enters and leaves the news organisation's building, which could facilitate physical attacks on members of the media.[551] This kind of psychological gaslighting could be replicated on a targeted individual scale if an intelligence agency manipulated a journalist's domestic IoT

[546] Shere ARK (2022) 6 ways the Internet of Things poses security threats to journalists. In: The Journalist's Resource. Available at: https://journalistsresource.org/media/6-ways-the-internet-of-things-poses-security-threats-to-journalists/ (accessed 6 December 2022).

[547] Nawir M, Amir A, Yaakob N, Lynn OB. Internet of Things (IoT): Taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED) [Internet]. Phuket, Thailand: IEEE; 2016. pp. 321-326. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7804660. p. 5.

[548] Romanek N. Cyberwar is Hell. FeedMagazine.tv. 2020 Mar;Who Goes There? The Cybersecurity Special(25): pp. 25-28; *Regime TV Channels hacked, showing MEK leader Massoud Rajavi's portray; January 27, 2022* (2022) YouTube. Available at: https://www.youtube.com/watch?v=AANEo9v_g-Q (accessed 5 December 2022).

[549] Popescul D (2018) Smart TVs: What Do They Know (and Tell) about Us? In: IACSS 2018 - IACLPM 2018 Joint Conference Proceedings, Czechia, 27 July 2018. The International Institute for Academic Development. Available at: https://www.academia.edu/37850674/Smart_TVs_What_Do_They_Know_and_Tell_about_Us (accessed 6 December 2022).

[550] Dhanjani N (2015) Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts. Sebastopol, CA, USA: O'Reilly Media, Inc.

[551] Michéle B and Karpow A (2014) Watch and be watched: Compromising all Smart TV generations. In: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), January 2014, pp. 351–356. IEEE. DOI: 10.1109/CCNC.2014.6866594.

devices to give the impression that secure communications channels and devices have been breached. This would possibly force them away from more secure communications channels that the adversary cannot breach (e.g. a channel entered via a gaming console, viewed via smart television) to a less secure one in panic.

Alternatively, another attack may involve socially engineering a journalist in different ways, such as by combining both threat categories 3.1.5 Data and device modification threats and 3.1.6 Networked devices threats. One example is by hacking a voice assistant and nudging the journalist such that they accidentally divulge the passwords to IoT devices or enable remote access to linked accounts.[552] This could facilitate continuous surveillance of the journalist, which may allow an adversary to remotely locate and eavesdrop on meetings that involve sensitive information, like source identities (per 3.1.3.1 Continuous surveillance, part of the Profiling Threats category). Another way in which social engineering might occur is if the functionality of an IoT device in the home is abused to scare family members of a journalist, which could add stressors that delay or even prevent the publication of a news story. For example, if an attacker accesses a baby monitor and makes an editor believe that their child is at risk,[553] that may chill or delay reporting on a particular topic. Additionally, any of the non-legal threat categories can overlap with category 3.1.2 Legal Threats if journalists are reluctant to report IoT breach issues to law enforcement. This could be due to credibility worries, data privacy concerns, or because police violence and indifference towards public violence against journalists has featured heavily in the news.[554]

Another example of a 3.1.3.1 Continuous surveillance threat is the risk of a journalist taking a call regarding a confidential source on an encrypted communications channel (e.g. Signal app), but in front of their smart television. The television may have a built-in microphone, and minimal security,[555] such that any information that can be picked up from the journalist's end of the call could be monitored or recorded and conveyed to a third party. This scenario was explicitly described by an exploratory study interviewee (I4) as being of particular concern (see: Chapter 4). The interviewee recognised that it might threaten source confidentiality or provide enough information on an as-yet unpublished story that the journalist and their news organisation could then be legally or physically targeted or threatened as secondary impacts of this information being accessed without consent via an IoT device. In fact, even if a journalist uses a pen and paper, instead of typing out notes on an interview with a source, they could still have their notes replicated by an attacker. This could be done via the hacking of a smart watch or fitness tracker, such that its motion recognition capabilities can then be used to estimate the content of something handwritten (per the Data and device modification threats category).[556] This shows the difficulty of finding measures that definitively protect against all emerging IoT threats, as discussed in Chapters 8 and 9.

---

[552] Nawir M, Amir A, Yaakob N, Lynn OB. Internet of Things (IoT): Taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED) [Internet]. Phuket, Thailand: IEEE; 2016. pp. 321-326. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7804660. p. 5.

[553] Wang AB (2018) Nest cam security breach: A hacker took over a baby monitor and broadcast threats, Houston parents say - The Washington Post. The Washington Post, 20 December. Available at: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/ (accessed 6 December 2022).

[554] Reporters Without Borders: 2020 World Press Freedom Index: "Entering a decisive decade for journalism, exacerbated by coronavirus" | RSF, https://rsf.org/en/2020-world-press-freedom-index-entering-decisive-decade-journalism-exacerbated-coronavirus.

[555] Bugeja J, Jacobsson A and Davidsson P (2018) An Empirical Analysis of Smart Connected Home Data. In: Internet of Things – ICIOT 2018 (eds D Georgakopoulos and L-J Zhang), Cham, 2018, pp. 134–149. Lecture Notes in Computer Science. Springer International Publishing. DOI: 10.1007/978-3-319-94370-1_10.

[556] Xia Q, Hong F, Feng Y, et al. (2018) MotionHacker: Motion sensor based eavesdropping on handwriting via smartwatch. In: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), April 2018, pp. 468–473. DOI: 10.1109/INFCOMW.2018.8406879.

As will be discussed in Chapter 7, some threat types, such as category 3.1.2 Legal Threats, target news organisations as a whole. These include stripping news outlets of their license to operate, live-streamed newsroom raids, pressures resulting in the withdrawal of advertising funds, and other surveillance and intimidation tactics that may not be legal but are nonetheless allowed by courts, such as in the case of Annika Smethurst.[557] The Internet-connected nature of the IoT combined with the dearth of cyber security legal frameworks means that state actors can intimidate journalists across international borders. This can be for reasons such as espionage (depending on a journalist's history of political sources), or even in order to destabilise democratic functions in other countries by threatening their press freedom.[558]

Similarly, incidents such as the Witness K case in Australia demonstrate that it is not just journalists and whistleblowers who are being prosecuted under national security laws for their access to classified information, but also - despite confidentiality expectations – lawyers, thereby creating uncertainty and fear about who journalists can rely on to protect them legally.[559] In fact, the evolution of IoT data collection, processing and transfer capabilities is accompanied by potential legal threats that may have not yet manifested simply because adversaries are only just realising that these censorship opportunities exist. There is already a documented chilling effect on the press resulting from states' attempts to legislate against strong encryption and national security and legitimate interest justifications used to allow intrusions into journalists' home and professional environments.[560]

5.3.2.2 Challenging areas and limitations

Even with validation techniques and interview data, however, these conceptual models inevitably have limitations in scope. For one, their application scenarios are relevant to journalists in relatively stable environments and so may not be as useful in all use cases. For example, for journalists working in warzones, there may be contextual uses of IoT that do not fit within the bounds of these conceptual models. However, journalists in such situations tend to be in immediate physical danger, which means that recognising and mitigating IoT threats may take a lower priority.

A limitation of this categorisation system is that IoT threat modelling is a nascent area, which is compounded by the fact that other intrusive technologies (e.g. Artificial Intelligence, biometrics, deep fakes, facial recognition, 5G, etc.) are emerging alongside the development of the consumer IoT, all of which intersect to facilitate unforeseen threats.[561] While this overlap has been mentioned in the conceptual model, it nevertheless remains an underexplored area within the broader cyber security field

[557] Phillips G. How the free press worldwide is under threat. The Guardian [Internet]. 2020 May 28 [cited 2020 Sep 11]; Available from: https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat; Noorlander MP. Background paper on the implementation of CM/rec(2016)4 on the safety of journalists and other media actors, for the Conference of Ministers responsible for Media and Information Society (Nicosia, Cyprus, May 2020) [Internet]. Council of Europe, Avenue de l'Europe F-67075 Strasbourg Cedex, France: Council of Europe; 2020 May [cited 2020 Sep 11] p. 26. Available from: https://rm.coe.int/background-paper-safety-of-journalists-and-other-media-actorsfinal/168094b396; Byrne E, Doran M. 'Far from over': News Corp journalist Annika Smethurst says High Court judgement a small victory [Internet]. Australian Broadcasting Corporation. 2020 [cited 2020 Sep 11]. Available from: https://www.abc.net.au/news/2020-04-15/annika-smethurst-wins-afp-fight-high-court/12147706

[558] Bobric G-D. STUDY REGARDING THE CYBER THREATS TO THE NATIONAL SECURITY. Bul Ştiinţ. 2020;1(49): pp. 18–25.

[559] Zifcak S. Why Bernard Collaery's case is one of the gravest threats to freedom of expression [Internet]. The Conversation. 2020 [cited 2020 Sep 11]. Available from: http://theconversation.com/why-bernard-collaerys-case-is-one-of-the-gravest-threats-to-freedom-of-expression-122463

[560] Brevini B. Metadata Laws, Journalism and Resistance in Australia. Media Commun. 2017 Mar 22;5(1): pp. 76–83.

[561] Wood P. Total Data Domination: 5G, IoT, AI Surveillance And The Smart City [Internet]. Technocracy News. 2019 [cited 2020 Sep 11]. Available from: https://www.technocracy.news/total-data-domination-5g-iot-ai-surveillance-and-the-smart-city/

as expert interviews, rather than published literature, give a fuller understanding of the compounded threat. Additionally, as demonstrated by the exploratory study (see: Chapter 4), journalists are largely unaware of IoT threats. Therefore the more clandestine threat scenarios that are explored in this model may go unreported, as journalists are gaslighted or simply do not realise that they might be occurring.[562]

Further, state actors, such as security and intelligence agencies, often do not disclose the full extent of their capabilities regarding computer network exploitation. Where these capabilities divulge that a specific journalist is perhaps investigating an issue that a government would prefer to remain covert, the current legal landscape regarding protection of journalists is murky. This could allow accusations and arrests on unrelated bases such that journalists can be silenced without their accusers needing to navigate press freedom concerns and protections, thereby allowing those technical surveillance and intimidation methods to go unrevealed.[563]

In fact, Smith noted that his colleague, "who spent a career in law enforcement (in the US, a country with constitutional privacy protections for citizens) observed that it's common practice for police to use illegal means to find out who's guilty—after which they then use legal means to obtain evidence for court."[564] There are therefore 'unknown unknowns' relating to IoT threat modelling that mean that there are currently gaps in this categorisation. Nevertheless, the goal of this system is to be iterative, based on continued expert interviews, and it will therefore continue to expand as this field does. As much of the IoT is dynamic, due to its portability and also models of shared ownership, this model is an organisational mechanism for journalist security training. It is not meant to imply that devices exist only in each specified environment.

Although the objective for this IoT threat categorisation is to inform journalists of their IoT threat landscape, it is conceivable that it would also highlight to IoT manufacturers the potential real-world impacts of their products' vulnerabilities. This would be a particularly welcome outcome, as a recent study demonstrated that the fundamental cyber security built into IoT products did not improve over 15 years, but that standards were instead slipping.[565] This concern is further discussed in Chapter 9.

5.3.3 Conceptual model 2 - Summary

One of the purposes of this categorisation is to galvanise the media industry to adopt industry-wide coordinated mitigation strategies (see: Chapter 8). Another benefit of this model is that it allows the descriptive and storytelling details of potential threats to be included without compromising visual clarity. As storytelling is a universal vehicle for educating and inspiring individuals, hypothetical consequence scenarios in this categorisation are intended to clarify information that could otherwise be too technical or otherwise inaccessible by framing it within the daily contextual reality of the target audience.[566]

[562] Moody. The enemy within: welcome to the Internet of gaslighting [Internet]. Privacy News Online by Private Internet Access VPN. 2020 [cited 2020 Sep 11]. Available from: https://www.privateinternetaccess.com/blog/the-enemy-within-welcome-to-the-internet-of-gaslighting/

[563] Deutsche Welle. Morocco arrests journalist on rape and spy charges [Internet]. www.dw.com. 2020 [cited 2020 Sep 11]. Available from: https://www.dw.com/en/omar-radi-morocco-journalist/a-54372595

[564] Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2017. p. 128.

[565] Cyber Independent Testing Lab. Binary Hardening in IoT products [Internet]. Cyber Independent Testing Lab. 2019 [cited 2020 Sep 11]. Available from: http://localhost:4000/2019/08/26/iot-data-writeup.html

[566] *The True Story of Using Fiction to Enhance Risk Intelligence* (2021) The Association of International Risk Intelligence Professionals (AIRIP). Available at: https://www.youtube.com/watch?v=qP_i94eP2Ho (accessed 18 January 2023); Lambe P. Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Oxford: Chandos Publishing (Oxford) Limited;

Further, the language for discussing as-yet unmanifested threats (particularly those related to law and cyber security) tends to be aggressive, invoking fear that can be debilitating.[567] This chapter intends to subvert that pattern by presenting threats in snapshots that communicate both the device capabilities and the stakes involved in possible escalation of the threats.

This model should therefore effectively raise awareness of common consumer IoT technologies and associated threats. In this way, it can be operationalised to provide a foundation for recommendations for minimising and mitigating these threats using journalists' personal and professional agency (see: Chapter 8).

5.4 Conclusion

The objective of this chapter was to create conceptual models that are directly relevant to the work of the free press, so that they understand the threats they may encounter from the IoT.

In the IoT devices by environment organisational model (see section 5.2), this objective was met by filtering devices by location and broad functionality, instead of by technical aspects (e.g. method of communication). This gives journalists and sources an accurate perception of where they might expect to find these devices so that they can be aware of their possible existence. The significance of this classification system for IoT devices is that it clearly demonstrates the ubiquity of these devices and their integration into daily life in all spheres.

Additionally, the IoT threat categorisation system (see section 5.3) highlighted that the IoT has the potential to pose an intentional or ambient threat to journalists' privacy, sources' confidentiality and therefore the security of both.

Both conceptual models are intended to elucidate IoT threats to journalists so that, even if they do not have the time or resources to invest in these kinds of solutions and mitigation methods, they would still recognise devices and related potential threats. The conceptual models enable the press to increase their awareness of IoT threats, before being presented with the recommendations for protections and mitigations in Chapter 8. It also expands on Chapter 4 by considering news organisations as well as individual journalists as potential victims. Later chapters (see: Chapters 6 and 7) will build upon this chapter by relating the threats explored here to the legislative and policy landscape in profiled countries. They will do so to establish the attention that can feasibly be given to these threats relative to others faced by the press, and to identify the structural causes of some of the threats. Then, Chapters 8 and 9 will discuss how these might be mitigated through individual, organisational and collective strategies and tactics.

2007. p. 119; Kazansky B (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society 8(1). SAGE Publications Ltd: 2053951720985557. DOI: 10.1177/2053951720985557.

[567] Lawson S (2012) Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. First Monday 17(7). DOI: 10.5210/fm.v17i7.3848; Cap P (2016) *The Language of Fear: Communicating Threat in Public Discourse*. London, UK: Springer.

Chapter 6: Main IoT risks perceived by interviewees: Laws

6.1 Introduction

This chapter compares and contrasts key details of the legislative and policy environments in Taiwan, Australia, the United Kingdom, and the United States. It thereby draws out the legal and law-related factors that increase IoT risk to journalists in these countries. This chapter contributes to this thesis's overall research question of "How can members of the press in democratic countries improve their identification of, protection from, and resilience against threats from the Internet of Things?" by investigating the most urgent barriers journalists and the media experience in protecting themselves from IoT threats, therefore illuminating the context in which any suggested improvements this thesis makes (see: Chapter 8) must operate.

This chapter and Chapter 7 report and analyse findings from 63 interviews with members of the media and cyber security experts, discussed thematically in conjunction with any extant reporting and literature to support the relevance of interviewee perceptions. Chapter 3, section 3.3, details the participant selection criteria, recruitment methods, and interview procedures. Further, Chapter 3, section 3.2.4.2, discusses the rationale for country selection, including that these countries are all primarily Anglophone democracies with unique geopolitical and legislative environments, thriving domestic IoT markets and historically positive press freedom records. The study included individuals with expertise and experience in laws relating to the media, privacy and data protection, surveillance, and regulation of the IoT. Some interviewees provided insights on more than one country.

These chapters present information from interviewees combined with secondary literary analysis,[568] to provide an evidence-based interpretation[569] presented in a thematic structure.[570] Specifically, the interview data was coded into themes (see: Chapter 3, sections 3.5.1 and 3.5.3) each representing a way in which interviewees perceived that IoT devices and related activity presented threats to the press.[571] These threats have been grouped into two overarching categories: legal and law-related risks (Chapter 6) and geopolitical and organisational risks (Chapter 7). Within each chapter, themes are presented in order of most to least concerning to interviewees. These two chapters should therefore be viewed as integrating results and discussion, embedding literature into the analysis of interview-derived "thick" findings.[572] This enables readers to understand the wider contextual factors that impact how the IoT threatens the press and the range of countermeasures and protections needed to enable mitigation, presented in Chapter 8.[573]

---

[568] Hesse-Biber, SN, & Johnson, RB (eds) 2015, The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry, Oxford University Press, Incorporated, Oxford. Available from: ProQuest Ebook Central: pp. 84, 198-200.

[569] Seidman I (2006) Interpreting The Material. In: *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. Third. New York: Teachers College Press, Columbia University, pp. 128–131.

[570] Hancock B, Ockleford E and Windridge K (2009) *An Introduction to Qualitative Research: Presenting Qualitative Research*. UK: The NIHR Research Design Service for Yorkshire & the Humber. Available at: https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/5_Introduction-to-qualitative-research-2009.pdf (accessed 21 December 2022).

[571] Erlingsson C and Brysiewicz P (2017) A hands-on guide to doing content analysis. *African Journal of Emergency Medicine* 7(3): 93–99. DOI: 10.1016/j.afjem.2017.08.001; Braun V and Clarke V (2013) Successful Qualitative Research: A Practical Guide for Beginners. London, UK: SAGE Publications Ltd.

[572] Yin RK (2009) *Case Study Research: Design and Methods*. Fourth. Applied Social Research Methods Series. California, USA: SAGE Publications, Inc; Hartley J (2004) Case Study Research. In: Cassell C and Symon G (eds) *Essential Guide to Qualitative Methods in Organizational Research*. London: SAGE Publications Ltd., pp. 323–333. DOI: 10.4135/9781446280119; Eisenhardt KM (1989) Building Theories from Case Study Research. *The Academy of Management Review* 14(4). Academy of Management: 532–550. DOI: 10.2307/258557.

[573] Ezzy D (2002) Chapter 6: Writing about qualitative data. In: *Qualitative Analysis: Practice and Innovation*. London, UK: Routledge, pp. 138–163.

In contrast to these two chapters, Chapter 5 did not have significant input from journalists, and focused more on what technical capabilities have been reported in the academic, grey, and government literature related to computer science and cyber security capabilities. Notably, however, despite the difference in sources used, one of the key threat areas presented in Chapter 5's threat categorisation is legal threats, and the overwhelming response from interviewees was also that legal threats relating to the IoT were seen as the most significant cause for concern. Chapter 6 therefore builds on Chapter 5 by emphasising and expanding on the significance of legal threats from the IoT, adding in primary qualitative data from a different set of experts to those presented in Chapter 5. This demonstrates the continued interdisciplinary and novel contribution of this research.

When asked about IoT threats to the press, interviewees overwhelmingly responded that laws and legislation that enable the acquisition of data from IoT devices by domestic government agencies is the most significant law-related IoT risk that they perceive to the media. This has been categorised under the theme heading "domestic government overreach," to encapsulate the interviewees' perception of these laws. Likewise, this chapter also explores the second most frequently observed threat raised by interviewees, termed "domestic government inadequacy" to convey their responses that detail areas where they perceive domestic governments should be more effectively protecting press freedom. These two themes are important findings to understand the lived realities of journalists and media organisations in four key countries. It also provides a useful foundation for ensuring that the countermeasures and mitigations recommended in this research (see: Chapter 8) will be practically relevant to the user population. The importance of journalist security tools being user-centric was explored in Chapter 2. Therefore, the framework set out in Chapter 8 will be able to take into account competing priorities and challenges at the forefront of real journalists' minds.

A further key audience for this chapter is policymakers, who will be able to compare the manifestation of certain threats and challenges across countries; they may derive useful insights regarding future-proofing technological legislation without eroding journalistic protections. Additionally, these insights about IoT risk to the media industry in each country can inform cyber security specialists and academic experts who focus on the security of highly targeted and under-resourced groups to understand how threats described in Chapter 5 are currently exemplified in each of these countries.

This chapter therefore begins by reporting and analysing the ways in which domestic government overreach occurs in the four countries, through carve-outs in laws, surveillance laws, and bulk data collection. It will then discuss the impact of domestic government inadequacy in each country and how it results in limited legal protections for journalists, insufficient IoT regulation, incompetent data protection, and cyber-physical criminal threats exacerbated by a lack of regulation of the IoT. Chapter 7 will then add to this analysis of legal and law-related risks by examining the geopolitical context and gaps in current protective mechanisms.

6.2 Theme 1: Domestic government overreach

The most frequently mentioned IoT-related threat to the press that interviewees perceived was domestic government overreach via legal means, via state agencies using mechanisms in legislation to access data that could include information on journalists and their sources. Their fear was that this would enable surveillance, including pattern of life analysis, which could divulge source identities or unpublished story details to domestic state actors.

When asked about existing legal protections for journalists and journalistic work, interviewees noted gaps that cause issues themselves and enable the other kinds of legislation explained below to negatively impact journalists and their work. While interviewees recognised limited instances of laws explicitly allowing law enforcement to hack IoT devices in order to collect data on targets for national security purposes, such as the one developed in the state of Queensland in 2019,[574] they also noted two main ways in which government overreach can occur, to the same effect: First, explicit clauses built into laws to allow state access to devices and data for national security reasons, such as the "Legitimate Interest" clause in the UK's Data Protection Act (2018)[575] and the US's Lawful Access to Encrypted Data Act (LAED Act) (2020).[576] Second, they mentioned laws that facilitate surveillance or weaken encryption, particularly technology-neutral ones that can incidentally cover the IoT, such as Taiwan's Cybersecurity Management Act (2018)[577] and Australia's Assistance and Access Act (2018). Research conducted for Chapter 2 suggested that the deployment of client-side scanning on even end-to-end encrypted private messaging systems is a trend, with the EU and now the UK's Online Safety Bill (2022) justifying this as necessary to counteract digital exploitation of children.[578] This sort of threat shows links between different types of government overreach, explored in subsequent subsections. Specifically, these issues could enable either bulk data collection or targeted data collection that can include information on or held by journalists and their sources.

One reason that interviewees reported fears about government overreach is that there is an absence of information available as to countries' authorities' capabilities regarding the consumer IoT.[579] For instance, P42, a journalist of 30 years, believes that Australian journalists remain unaware of IoT threats, beyond those associated with cameras.[580] This is in spite of the fact that interviewees noted that there has been reporting of unsecure consumer IoT devices in Australia being discovered, indexed and made accessible via the Internet regularly.[581] P26, who has 15 years of experience regarding legislation relating to the media and state surveillance capabilities in the UK, also recognised that the obfuscation of state capabilities has resulted in the challenges brought to the IPT being conducted with hypothetical rather than provable examples.[582] They noted that this is because "unless you have a way of accessing the security services' databases and technological capabilities, you will never know what's being used, and they all seem to me to be technically possible and even potentially legally permissible."[583]

[574] Interviewee: P33

[575] Shere A (2020) Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis. *The New Collection* 14: 3–21; Shere ARK (2020) Now you [don't] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy* 5(3). Routledge: 429–448. DOI: 10.1080/23738871.2020.1832129.

[576] Interviewee: P34; Pfefferkorn R (2020) There's Now an Even Worse Anti-Encryption Bill Than EARN IT. That Doesn't Make the EARN IT Bill OK. In: Center for Internet and Society at Stanford Law School. Available at: /blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok (accessed 1 January 2021).

[577] Interviewee: P49

[578] Gude K (2022) Encryption Helps Ukrainians Resist Russia's Invasion, but a European Plan Threatens the Underlying Trust Any Tech User Needs. *Just Security*, 17 November. Available at: https://www.justsecurity.org/84156/encryption-helps-ukrainians-resist-russias-invasion-but-a-european-plan-threatens-the-underlying-trust-any-tech-user-needs/ (accessed 20 November 2022).

[579] Interviewees: P30, P52

[580] Interviewee: P42

[581] Interviewees: P27, P52, P48; Roberts G (2020) Australians filmed through hacked private security cameras, live streamed on Russian-based website. *ABC News*, 23 June. Available at: https://www.abc.net.au/news/2020-06-24/security-cameras-hacked-streamed-on-russian-website/12380606 (accessed 31 December 2020).

[582] Interviewee: P26

[583] Interviewee: P26

UK interviewees argued that the Snowden disclosures had drastically increased journalists' security consciousness,[584] but that this is "vastly outweighed by the increased capabilities and availability of IoT devices, which are so much more substantial,"[585] and weaken the security of source communications. They noted that the lack of clarity regarding state agencies' potential decryption or data aggregation capabilities chills potential confidential sources.[586]

Therefore, this section will first discuss how interviewees understood existing protections for journalistic work to be lacking or impeded, then explore how interviewees described how legitimate interest carve-outs included in, for example, data protection laws allow access and use by state agencies and law enforcement agencies. It will then explore how interviewees perceived national security legislation to facilitate journalistic and source data being swept up in IoT surveillance. Next, it will discuss threats understood by interviewees regarding mass surveillance and bulk data collection by governments, leading to the formation of "Big Data." Finally, the section will cover any steps being taken to limit overreach in any of the four countries that interviewees reported.

Throughout, interviewees offered comparisons between three Five Eyes countries, as Australia's legal procedures derive from the UK's,[587] and Australia has a federal-state divide that impacts regulation akin to the US. Additionally, as members of this intelligence network, they have similar priorities and histories regarding surveillance laws, which are relevant to the IoT and press freedom. Although individual interviewees did not often liken Taiwan to the other three countries, comparative analysis revealed sufficient similarities across all four countries to demonstrate that Taiwan is only superficially an outlier.

6.2.1 Carve-outs in laws

Interviewees noted that one way in which states can access data and devices is through clauses in data protection legislation that purportedly limits access and transfer of data. They pointed out that this occurs through clauses that allow the state to access user data under the banner of justifications including national security.

For instance, UK surveillance in the name of national security relating to counterterrorism and anti-foreign interference was named as often being sufficient justification to override pre-existing legal protections, including for journalists.[588] This includes Section 50 of RIPA which requires subjects to disclose "any key in his possession to obtain access to the information or to put it into an intelligible form,"[589] which could include passwords to IoT devices, encryption keys or associated Cloud accounts and UK interviewees were concerned that refusal is punishable by a prison sentence.[590] Similarly, US interviewees also recalled repeated attempts to legislate for minimal encryption in the name of national security, which would leave devices easily compromised and threaten the confidentiality of conversations between journalists and their sources and editors.[591] These include the government-mandated inbuilt backdoor in the encryption

[584] Interviewees: P1, P15, P4, P53
[585] Interviewees: P4, P17; GCHQ (2019) The Equities Process. Available at: https://www.gchq.gov.uk/information/equities-process (accessed 1 January 2021).
[586] Interviewees: P43, P44
[587] Kercher B (2020) An Unruly Child: A History of Law in Australia. New York, NY, USA: Routledge.
[588] Interviewee: P26
[589] Parliament of the United Kingdom (2000) Regulation of Investigatory Powers Act 2000: Part III: Power to require disclosure: Section 50: Effect of notice imposing disclosure requirement. 2000 c. 23. Statute Law Database. Available at: https://www.legislation.gov.uk/ukpga/2000/23/section/50 (accessed 1 January 2021).
[590] Interviewees: P4, P15
[591] Interviewees: P59, P32

1993 Clipper chip,[592] the EARN IT Act (2020)[593] and the 2020 Lawful Access to Encrypted Data Act (LAED Act), named by interviewees.[594] Further, P25, a Taiwanese lawyer with expertise in information technology, communications and telecoms, and technology law and policy, also said that the Taiwanese national security agencies have enough legal authority that they "don't need to go through the detailed and transparent, maybe judicial process before they directly collect the data from the companies."[595]

Research conducted to corroborate the issues raised by interviewees found that there are also carve-outs exempting over twenty Australian government agencies from compliance with the Privacy Act (1988),[596] Australia's federal data protection framework. As a result of these clauses in legislation that otherwise limits data access and control, domestic government agencies may be granted access to IoT devices and data associated with journalists. This could enable state agencies to identify sources, prevent the release of stories, and tie journalists and media organisations up in lawsuits that drain their resources and hinder future reporting.

6.2.2 Surveillance laws

Interviewees considered surveillance laws that allow government access to data and devices via legal means to be less insidious and more common than legal carve-outs, but nevertheless overzealous means for domestic governments to threaten press freedom. Putting this interviews-derived theme in context of the thesis, this finding is relevant to IoT devices because their range of functionalities and the kinds of data that they can both collect and connect mean that journalists may be surveilled in new ways without governments needing to expand existing laws. Further, the prevalence of consumer IoT devices lowers the financial barrier for state agencies who might otherwise have had to invest in their own hardware, as now journalists may be monitored through their own devices and using the information they provide in private environments where there is the capacity for ambient surveillance.

For example, Australia interviewees were concerned about the Assistance and Access Act (2018), which provides legal authorisation for the authorities to compel telecommunications companies to inject malware packets into targeted IoT devices, to "slave" video or audio capabilities.[597] This was confirmed by a recent paper by Harkin and Mann, which found that a major impact of electronic surveillance laws in Australia was journalists having to turn down stories from sources who had not taken adequate security steps or who seemed like they were already being watched, both of which meant the journalist could not adequately engage in source protections.[598] This is consistent with Lashmar's work which noted that journalistic privacy and security have clear impacts on public interest and press freedom, such that

[592] Interviewees: P51; Carney D (1999) Summary: Security and Freedom through Encryption (SAFE) Act in 106th Congress. Available at: http://www.techlawjournal.com/cong106/encrypt/Default.htm (accessed 1 January 2021).
[593] Interviewee: P59
[594] Interviewee: P34; Pfefferkorn R (2020) There's Now an Even Worse Anti-Encryption Bill Than EARN IT. That Doesn't Make the EARN IT Bill OK. In: Center for Internet and Society at Stanford Law School. Available at: /blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok (accessed 1 January 2021).
[595] Interviewees: P25, P29
[596] Australian Government: Australian Law Reform Commission (2010) The number and scope of exemptions. Available at: https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/33-overview-exemptions-from-the-privacy-act/the-number-and-scope-of-exemptions/ (accessed 25 October 2022).
[597] Interviewee: P40
[598] Harkin D and Mann M (2022) Securing Australian Journalism from Surveillance. ACCAN Grants Program, August. Australia: Deakin University. Available at: https://blogs.deakin.edu.au/criminology/wp-content/uploads/sites/2/2022/09/Deakin_Report_Electronic-surveillance_V03-1.pdf (accessed 15 November 2022).

intelligence agencies' domain expansion and state intrusion against the media are serious threats to democracy.[599]

Interviewee responses on this topic were similar across the US, UK, and Australia, which could be attributed to the three countries' role in the Five Eyes intelligence alliance.[600] Interviewees for these countries reiterated the substantial amount of national security and surveillance legislation that has been passed in the aftermath of 9/11.[601] This was true in Australia,[602] which P42, a journalist of 30 years, stated to have "at least 82 [pieces of legislation], which is more than any other Western democracy."

Further, four interviewees reported that Australia's cyber laws – which are a combination of state-level and territorial laws that overlap with federal-level national security legislation regarding surveillance[603] – were seen as lacking when compared to European regulations;[604] asserting that this is likely to the benefit of the Australian government and the Five Eyes Intelligence network.[605] Four interviewees discussed that the speed of these kinds of laws being created made it difficult to raise concerns about them regarding press freedom.[606] Similarly, Pearson and Galvin assessed the role of Australia's Parliament in ensuring press freedom, compared to regional and global standards.[607] They noted that in debates, parliamentarians cite similar issues and solutions that have occurred abroad, signalling an awareness of the international significance of national press freedom. However, the authors also recognised that only 78 speeches out of roughly 190,000 in the decade mentioned press freedom, indicating a low prioritisation of the topic.

P30, an expert in law, technology, data sovereignty and data protection in the UK and Australia, posited that the continual introduction of new national security laws has allowed the Australian government and state agencies to "creep" and impinge on journalist protections, as the courts have not yet defined the parameters of these powers.[608] For example, P56, an expert in Australian laws relating to security and state surveillance in Australia, noted that under the National Security Legislation Amendment (Espionage

[599] Lashmar P (2020) Spies, Spin and the Fourth Estate: British Intelligence and the Media. Edinburgh, Scotland: Edinburgh University Press.
[600] Interviewees: P15, P26, P44, P4; Wells AR (2020) Between Five Eyes: 50 Years of Intelligence Sharing. United Kingdom: Casemate.
[601] Jones DM (2018) Intelligence and the management of national security: the post 9/11 evolution of an Australian National Security Community. Intelligence and National Security 33(1). Routledge: 1–20. DOI: 10.1080/02684527.2016.1259796.
[602] Interviewees: P55, P42, P33
[603] Interviewees: P28, P30; DLA Piper (2019) Law in Australia. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=AU&c2= (accessed 26 January 2020).
[604] Interviewees: P28, P33, P40, P30
[605] Interviewees: P28, P40; Mann M, Daly A and Molnar A (2020) Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications. Internet Policy Review 9(3). Available at: https://policyreview.info/articles/analysis/regulatory-arbitrage-and-transnational-surveillance-australias-extraterritorial (accessed 16 November 2022).
[606] Interviewee: P55, P42, P56, P40; Parliament of Australia (2011) *Cybercrime Legislation Amendment Bill 2011*. Bills Digest no. 31 2011-12. Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1112a/12bd031#_Toc301448354 (accessed 31 December 2020); Parliament of Australia (2012) *Cybercrime Legislation Amendment Act 2012*. No. 120, 2012-C2012A00120. Attorney-General's Department. Available at: https://www.legislation.gov.au/Details/C2012A00120/Html/Text, http://www.legislation.gov.au/Details/C2012A00120 (accessed 31 December 2020); The Australian Privacy Foundation (2011) *The Cybercrime Bill is Excessive and Unbalanced*. 7 September. The Australian Privacy Foundation. Available at: https://www.privacy.org.au/Papers/Cybercrime-PS-110904.html (accessed 31 December 2020).
[607] Pearson M and Galvin C (2019) The Australian Parliament and press freedom in an international context. *Pacific Journalism Review* 13(2). Pacific Media Centre. DOI: 10.24135/pjr.v13i2.910.
[608] Interviewees: P55, P42, P56, P40, P30

and Foreign Interference) Act 2018, "any journalist and their source who informs the public of [security service] misconduct may be imprisoned for up to 20 years, regardless of the gravity and circumstances of the crime committed."[609] This is irrespective of the level of public interest of the information or harm caused by its revelation - with no exemption from prosecution for journalists.[610]

UK-focused interviewees were similarly concerned about the surveillance enabled by the 2016 Investigatory Powers Act (IPA)[611] and, Daly *et al.* found that UK journalists are also concerned about the potential impact of the National Security Bill (2022) to cause sources to be treated in the same manner as spies.[612] Further, in the US, P35, a privacy advocate with four years of experience working on digital civil liberties in the US, mentioned that two federal laws - the 1986 Computer Fraud and Abuse Act (CFAA) and the Stored Communications Act (1986) - "come up very frequently with relation to First Amendment challenges" and are therefore likely relevant to use of devices against the press.[613] The CFAA prohibits unauthorised access to computers and the Stored Communications Act relates to disclosure of stored communications data to third parties, although an interviewee acknowledged that government powers in this regard were expanded by the USA PATRIOT Act (2001).[614]

Interviewees commented on an element of legislation facilitating surveillance – the need, or lack thereof, for a warrant: in some countries, it is overwhelmingly difficult to challenge a warrant, and in other cases, there could be no legal requirement for a warrant in order to access media property and information. For instance, Australia interviewee P30, a law and cyber security expert on the UK and Australia, pointed out that access to devices that are capable of ambient surveillance requires a warrant signed by a magistrate, with the implication that this could limit government interference.[615] They nevertheless recognised that there are ways of expediting this process, including the South Australian system of granting *ex parte* warrants over the phone to allow law enforcement officials to compel access to devices - a concerning possibility given the variety of kinds of data collected by the IoT.[616]

Also in Australia, interviewees recognised that challenging a warrant for access to journalistic material is hard because of the inherent weakness in an "implied" right when compared to the legal legitimacy of a warrant.[617] There, the High Court can assess whether a governmental mechanism or action perceived by a journalist as being contrary to their ability to politically communicate is "reasonably appropriate and adapted to achieving a legitimate end,"[618] which P30 said has "pushed the issue of rights into the judicial

[609] Interviewee: P56; Alliance for Journalists' Freedom (2019) *White Paper: Press Freedom in Australia*. May. Queensland, Australia: Alliance for Journalists' Freedom. Available at: https://www.journalistsfreedom.com/wp-content/uploads/2019/06/AJF-Press-Freedom-In-Australia-2019.pdf (accessed 31 December 2020).
[610] Interviewee: P40
[611] Interviewees: P4, P26, P44, P17, P43
[612] Daly A, Robinson E and McMenemy D (2022) Cyber security, surveillance and journalism in Scotland. Science, Policy and Law Series 1, Leverhulme Research Centre for Forensic Science, 27 September. Dundee, Scotland: University of Dundee. Available at: https://discovery.dundee.ac.uk/ws/files/81462869/CyberSecurity_DigitalReport_1.0.pdf; Patel P (2022) National Security Bill - Parliamentary Bills - UK Parliament. Bill 165 2022-23. Available at: https://bills.parliament.uk/bills/3154 (accessed 15 November 2022).
[613] Interviewee: P35
[614] Interviewee: P35; Internet Law Treatise (2013) Computer Fraud and Abuse Act (CFAA). Available at: https://ilt.eff.org/Computer_Fraud_and_Abuse_Act_(CFAA).html (accessed 28 October 2022).
[615] Interviewee: P30
[616] Interviewee: P30
[617] Interviewee: P42
[618] Griffiths L (2005) The Implied Freedom of Political Communication: The State of the Law Post Coleman and Mulholland. *James Cook University Law Review* 12: 93.

space, rather than it being a civic and cultural understanding of what those rights might be."[619] Meanwhile, interviewees noted that in the UK, under the framework of the IPA, the Investigatory Powers Commissioner's Office (IPCO) must approve invasive powers such as surveillance warrants. However, the warrants are granted in secret and there is no clear information about what knowledge or beliefs these judicial commissioners hold about journalist protection.[620]

Research conducted for publications related to this thesis found that both a former Investigatory Powers Commissioner and the National Union of Journalists (NUJ) have argued that the powers granted by the IPA are too far-reaching, in the latter case as they include inadequate safeguards for confidential journalistic sources.[621] Further, following the completion of interviews for this thesis, a 2021 High Court decision was made that general warrants granted under the 1994 Intelligence Services Act are incompatible with the country's general legal principles. However, the scope of the case did not cover any powers granted using the IPA.[622]

Regardless of the need for a warrant, access to media property through raids by law enforcement was at the forefront of journalist interviewees' minds in Australia in particular, as another common theme that emerged was the demonisation of the press by the Australian authorities. This is evidenced by multiple legal cases such as Annika Smethurst's,[623] Witness K and Bernard Collaery's,[624] and the Afghanistan war reporters' cases,[625] which were echoed by multiple participants.[626] This fraught relationship includes raids on newsrooms and journalists' homes that were considered by two interviewees to be conducted in an aggressive manner for the purpose of signalling and thereby chilling journalism.[627] Harkin and Mann noted that these recent AFP raids signalled new era of media information security, as they forced news organisations to consider designing protocols for mitigating the impact of these threats in the future.[628]

In the UK, there have also been notable similar cases that interviewees raised. One example of UK policing that impinged on protection of source information is the 2018 Northern Irish case involving journalists Trevor Birney and Barry McCaffrey, who were subjected to aggressive police tactics, including having their

[619] Interviewee: P30
[620] Interviewees: P17, P4
[621] Bowcott O (2019) 'Bulk hacking' by UK spy agencies is illegal, high court told. Available at: http://www.theguardian.com/technology/2019/jun/17/liberty-mounts-latest-court-challenge-to-snoopers-charter-mi5-gchq (accessed 1 January 2021).
[622] Scottish Legal News (2021) English High Court rules GCHQ general warrants require sufficient specificity. Scottish Legal News, 11 January. Available at: https://www.scottishlegal.com/article/english-high-court-rules-gchq-general-warrants-require-sufficient-specificity (accessed 1 March 2021).
[623] Interviewees: P42, P52, P55, P30, P40; Byrne E and Doran M (2020) 'Far from over': News Corp journalist Annika Smethurst says High Court judgement a small victory. Available at: https://www.abc.net.au/news/2020-04-15/annika-smethurst-wins-afp-fight-high-court/12147706 (accessed 11 September 2020).
[624] Interviewees: P55, P40, P56, P60, P42; Knaus C (2019) Witness K and the 'outrageous' spy scandal that failed to shame Australia. *The Guardian*, 9 August. Available at: http://www.theguardian.com/australia-news/2019/aug/10/witness-k-and-the-outrageous-spy-scandal-that-failed-to-shame-australia (accessed 31 December 2020).
[625] Interviewees: P28, P42, P56, P40, P60; Lyons J (2019) AFP raid on ABC reveals investigative journalism being put in same category as criminality. *ABC News*, 15 July. Available at: https://www.abc.net.au/news/2019-07-15/abc-raids-australian-federal-police-press-freedom/11309810 (accessed 31 December 2020); Politics Desk (2020) ABC journalist Dan Oakes will not be prosecuted over Afghan Files leak. *ABC News*, 15 October. Available at: https://www.abc.net.au/news/2020-10-15/dan-oakes-afghan-files-prosecution-decision/12771304 (accessed 31 December 2020).
[626] Interviewees: P30, P56, P40, P52, P55, P42, P60
[627] Interviewees: P52, P56
[628] Harkin D and Mann M (2022) Securing Australian Journalism from Surveillance. ACCAN Grants Program, August. Australia: Deakin University. Available at: https://blogs.deakin.edu.au/criminology/wp-content/uploads/sites/2/2022/09/Deakin_Report_Electronic-surveillance_V03-1.pdf (accessed 15 November 2022).

homes and offices raided and journalistic materials seized.[629] Laws they mentioned that can be used to justify law enforcement access to media documents and devices range from use of the Official Secrets Act[630] (as in this case, along with the Northern Irish Police and Criminal Evidence Order 1989),[631] to detention or the seizure and search of devices related to published materials under the Terrorism Act (2000),[632] and charges brought under the Computer Misuse Act and the Regulation of Investigatory Powers Act 2000 (RIPA).[633] Although the warrant used for the Birney and McCaffrey case was deemed unlawful post-hoc, extrapolating from interviewee reports suggests that the fact that the raid was able to happen at all offers a potentially chilling precedent to journalists.

In contrast to the overt nature of raids, in Australia, interviewees named highly publicised anti-strong-encryption proposals, such as the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, also known as the Assistance and Access Act.[634] This requires relevant companies to assist the authorities in decrypting communications. P42, a journalist of 30 years, argued that "the warrant regime around that is incredibly lax, so the journalist's own data is exposed to police investigation and the relationship between journalists and their sources is exposed to police inquiry, and the sources themselves are becoming vulnerable to police prosecution."[635] P40, an investigative journalist with eight years of experience, including working on multiple international collaborative investigations, noted that the Assistance and Access Act allows states to engage in "murky and nefarious" applications that corporate actors could not legally do.[636] P40 noted that these include "an example of a certain attack that was canvassed in parliamentary hearings, was a carrier level insertion of malware into a device."[637]

Interviewees acknowledged that similar attempts to legislate weak encryption have occurred in the US, such as backdoor provision for law enforcement included in the EARN IT Act (2020),[638] which could threaten confidential journalist-source communications. They recognised that source confidentiality is also threatened by vehicular surveillance, such as the presence of Automatic Number Plate Recognition (ANPR) technologies across all American states.[639] These data aggregated at the federal level could be used to identify meetings between whistleblowers and journalists.[640] While ANPR data is centralised, the federal-state divide has resulted in fragmentation of the implementation of other surveillance capabilities. P32, who has over five years' experience with legal, political, and technological press freedom issues,

[629] Interviewees: P44, P15, P45; Northern Ireland Desk (2020) Loughinisland: Journalists search warrants wrongly obtained. BBC News, 10 July. Available at: https://www.bbc.com/news/uk-northern-ireland-53367027 (accessed 1 January 2021).
[630] Interviewees: P15, P1
[631] In The High Court Of Justice In Northern Ireland, Queen's Bench Division (Judicial Review), In The Matter Of An Application By Fine Point Films And Trevor Birney For Judicial Review And In The Matter Of An Application By Barry Mccaffrey And In The Matter Of An Application By PSNI And Durham Constabulary For Search Warrants (2020) Ref: MOR11288. Available at: https://www.judiciaryni.uk/sites/judiciary/files/decisions/Fine%20Point%20Films%20and%20Birney,%20McCaffrey%20and%20PSNI%20and%20Durham%20Constabulary%20Applications.pdf.
[632] Interviewees: P15, P17; Bowcott O (2016) Terrorism Act incompatible with human rights, court rules in David Miranda case. Available at: https://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case (accessed 1 January 2021).
[633] Interviewee: P15; Thipursian ED, Thogarcheti S, Fahad AA, et al. (2014) Case Study – News of the World Phone Hacking Scandal (NoTW). Available at: https://resources.infosecinstitute.com/topic/case-study-news-world-phone-hacking-scandal-notw/ (accessed 1 January 2021).
[634] Interviewees: P40, P42, P28, P33, P55, P36, P52, P56
[635] Interviewee: P42
[636] Interviewee: P40
[637] Interviewee: P40
[638] Interviewee: P59
[639] Interviewee: P59
[640] Interviewee: P59

noticed carve-outs for state offices and law enforcement as a standard across most US privacy legislation.[641] They were concerned that this allows information sharing across decentralised agencies.[642]

Another feature of surveillance laws that interviewees found harrowing was the lack of confirmation as to whether surveillance was happening at all, preventing them from accurately assessing the risk to them and their sources. For example, P4, an expert in state capabilities and legislation relating to use of IoT devices for surveillance of the press in the UK, mentioned that in the UK, any suspected unlawful surveillance cases can be taken to the Investigatory Powers Tribunal (IPT), which operates under a "neither confirm nor deny" policy regarding whether the surveillance is happening at all.[643] The USA PATRIOT Act (2001), too, was described by interviewees as being "draconian" in its allowance of intrusive technical measures to enable access to data through hacking devices.[644] Additionally, the US's Electronic Communications and Privacy Act (1986) was noted by interviewees as only requiring a warrant to access digital content that is under 180 days old, and it may otherwise be accessed through a court order or administrative subpoena. McGregor noted neither of these require "significant judicial oversight" to be granted, nor do data subjects need to be notified in a timely fashion.[645]

A further issue that interviewees recognised as eking away at journalistic exemptions from surveillance is the existence of surveillance laws that do not include IoT-specific privacy provisions or exemptions; these can be termed "technology-neutral" because they apply across a range of technologies.[646] Multiple interviewees acknowledged that this incidental coverage of IoT capabilities in existing government responses makes exploitation of devices by state agencies possibly lawful because it has not been banned, such as those intended to relate to CCTV cameras.[647] An example named by interviewees of the UK not mentioning the IoT in recent policy materials is its Online Harms White Paper (2019), which recognised the potential for physical and psychological harm through Internet access but did not cover the IoT.[648] Extrapolating from interviewee responses, this is concerning for journalists who may be susceptible to IoT threats because of an absence of enforced regulation of top-down technical and policy protections.

Interviewees noted that many of Australia's recent proposals regarding both surveillance legislation and IoT self-regulation are modelled on ideas from the UK, with slight deviations, meaning there is vague technical language in each country's laws.[649] For example, when comparing the UK's 2016 Investigatory Powers Act (IPA) and subsequent Australia's Assistance and Access Act (2018), P30, a law and cyber security expert on the UK and Australia, noted that the IPA includes specialist terms such as "Technical Capability Order" that are ill-defined within the legislation. This has the effect of allowing varied

[641] Interviewee: P32
[642] Interviewees: P32, P47
[643] Interviewee: P4
[644] Interviewee: P41
[645] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[646] Interviewee: P17
[647] Interviewees: P17, P4, P26, P30, P52
[648] Interviewees: P43, P31; Tanczer L (2020) Gender and the Internet of Things ('IoT'): Futureproofing Online Harms legislation. Tech Abuse, February. London, UK: UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP). Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/ucl_g-iot_online_harms_tech_abuse_one_pager_-_feb2020.pdf (accessed 1 January 2021); Secretary of State for Digital, Culture, Media & Sport and Secretary of State for the Home Department (2020) Online Harms White Paper: Full Government Response to the consultation. December. London, UK: HM Government. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf (accessed 1 January 2021).
[649] Interviewees: P30, P55

interpretations of legitimate actions including decryption of communications, where interviewees saw Australian law as more "forthright" in its intention to weaken encryption than UK law.[650] Similarly, Taiwan interviewees mentioned the Cybersecurity Management Act (2018), which regulates the cyber security of infrastructure such as telecoms cables[651] but which has vague terms.[652]

6.2.3 Bulk data collection

The current state of legal surveillance discussed above was considered by interviewees to be indicative of a cultural norm of maximising intelligence gathering, resulting in large-scale data collection and retention. This means that governments have access to Big Data, i.e. datasets that are huge, fast-accumulating and complex.[653] Interviewees were troubled by the implications of these concepts for press freedom because they allow government agencies to aggregate, link and cross-reference metadata to create rich profiles on an individual that could be used to identify sources and stories and to threaten journalists.[654] Additionally, Sinha found "chilled" relations between officials and journalists as a result of the legalisation and normalisation of large-scale surveillance, facilitated by the increased risk that any digital actions will leave identifiable traces (both regarding content and metadata).[655]

One of the paradoxes that will plague the future of the media that Berger identified is the "ambiguous digital sword," which acknowledges both the attractiveness of increased digitisation for journalism, and the dangers for journalists and sources of the data generated to be accessed by malicious actors.[656] As noted by US interviewees, international collaborative journalism that relies on networked technologies, like the Panama Papers, might not be possible if there is lawful warrantless access for intelligence agencies to all IoT-generated profiles or databases that could then alert authorities to journalists' news subjects and sources and chill reporting.[657]

An extreme example of bulk data collection that was seen by Australia interviewees as specifically designed to enable government access is the Australian Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.[658] This law compels telecoms companies to retain the metadata associated with Australian citizens for at least two years. Research into interviewee concerns about this law found that it has been criticised for a number of reasons, including the fact that the legislation gives 22 government agencies access to the metadata without the need for a warrant,[659] and the telecoms companies have reported multiple instances of other agencies requesting illegal access to journalists' metadata.[660] Further, former Australian Privacy Commissioner Timothy Pilgrim noted that two years may

[650] Interviewee: P30, P55
[651] Interviewees: P25, P49
[652] Interviewee: P49; P63 asserted that "there are not enough specifications for modern data collection" inherent in the data protection legislation.
[653] Casanovas P, De Koker L, Mendelson D, et al. (2017) Regulation of Big Data: Perspectives on strategy, policy, law and privacy. *Health and Technology* 7(4): 335–349. DOI: 10.1007/s12553-017-0190-6.
[654] Interviewee: P61
[655] Sinha, G.A.: With liberty to monitor all: how large-scale US surveillance is harming journalism, law and American democracy. Human Rights Watch, New York, N.Y. (2014).
[656] Berger G (2018) Is There a Future for Journalism? *Journalism Practice* 12(8). Routledge: 939–953. DOI: 10.1080/17512786.2018.1516117.
[657] Interviewees: P32, P47, P34
[658] Interviewees: P40, P42, P28, P30, P33, P55, P36, P52
[659] Interviewees: P42, P28, P52, P33, P55
[660] Karp P and Taylor J (2019) Police made illegal metadata searches and obtained invalid warrants targeting journalists. Available at: http://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists (accessed 31 December 2020); Communications Alliance (2020) Government Must Support Security Committee Recommendations And Repair The Data Retention Regime. 2020 Media Release 31, 29 October.

be unjustifiable when compared to the fact that "90 percent of investigations relying on retained data only use data that is less than one year old."[661] Critics of this kind of data retention scheme also argue that the IoT industry is aware of the enormous volume of data captured by just one IoT device and do not want to be responsible for storage of the data generated by multiple devices.[662] Although there is a provision in the law intended to protect press freedom by requiring a warrant before any retained data can be accessed by state agencies for investigations focused on journalists, this still has the potential to "chill" journalistic expression, given the ubiquity of the IoT.[663]

Similarly, P15, a media lawyer at an international news organisation, expressed concern that there are insufficient safeguards to prevent journalists' or sources' data from being swept up via the UK's Data Retention and Investigatory Powers Act 2014 (DRIPA), which allows UK state agencies to collect and retain vast amounts of information.[664] They recognised that the IPA replaced some, but not all, elements of the Regulation of Investigatory Powers Act 2000 (RIPA) and DRIPA, which have been criticised for their limited journalist protections, including by a former Interception of Communications Commissioner.[665] P15 noted that there may not be adequate mechanisms for scrubbing any inadvertently collected protected information from state systems or from removing such data from bulk materials requested from commercial entities such as telecoms providers.[666] Interviewees noted that this gives rise to fears that sources may be identified if agencies cross-reference article publication dates with historic data collected on potential whistleblowers, which could have a chilling effect.[667]

Relatedly, both Noto La Diega and Tanczer *et al*. recognised the conflict between the imperative to protect IoT-generated data and the existence of laws such as the Investigatory Powers Act (2016), which allow government collection and analysis of such consumer data.[668] US interviewees were concerned about the legal dragnet effects of comprehensive and quasi-indiscriminate surveillance,[669] mentioning the 1978 Foreign Intelligence Surveillance Act (FISA) and the Foreign Intelligence Surveillance Court (FISC).[670]

However, interviewees reported that the US struggles to regulate surveillance technologies, with federal equipment grants sometimes providing financial incentive for commercial companies to maximise their

Sydney, Australia: Communications Alliance. Available at: https://www.commsalliance.com.au/Documents/releases/2020-media-release-31 (accessed 31 December 2020).

[661] Reichert C (2015) Data retention a barrier for IoT. Available at: https://www.zdnet.com/article/data-retention-a-barrier-for-iot/ (accessed 26 February 2020).

[662] Reichert C (2015) Data retention a barrier for IoT. Available at: https://www.zdnet.com/article/data-retention-a-barrier-for-iot/ (accessed 26 February 2020).

[663] Lashmar P (2020) Spies, Spin and the Fourth Estate: British Intelligence and the Media. Edinburgh, Scotland: Edinburgh University Press.

[664] Interviewee: P15

[665] Interviewee: P45; Townend J and Danbury R (2017) Protecting Sources and Whistleblowers in a Digital Age. 22 February. London, UK: Information Law and Policy Centre, Institute of Advanced Legal Studies. Available at: https://infolawcentre.blogs.sas.ac.uk/source-protection-report-2017/ (accessed 1 January 2021).

[666] Interviewee: P15

[667] Interviewees: P41, P15

[668] Noto La Diega G (2016) Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom. *Journal of Law & Economic Regulation* 9(1): 69–93; Tanczer L, Brass I, Elsden M, et al. (2019) The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In: *Rewired: Cybersecurity Governance*. Hoboken, NJ: Social Science Research Network, pp. 37–56. Available at: https://papers.ssrn.com/abstract=3385548 (accessed 22 April 2021).

[669] Interviewees: P32, P34

[670] Interviewees: P32, P17

data collection capabilities.[671] P32, who has over five years' experience with legal, political and technological press freedom issues, noted that IoT devices were first marketed in an "open-ended" way; then this became security-related in increments, until the advertising justified its use by law enforcement, as in the case of Ring doorbells, which pose both ambient privacy threats and associated legal threats.[672]

Legal threats relating to use of the IoT as evidence to incriminate individuals are not restricted to Ring, with US interviewees recalling cases of voice assistants witnessing murders and health monitoring devices refuting the alibi of a suspect.[673] Similarly, P63, an investigative reporter, discussed the Taiwanese authorities' predilection for the construction of Big Data and their encouragement of private sector data collection, noting that Big Data from the IoT may be applied in law enforcement activities when the market becomes more developed.[674] Thus, interviewees claimed that source confidentiality is threatened by the imperative that private entities are driven to collect and share data with state agencies.[675]

Further, common across the countries, interviewees expressed concerns about how data aggregation and linkability could both compromise privacy, as they can be used to identify and track individuals across various IoT datasets, enabling further emergent threats such as doxxing or blackmail and discovering a story prior to publication.[676] P33, who has expertise in regulation of the IoT and 16 years of experience in researching technological threats to the press in Australia, noted the danger of Big Data regarding information collected about a journalist by the IoT. They were worried that this could allow adversaries to analyse behavioural patterns to such a fine degree that they can establish markers to denote certain journalistic activities (e.g. being contacted by a confidential source).[677] Multiple interviewees feared that this would result in undesirable journalistic work being inferred and prevented prior to publication.[678]

Secondary threats mentioned by interviewees include the creation and use of information campaigns against journalists through microtargeted political or commercial advertising, in order to undermine social cohesion in a multicultural country like Australia by propagating disinformation and propaganda.[679] Other secondary physical threats that were raised include identification of a journalist's domestic devices and to target them to cause fires, to facilitate break-ins,[680] or to exploit devices in a series of chained attacks.[681] Interviewees recognised that in the UK at least, this scenario is more likely because data aggregation is legally permissible because legislators did not anticipate or outlaw scenarios of infringements of bystander privacy by commercial actors;[682] nor did UK legislators preclude this data being given to law enforcement and aggregated in order to profile individuals or create databases that would harm press freedom by chilling both sources and journalistic activities.[683]

[671] Interviewees: P34, P32, P47; New York Desk (2021) America grapples with regulating surveillance technology. The Economist, 9 March. Available at: https://www.economist.com/united-states/2021/03/09/america-grapples-with-regulating-surveillance-technology (accessed 23 March 2021).
[672] Interviewees: P6, P62, P32, P34, P37, P21, P35
[673] Interviewees: P37, P51
[674] Interviewee: P63
[675] Interviewees: P9, P44, P47
[676] Interviewees: P61, P37, P34, P62, P51, P47, P40, P33, P27, P56
[677] Interviewee: P33
[678] Interviewees: P33, P40, P55, P52, P48
[679] Interviewee: P14
[680] Interviewee: P8
[681] Interviewee: P24
[682] Interviewees: P26, P43, P45, P4
[683] Interviewees: P26, P43, P45, P4

6.3 Theme 2: Domestic government inadequacy

Intentional government overreach is not the only threat interviewees perceived to journalists from domestic governments. They further recognised that inadequate protections and regulations can increase IoT risk and prevent journalists from being able to prioritise the IoT, relative to other drains on their time, energy, and resources. This section will first discuss some legal threats interviewees named as limiting press freedom and the media's ability to counter IoT risk. Then, it will examine threats that interviewees saw can stem from governments collecting data without installing satisfactory protections. It will then follow interviewees' discussions of the lack of IoT regulation that mandates high levels of security and privacy by design, followed by data protection laws that do not provide enough incentive to minimise IoT risk. Finally, it will explore some of the criminal threats exacerbated by the aforementioned insufficient IoT regulation that interviewees found concerning.

6.3.1 Insufficient journalist legal protections

For all kinds of domestic government overreach, interviewees for all four countries registered concern that established journalistic legal protections were proving insufficient against government overreach and surveillance, including direct government interference. UK and US interviewees argued that source confidentiality and security are deteriorating despite the fact that the UK and the US have both significant journalistic protections against this kind of overreach: the First Amendment of the US Constitution and the UK's Bill of Rights.[684] They framed this within the context of the erosion of other democratic values due to changing norms in government enforcement that reduce pre-existing safeguards.[685] Taking this to an extreme, rather than a legislatively enshrined 'right to free speech,' interviewees noted that Australia has an 'implied freedom of political communication,' inferred from the Australian Constitution by the High Court during the 1997 Lange v Australian Broadcasting Corporation court case.[686]

While there is no statutory regulation of journalism in either the UK or US, interviewees recognised norms and legislation that are intended to legally restrict press capabilities.[687] One example of informal press regulation in the UK that was named is the D-notice committee, which implements a UK-press-specific system intended to preserve national security.[688] Interviewees described its purpose as nudging journalists to self-censor stories that could compromise military affairs, without creating public furore.[689] P45, an expert in press freedom and surveillance law, also criticised guidelines released by the Crown Prosecution Service that advise on how journalists and sources may be prosecuted "where it may not be in the public interest to do so."[690] Although the First Amendment provides protection for journalists in the

[684] Interviewees: P30, P55, P42, P27

[685] Interviewees: P9, P44, P47, P23, P17, P4, P26, P43

[686] Interviewees: P30, P42; Rule of Law staff (2019) Implied Freedom of Political Communication - Case Note and New Resource. In: *Rule of Law Education Centre*. Available at: https://www.ruleoflaw.org.au/implied-freedom-of-political-communication-case-note-and-new-resource/ (accessed 31 December 2020); High Court of Australia (1997) *Lange v Australian Broadcasting Corporation ('Political Free Speech case')*. 25. Available at: http://www7.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/1997/25.html (accessed 31 December 2020).

[687] Interviewees: P22, P23

[688] Interviewees: P41, P4; Greenslade R (2015) The D-notice system: a typically British fudge that has survived a century. Available at: http://www.theguardian.com/media/2015/jul/31/d-notice-system-state-media-press-freedom (accessed 1 January 2021).

[689] Interviewees: P41, P4; Greenslade R (2015) The D-notice system: a typically British fudge that has survived a century. Available at: http://www.theguardian.com/media/2015/jul/31/d-notice-system-state-media-press-freedom (accessed 1 January 2021).

[690] Interviewee: P45; Crown Prosecution Service (2019) Media: Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists | The Crown Prosecution Service. Available at: https://www.cps.gov.uk/legal-guidance/media-prosecuting-cases-where-public-servants-have-disclosed-confidential#c5 (accessed 1 January 2021); Crown

US,[691] interviewees were still concerned about legal threats to sources; they most often referenced the Espionage Act (1917),[692] Participants acknowledged that this has never been used to prosecute a mainstream news publisher but that it lacks a public interest defence and has been increasingly used against whistleblowers.[693] Similarly, P55, who has thirteen years of experience as a cyber security journalist, stated that there is a constant propagation of a national security imperative by the Australian authorities, which few organisations feel able to challenge.[694]

In something of a contrast, P5, who has 25 years of experience working on press freedom in Taiwan, posited that direct attacks on the press or press freedom in Taiwan "would be considered against Taiwanese values and would be noticed by the public," and instead framed Taiwan's challenges in this area as fundamentally due to a "misunderstanding of 'press freedom' as a concept."[695] Interviewees argued that this misunderstanding stems from a history of martial law and the country's proximity with China, leading to the Taiwanese government being afraid of restricting press freedom to such an extent that it under-regulates other threat factors and at the same time appears complacent regarding attacks on the media within Taiwan, because of their juxtaposition with China's treatment of journalists.[696] Analysis of interviewees responses found that this has resulted in a similar problem in Taiwan as in the other three countries: reporting on cyber security threats to journalists is low, despite ample media coverage of such threats to each country in general.[697]

In addition to the laws below that are specifically threatening journalists' security via the IoT, interviewees mentioned other legal threats to media freedom that can be combined with carve-outs, surveillance laws, and bulk data collection to compound the impacts on journalists of domestic government overreach. This includes legislation that UK interviewees believed impacts press freedom includes libel law,[698] which interviewees reported meant that "anybody who had access to lawyers and funds could tie newspapers up for months, if not years in litigation over risk to reputation."[699] Interviewees feared that this drains financial resources, time and energy until the news organisation folds, sending a chilling message to the wider press. Interviewees noted that there is a recent increase in "vexatious litigation" where claims are taken to UK courts in strategic lawsuits against public participation (known as SLAPP cases) that are intended to overwhelm and incapacitate sources of independent public interest journalism.[700] [701] British law firms and courts were noted by interviewees as often being chosen through "forum shopping" for a jurisdiction with laws that are preferential to claimants.[702] They gave the example of Appleby suing only

Prosecution Service (2019) Media: Assessing the Public Interest in Cases Affecting the Media | The Crown Prosecution Service. Available at: https://www.cps.gov.uk/legal-guidance/media-assessing-public-interest-cases-affecting-media (accessed 1 January 2021).

[691] Interviewees: P47, P23, P17

[692] Interviewees: P9, P44, P47

[693] Interviewees: P9, P44, P47

[694] Interviewee: P55

[695] Interviewee: P5

[696] Interviewees: P5, P49

[697] Interviewees: P49, P5

[698] Interviewees: P4, P22, P1, P53, P15, P44

[699] Interviewee: P1

[700] Neate R and correspondent RNW (2022) Senior media figures call for law to stop oligarchs silencing UK journalists. *The Guardian*, 29 November. Available at: https://www.theguardian.com/news/2022/nov/29/slapps-senior-media-figures-call-for-law-stop-oligarchs-silencing-uk-journalists (accessed 21 December 2022).

[701] Interviewees: P15, P44

[702] Interviewee: P44; Phillips G (2020) How the free press worldwide is under threat. The Guardian, 28 May. Available at: https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat (accessed 11 September 2020).

the UK news organisations of the over 90 media partners involved in the Paradise Papers revelations for breach of confidence relating to the source materials.[703] P44, an expert in threats to press freedom in the UK and US, stated that "that felt very much like a test case [... and ...] the fact of that suit was concerning because it demonstrates that there's something about the UK's legal climate that makes it more attractive to take legal action against journalists here than in other jurisdictions."[704]

6.3.2 Insufficient IoT regulation

Multiple interviewees across all countries registered concern that a lack of IoT regulation increases risk for journalists and the press as a whole. Specifically they felt that the lack of regulation removed the incentive for security and privacy by design,[705] which enables data breaches that would threaten source confidentiality, as discussed in Chapter 2. However, interviewees acknowledged established challenges associated with attempted regulation of the IoT.[706] They noted that some experts prefer technical compartmentalisation and separate controls for each aspect of a device but acknowledge that this also relies on consistent policies related to patching.[707] Some argue that a usability focus is the only way to minimise the number of successful social engineering attacks,[708] while others are interested in adaptive governance models that deviate substantially from traditional safety regulation processes.[709] After this study concluded, a 2022 Atlantic Council report on multinational work to secure the IoT ecosystem separately reached similar conclusions to the points raised in this subsection.[710]

Specifically, this subsection will first discuss interviewee perceptions of the state of IoT markets and regulatory cultures in each country to understand challenges to creating sufficient legislation. Then it will cover interviewees' thoughts on the way these states have attempted self-regulation and their critiques of these efforts. The subsection will then examine interviewee discussion of current efforts towards direct legislative intervention, including options such as mandatory baseline security, labelling programmes, and the interconnectedness of IoT regulation with other laws, such as around data and privacy. Finally, it will note key considerations in improving IoT regulation and legislation, as raised by interviewees.

To understand the scale of the impact of the lack of IoT regulations and their effect on threats to journalists, interviewees were asked about factors influencing the consumer IoT market and uptake in each country. Taiwan interviewees offered mixed and sometimes contradictory accounts of the consumer IoT landscape,[711] with some indicating that there was high market saturation of IoT devices in Taiwan,[712] and others sharing their view that the Taiwanese IoT market is undeveloped, and that the consumer IoT has not yet penetrated Taiwanese society.[713]

---

[703] Guardian staff (2017) Paradise Papers legal action against BBC and Guardian condemned. Available at: http://www.theguardian.com/uk-news/2017/dec/19/paradise-papers-legal-action-against-bbc-and-guardian-condemned (accessed 1 January 2021).
[704] Interviewee: P44
[705] Interviewee: P5
[706] Interviewees: P2, P20, P50
[707] Interviewee: P2
[708] Interviewee: P2
[709] Interviewee: P20
[710] Mitchell P, Rowley L, Sherman J, et al. (2022) *Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem*. 26 September. Washington, D.C.: The Atlantic Council's Cyber Statecraft Initiative, under the Digital Forensic Research Lab (DFRLab). Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/ (accessed 24 October 2022).
[711] Interviewees: P5, P25, P39, P29, P58, P38, P63
[712] Interviewees: P38, P29
[713] Interviewees: P25, P63

In contrast, Australians are seen by interviewees as rapid and prolific adopters of technologies,[714] although P55, who has thirteen years of experience as a cyber security journalist, speculated that uptake of the consumer IoT has been limited "by the relatively slow speeds of the National Broadband Network."[715] P36, an expert in Australia's national cyber security strategy, noted that the first wave of purchases in Australia related to home security and home entertainment devices but not voice assistants, and the second wave related to recreational-use drones – which is when Australians began to conceptualise IoT threats.[716] P36 also stated that the uptake of smart TVs in Australia was rapid, reflected by the "rapid flex, really significant uptake of sensor networks in advanced manufacturing environments."[717]

Similarly, unlike other emerging technologies in the UK, interviewees saw minimal market consolidation regarding IoT,[718] with actors including large technology firms (e.g. Google and Amazon), as well as "a very large number of new entrants that either are providing IoT solutions (IoT-based services) or were in the traditional product space and are now doing connected devices."[719] Interviewees recognised that these latter players are indicative of the omnipresence of IoT products across multiple markets and sectors, which has been a factor complicating UK regulatory efforts.[720] This is despite the fact that interviewees believed the UK to be relatively advanced in terms of IoT research and identification of security issues.[721]

Economic factors also influence IoT regulation in each country, with interviewees noting that Australia's "medium-sized economy" prevents it from mandating standards on commodities without having to pay a price premium, unless other countries do the same and cause a structural shift in the market.[722] Meanwhile, interviewees acknowledged that the UK has taken a traditional perspective of regulatory measures needing to be balanced with continued innovation and market growth, which has enabled security vulnerabilities to persist.[723] This helps explain a finding from the literature synthesis conducted in Chapter 2: a lack of IoT regulation and also illustrates why a large grey area exists in the UK for which IoT devices can create legal threats for journalists. In contrast, interviewees expressed that the US does not have a culture of active regulation of markets and the lack of IoT regulatory framework means that there is currently no consistent incentive for commercial entities to self-regulate.[724] This is similar to Taiwan, as Taiwan interviewees said that the issue of IoT regulation is predominantly seen by the government as necessary to ensure fair market competition, rather than to increase device security for the sake of consumer protection.[725]

[714] Interviewees: P55, P36; Australian Bureau of Statistics (2018) Household use of information technology, 2016-17 financial year. Available at: https://www.abs.gov.au/statistics/industry/technology-and-innovation/household-use-information-technology/latest-release (accessed 31 December 2020); Australian Bureau of Statistics (2018) Internet Activity, Australia, June 2018. Available at: https://www.abs.gov.au/statistics/industry/technology-and-innovation/internet-activity-australia/latest-release (accessed 31 December 2020).
[715] Interviewee: P55
[716] Interviewee: P36
[717] Interviewee: P36
[718] Interviewee: P20
[719] Interviewee: P20
[720] Interviewee: P20, P18, P41, P10, P2
[721] Interviewees: P20, P18
[722] Interviewee: P14
[723] Interviewee: P20
[724] Interviewees: P61, P17, P57, P32; Crawford D and Sherman J (2018) Gaps in United States federal government IoT security and privacy policies. *Journal of Cyber Policy* 3(2). Routledge: 187–200. DOI: 10.1080/23738871.2018.1514061.
[725] Interviewees: P25, P49

Given these challenges to imposing regulations, interviewees discussed how self-regulation within the IoT industry was the initial strategy for multiple countries. For example, interviewees mentioned the UK's Department for Digital, Culture, Media and Sport (DCMS) developed a proactive optional Code of Practice (CoP) in collaboration with industry, academia and the NCSC which has 13 points to guide manufacturers to implement security by design principles.[726] Inspired by this, recent IoT security regulation discussions in Australia have been led by the IoT Alliance Australia (IoTAA) industry body, modelled on the UK's voluntary CoP.[727]

P60, an expert in cyber security and democratic resilience in Australia, stated that the effects of this are intended to be felt in the future, rather than immediately,[728] and the similarity in policy has resulted in similar critiques (see below). As mentioned, the US has left regulation to each state, and P19, an expert in telecommunications regulation, also noted that a reliance on companies voluntarily complying with normative device standards is a common regulatory practice in Taiwan.[729] However, they recognised that the development of rules regarding device security and abuse would be difficult, given the length of time necessary to create rules and the pace at which the IoT market is progressing in Taiwan.[730]

US interviewees noted the quasi-regulatory role of civil society organisations such as the Global Network Initiative, Ranking Digital Rights (RDR) Corporate Accountability Index and Access Now in putting pressure on technology companies to design more secure products.[731] Also relating to self-regulation, P17, an expert in surveillance and Internet regulation, posited that consumers could successfully litigate against parties in the IoT supply chain, which could incentivise the industry to improve device security.[732]

Nonetheless, critiques of self-regulation of the IoT abounded: both UK and Australian interviewees contended that the presence of smaller commercial players that can undercut larger corporations means a lack of financial incentive to abide by a CoP,[733] leading to a low success rate at the implementation stage.[734] For this reason, P50, a former compliance officer and current researcher of consumer IoT device cyber security, argued that standards institutes such as the British Standards Institute are incorrect about standardisation mitigating harm more effectively than enforced regulation.[735] Research conducted to investigate interviewee responses and for Chapter 2, such as literature by Tanczer *et al*., also recognised that the UK's attempt at enticing IoT manufacturers to self-regulate was unlikely to adequately affect the expansion of users' attack surfaces that occurs as a result of IoT vulnerabilities.[736] Further, to address the lack of IoT market surveillance in the UK, Blythe *et al*. compared the UK's existing self-regulatory criteria to the security features of 270 consumer IoT devices, finding little user instruction on maintaining good

[726] Interviewees: P17, P20, P18, P50, P31; Department for Digital, Culture, Media & Sport (2018) Code of Practice for Consumer IoT Security. 14 October. London, UK: Department for Digital, Culture, Media & Sport. Available at: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security (accessed 1 January 2021).
[727] Interviewees: P30, P55, P48, P27, P14, P60, P3
[728] Interviewee: P60
[729] Interviewee: P19
[730] Interviewee: P19
[731] Interviewee: P47, P21
[732] Interviewee: P17
[733] Interviewees: P20, P50, P60, P48, P31
[734] Interviewees: P18, P20, P31, P50
[735] Interviewees: P31, P50
[736] Tanczer L, Brass I, Elsden M, et al. (2019) The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In: *Rewired: Cybersecurity Governance*. Hoboken, NJ: Social Science Research Network, pp. 37–56. Available at: https://papers.ssrn.com/abstract=3385548 (accessed 22 April 2021).

cyber hygiene, as well as no standardisation of the information available.[737] Their recommendations included government intervention to assure the baseline security of devices.

Interviewees mused that this may be why the UK government decided to make some of the points mandatory.[738] Following these interviews, a proposal released in April 2021 signalled the advent of The Product Security and Telecommunications Infrastructure (PSTI) Bill, which will force manufacturers to fulfil some fundamental criteria, to be verified by retailers.[739] These criteria include clearly informing consumers of the timeline for device security updates, a ban on universal default passwords and signposting a point of contact for the public to report vulnerabilities.[740] Comparing this new information to the points interviewees raised, it seems that while these changes would improve device security, there remain questions as to how retailers will be able to verify the length of time for which devices will continue to be updated.

Likewise, the US has also attempted regulation through legislation, as the Internet of Things Cybersecurity Improvement Act of 2020[741] compels the National Institute of Standards and Technology (NIST) to create "standards and guidelines" for IoT devices purchased and used by federal agencies, with mandatory compliance by federal contractors and enforcement by both the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). While it is significant that the IoT Cybersecurity Improvement Act signals the US government's recognition that IoT threats could undermine democratic systems, these new regulations solely provide incentive for IoT manufacturers and vendors for federal systems. However, states such as California and Oregon are following suit and have developed their own regulations for consumer IoT devices to be implemented from 2021.[742]

---

[737] Blythe JM, Sombatruang N and Johnson SD (2019) What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity* 5(1). DOI: 10.1093/cybsec/tyz005.

[738] Interviewees: P31, P50; NCC Group. UK government announces plans for new IoT security law. NCC Newsroom 2021; Department for Digital, Culture, Media & Sport, Warman MP M. Press release: New cyber security laws to protect smart devices amid pandemic sales surge. GOVUK 2021; Department for Digital, Culture, Media & Sport. Policy Paper: Government Response to the Call for Views on Consumer Connected Product Cyber Security Legislation. London: Department for Digital, Culture, Media & Sport, 2021.

[739] NCC Group (2021) UK government announces plans for new IoT security law. In: *NCC Newsroom*. Available at: https://newsroom.nccgroup.com/news/uk-government-announces-plans-for-new-iot-security-law-425797 (accessed 23 April 2021); Department for Digital, Culture, Media & Sport and Warman MP M (2021) Press release: New cyber security laws to protect smart devices amid pandemic sales surge. In: *GOV.UK*. Available at: https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge (accessed 19 May 2021); Department for Digital, Culture, Media & Sport (2021) *Policy Paper: Government response to the call for views on consumer connected product cyber security legislation*. 21 April. London: Department for Digital, Culture, Media & Sport. Available at: https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation (accessed 19 May 2021); Department for Digital, Culture, Media & Sport (2021) The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet. Available at: https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet (accessed 15 November 2022).

[740] NCC Group (2021) UK government announces plans for new IoT security law. In: *NCC Newsroom*. Available at: https://newsroom.nccgroup.com/news/uk-government-announces-plans-for-new-iot-security-law-425797 (accessed 23 April 2021).

[741] Kelly RL (2020) Text - H.R.1668 - 116th Congress (2019-2020): IoT Cybersecurity Improvement Act of 2020. Available at: https://www.congress.gov/bill/116th-congress/house-bill/1668/text (accessed 1 January 2021); Dullea E and Bowman B (2020) Privacy Attorneys | Internet of Things (IoT) Cybersecurity Improvement Act. Available at: https://www.bytebacklaw.com/2020/12/congress-passes-the-internet-of-things-iot-cybersecurity-improvement-act/ (accessed 1 January 2021).

[742] Stauss D, Bowman B and Rogers M (2019) Two New State IoT Laws Go into Effect on January 1. Available at: https://www.bytebacklaw.com/2019/10/two-new-state-iot-laws-go-into-effect-on-january-1/ (accessed 1 January 2021).

Alternatives to self-regulation like the CoP and strict laws that were mentioned by interviewees include regulation by proxy, such as the 2017 Australian suggestion of a labelling system for devices that would inform consumers about the level of inbuilt security in a device.[743] Interviewees recognised that this was intended to pressure both manufacturers (to guarantee certain security provisions to get a certain rating, e.g. a specified number of years of security updates) and consumers (who would be able to learn about and choose their devices more responsibly).[744] Similarly, in 2022, the Biden Administration began to roll out a labelling programme for consumer IoT devices that would rely on vetting by US government entities, and would align with the standards set by NIST and the European Union, to allow the labels to be meaningful overseas.[745] However, preceding this announcement, US interviewees had noted that regulation according to the level of risk presented by a device is difficult as the IoT is not "sector-specific" and device capabilities are not directly comparable.[746]

In contrast, two Australian interviewees argued that a rating is entirely transient as it would be invalidated by the discovery of a security vulnerability.[747] Both Australian interviewees and US cyber security experts interviewed in the media following the 2022 US announcement also noted that labelling devices could lead to manufacturers doing the bare minimum for their desired rating but not following through with other promises, including on-going patching. They argued that this would give consumers a false sense of security and make comparison of two devices unfair.[748] Instead, P14, who has 13 years of expertise in technology policy in Australia, posited that a risk assessment of the environments in which devices would be found and then increasing security depending on the outcome of the risk assessment could be a longer-term option.[749]

US interviewees often referred to strong encryption as important to enshrine in law because of the amount of data collected, stored, and trafficked by IoT devices,[750] indicating that IoT regulation cannot be entirely extricated from data protection and privacy laws and policies. They noted some prolific manufacturers that have a documented history of weak encryption of their IoT devices, such as Amazon's smart TV using an "outdated cryptographic library that potentially allows anybody to intercept traffic in the middle" or even not using encryption for IoT traffic.[751] Further, P32, who has over five years' experience with legal, political and technological press freedom issues, recognised that strong encryption might prevent adversaries from intercepting traffic in transit but that state agencies could potentially legally access endpoint devices, within which there may not be adequate internal protections.[752]

This is consistent with existing academic literature such as Mathews Hunt, who noted the lack of comprehensive privacy legislation in Australia, stymying effective regulation of the consumer IoT and

[743] Interviewees: P55, P27, P14; Sadler D (2017) Security ratings for IoT devices? In: *InnovationAus*. Available at: https://www.innovationaus.com/security-ratings-for-iot-devices/ (accessed 31 December 2020).
[744] Interviewees: P55, P27, P14
[745] The White House (2022) FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/ (accessed 12 October 2022).
[746] Interviewees: P6, P37
[747] Interviewees: P27, P14
[748] Interviewees: P27, P14; Smalley S (2022) White House to unveil ambitious cybersecurity labeling effort modeled after Energy Star. *CyberScoop*, 11 October. Available at: https://www.cyberscoop.com/white-house-to-unveil-internet-of-things-labeling/ (accessed 12 October 2022).
[749] Interviewee: P14
[750] Interviewees: P32, P6, P35
[751] Interviewee: P6
[752] Interviewee: P32, P34.

salient threats.[753] Sheikhmiri and Issa built on this finding by discussing the increasing commercial importance of Big Data as a potential incentive for businesses to use specific IoT devices to decrease their energy consumption, but also acknowledged that the associated privacy threats necessitate stronger protections - both technical and policy-derived.[754] Further, US interviewees noted that it is challenging to trust that data protection is effective regarding IoT devices and the information they collect because of the various parties in the custodial chain.[755]

Suggestions from interviewees for mitigating this problem included the creation of "data trusts" that allow individuals to control and monitor the use of their personal data.[756] However, P24, who has expertise in the law and policy implications of emerging technologies in the US, noted that privacy by design and data governance by design recommendations are "reliant on creating new data infrastructures." [757] P24 noted that these are still inaccessible to consumers because of the vast amounts of content generated.[758]

P32, who has over five years' experience with legal, political and technological press freedom issues, expressed frustration that "the law only comes in after something bad has happened," making it unlikely that effective IoT regulation will be designed and implemented until after a significant breach.[759] In the US, Section 230 of the Communications Decency Act (1996) effectively absolves technology companies of the consequences of their platform products.[760] While two Australian interviewees stated that there are rigorous physical fail safes for many IoT devices, they acknowledged that this is not true of all kinds of device and these product safety requirements do not necessarily prevent psychological threats such as targeted gaslighting.[761] P14, who has 13 years of expertise in technology policy in Australia, noted that Australia's International Cyber Policy Centre views consumer IoT threats as relating to both personal safety issues and also international espionage,[762] an issue that is relevant to highly targeted groups like the press. Therefore, combining findings from the interviews with existing academic literature, there is a clear need for IoT-specific risk assessments to address the expanded attack surface that results from increasing IoT prevalence, and the lack of security standards enshrined in law.[763] This provides a clear real-world gap to be filled by the contributions of this thesis.

6.3.3 Incompetent data protection

This subsection covers issues discussed by interviewees relating to incompetent data protection, such as post-access by governments, mandatory data retention and access laws, and inadequate data protection and privacy laws and regulations. When reviewing findings from the interviews against existing academic

[753] Mathews Hunt K (2018) consumeR-IOT: where every thing collides Promoting consumer internet of things protection in Australia. Faculty of Law. Bond University, Robina, Gold Coast, Queensland. Available at: https://research.bond.edu.au/en/studentTheses/consumer-iot-where-every-thing-collides-promoting-consumer-intern (accessed 23 April 2021).

[754] Sheikhmiri M and Issa T (2020) Awareness Factors, Opportunities and Challenges of Iot Application in Australia. In: Issa T, Issa Theodora, Issa TB, et al. (eds) Sustainability Awareness and Green Information Technologies. Green Energy and Technology. Cham: Springer International Publishing, pp. 271–320. DOI: 10.1007/978-3-030-47975-6_12.

[755] Interviewees: P8, P32, P24

[756] Interviewee: P24

[757] Interviewee: P24

[758] Interviewee: P24

[759] Interviewee: P32

[760] Besen SM and Verveer PL (2021) Section 230 and the Problem of Social Cost. Journal of Law and Policy 30: 68.

[761] Interviewees: P27, P3

[762] Interviewee: P14

[763] Nurse JRC, Creese S, De Roure D. Security Risk Assessment in Internet of Things Systems. IT Professional 2017;19:20–6; Wachter S (2018) The GDPR and the Internet of Things: a three-step transparency model. Law, Innovation and Technology 10(2). Routledge: 266–294. DOI: 10.1080/17579961.2018.1527479.

literature, it is clear that these problems compound those discussed in the previous subsection because data protection and privacy have an impact on the regulation of the design and maintenance of IoT devices and data collection and storage features. This results in decreased security of data and devices and so increased risk to journalists from the IoT.

For example, interviewees noted that the UK and US have established legal exemptions for journalists' data, but recent history demonstrates an erosion of existing journalistic legal protections.[764] They also acknowledged that this could be dangerous for source identification if rich IoT bulk datasets are made accessible to state agencies without adequate filtering to remove relevant results. In contrast, interviewees noted that Australia's protections are "implied,"[765] while Taiwan's lack of governmental interference in both the media and technology industries has left journalists vulnerable to expansions in the IoT market, although interviewees said this might be affected by the Personal Data Protection Act (2015).[766] This subsection will first discuss the different kinds of gaps in data protection legislation and the risks they create as recognised by interviewees, before noting some positive steps to improved legislation that interviewees noted, before discussing their thoughts on how government legislation is perceived in relation to criminal activity.

Interviewees felt there is a clear need for more relevant and stringent data protection legislation, as existing laws across the countries are not sufficient to prevent breaches and data leakage through effective enforcement of consequences. One cause that interviewees pointed to in order to explain ineffective legislation are instances where laws have not been kept updated. For example, P30, a law and cyber security expert on the UK and Australia, noted that amendments made to the Australian federal Privacy Act in 2000 were modelled on the 1995 EU Data Protection Directive.[767] P30 also noted that it is superseded by legislative frameworks relating to the management of Commonwealth records so that it has exemptions for government data use.[768] They further mentioned that Australia's Privacy Act sets out National Privacy Principles that apply to corporations with an annual turnover of over $3 million (AUS),[769] which leaves all other bodies to be governed only by state laws, if these exist. Similarly, although the US Federal Trade Commission supervises and enforces consumers' privacy interests, effectively punishing some IoT companies for their lapses in security,[770] the US does not have a federal law comprehensively addressing data breach response. However, unlike in Australia, digital civil liberties expert P35 noted that in the US all states have adopted their own data breach notification legislation.[771]

Regarding privacy law, P33, an expert in regulation of the IoT with 16 years researching technological threats to the press in Australia, noted that Australia deviates from the pattern among most common law jurisdictions, including the UK and to a lesser extent the US, in that Australia has only had a small number of privacy-related cases and therefore lacks privacy protections.[772] P30, a law and cyber security expert on the UK and Australia, suggested this was why legislation has not been updated, despite the country's

[764] Interviewees: P26, P30, P55, P42, P27
[765] Interviewees: P30, P42
[766] Interviewees: P25, P49
[767] Interviewee: P30
[768] Interviewee: P30
[769] Interviewee: P30
[770] Banasiński C, Rojszczak M. Cybersecurity of consumer products against the background of the EU model of cyberspace protection. Journal of Cybersecurity 2021;7, DOI: 10.1093/cybsec/tyab011.
[771] Interviewee: P35
[772] Interviewee: P33; Victoria Park Racing & Recreation Grounds Co Ltd v Taylor [1937] HCA 45; (1937) 58 CLR 479 (26 August 1937)

reputation for research on the use of the IoT in intimate partner violence scenarios.[773] P27, who has 26 years of expertise in technological threats to the press in Australia, noted that in 2014, the Australian Law Review Council recommended the development of a common law tort of invasion of privacy, in contrast to the current purely statutory scheme which does not allow private legal action relating to breach of individual privacy, but this has not yet occurred.[774] Interviewees said that this left the opportunity for state-level courts to begin to develop protections, which may not be useful without effective mapping of existing laws.[775] P33 mentioned that, in 2019, the Australian Competition and Consumer Commission released a report that called for the Australian privacy framework, including the Privacy Act, to be revamped, but no progress has yet been made.[776] Interviewees' frustration with this lack of jurisprudential delineation of privacy suggests that it contributes to superficiality in discussions around IoT consumer rights and individuals' threat tolerance.

Another area of weakness in existing legislation that interviewees raised is unrealistic laws and regulations that do not work well in practice. For example, the 2018 California Consumer Privacy Act (CCPA) was noted by interviewees as being difficult both for companies to comply with and for consumers to understand and limited because of a lack of consistent enforcement.[777] Similarly, interviewees suggested that while the GDPR includes the right to data portability,[778] which means journalists should be able to access their personal data collected by a company in the IoT supply chain,[779] this aspect of GDPR is unrealistic due to the heterogeneity of the consumer IoT. They were concerned that, for example, two devices with the same label, e.g. both marketed as fitness trackers, might store their data so differently that effective collation or comparison of these datasets is unfeasible.[780] This, they expressed, is another barrier to journalists' understanding of IoT threats.[781] Literature corroborates such issues, such as Noto La Diega pointing out the difficulty of forcing IoT consumers to deal with challenges by wading through the "contractual quagmire" of overlapping legal documents pertaining to even one device, given the huge investment by UK decision-makers in IoT devices such as mandatory smart meters.[782] As is clear from Chapter 4's exploratory study, these consumers would necessarily include UK journalists and sources, complicating their efforts to minimise personal IoT risk.

Even within existing laws and protections, one further issue interviewees expressed concern about is the fact that governments either mandate access to or storage of data, but do not set a strong security baseline, thus leaving the data unprotected, including ill-defined metadata. For example, two interviewees noted that the Australian government is eager to collect data and metadata from any available sources but shirks responsibility for ensuring that it is safeguarded through effective governance

[773] Interviewee: P30

[774] Interviewee: P27; Australian Law Reform Commission (2014) A common law action for breach of privacy in Australia? Available at: https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/3-overview-of-current-law-2/a-common-law-action-for-breach-of-privacy-in-australia-2/ (accessed 31 December 2020).

[775] Interviewees: P28, P33

[776] Interviewee: P33

[777] Interviewee: P24

[778] Interviewees: P17, P30

[779] Interviewees: P31, P50

[780] Interviewee: P50; Turner Sarah, Galindo Quintero J, Turner Simon, et al. (2020) The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*. SAGE Publications: 1461444820934033. DOI: 10.1177/1461444820934033.

[781] Interviewee: P50; Turner Sarah, Galindo Quintero J, Turner Simon, et al. (2020) The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*. SAGE Publications: 1461444820934033. DOI: 10.1177/1461444820934033.

[782] Noto La Diega G (2016) Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom. *Journal of Law & Economic Regulation* 9(1): 69–93.

standards.[783] They expressed that this can be seen through a record of data breaches and leaks, including some state agencies illegally obtaining access to journalists' metadata.[784] They felt this could be in part due to a lack of governmental understanding of the threats and vulnerabilities, or indeed what metadata reveals,[785] as well as due to wilful negligence regarding accountability through policy or enforcement.[786] UK interviewees likewise discussed the fact that metadata is less stringently protected, for example by the Data Protection Act (2018).[787] They felt that this is problematic for journalists, as lawmakers did not take into account the vast amounts of metadata generated by the IoT.[788]

Still, there are a few positive notes regarding existing laws and protections that were recognised by interviewees. They named two prominent US state-level laws as being relevant to regulating the consumer IoT: CCPA and BIPA.[789] CCPA was mentioned as a positive step in terms of data protection mechanisms as it brings the US closer to the kind of regulation implemented internationally, such as the GDPR.[790] Interviewees acknowledged that a patchwork of other US laws are emerging that emphasise the importance of consumers' data protection and privacy, but they are applied on the basis of location, industry and size of data controller, which complicates compliance and enforcement.[791] In the UK, interviewees knew that the GDPR and the Data Protection Act (2018) (DPA) regulate data collection, transfer and storage,[792] which has ostensibly required companies developing and manufacturing IoT devices for sale in the UK to ensure compliance and thereby include a modicum of data protection and therefore also privacy by design.[793]

However, although there is currently no overarching US federal data protection law, the American Data Privacy and Protection Act (2022) was proposed after the interviews ended and garnered bipartisan support for its proposal to minimise data collection and transfer to third parties.[794] Also after interviews concluded, a 2021 UK ruling determined that surveillance technology (including a Ring doorbell) invaded the privacy of a neighbouring property, which resulted in potential personal damages of up to £100,000.[795]

---

[783] Interviewees: P42, P55, P33

[784] Interviewees: P33, P36; Karp P and Taylor J (2019) Police made illegal metadata searches and obtained invalid warrants targeting journalists. Available at: http://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists (accessed 31 December 2020); Communications Alliance (2020) *Government Must Support Security Committee Recommendations And Repair The Data Retention Regime*. 2020 Media Release 31, 29 October. Sydney, Australia: Communications Alliance. Available at: https://www.commsalliance.com.au/Documents/releases/2020-media-release-31 (accessed 31 December 2020).

[785] Casanovas P, De Koker L, Mendelson D, et al. (2017) Regulation of Big Data: Perspectives on strategy, policy, law and privacy. *Health and Technology* 7(4): 335–349. DOI: 10.1007/s12553-017-0190-6.

[786] Interviewees: P28, P33, P52, P55; Taylor J (2020) Melbourne professor quits after health department pressures her over data breach. Available at: http://www.theguardian.com/australia-news/2020/mar/08/melbourne-professor-quits-after-health-department-pressures-her-over-data-breach (accessed 31 December 2020).

[787] Interviewees: P17, P30

[788] Interviewees: P45, P4

[789] Interviewees: P24, P35, P13, P21, P37, P51

[790] Interviewees: P24, P35, P13, P21, P37

[791] Harrington D (2022) U.S. Privacy Laws: The Complete Guide. Available at: https://www.varonis.com/blog/us-privacy-laws (accessed 15 November 2022).

[792] Interviewees: P17, P30

[793] Ismail N (2017) IoT boom and GDPR raise the stakes of a cyber security breach. In: Information Age. Available at: https://www.information-age.com/iot-gdpr-raise-stakes-cyber-security-breach-123464318/ (accessed 1 January 2021).

[794] Pallone F, McMorris Rodgers C and Wicker R (2022) American Data Privacy and Protection Act. H.R. 8152. Available at: https://www.commerce.senate.gov/services/files/6CB3B500-3DB4-4FCC-BB15-9E6A52738B6C (accessed 15 November 2022).

[795] Charlesworth A (2021) Smart doorbells: how to use them without infringing a neighbour's privacy. Available at: http://theconversation.com/smart-doorbells-how-to-use-them-without-infringing-a-neighbours-privacy-170180 (accessed 9 November 2021).

However, some literature read for Chapter 2 and to supplement these interviews illustrated the importance of consequences for breaches due to poor security, such as the perceptions of Banasiński and Rojszczak that US laws and bodies on consumer protections are more effective than those in the EU.[796] Expanding on this ranking of legislative domains, the UK's adoption of the DPA was seen by interviewees as a more effective regulatory tool than Australia's federal 'Privacy Act' (1988), the latter which was criticised by interviewees as being counterintuitively related to data protection rather than privacy and also being limited in scope and strength.[797]

6.3.4 Cyber-physical criminal threats exacerbated by insufficient IoT regulation

A further threat recognised by interviewees as resulting from domestic government inadequacy regarding protection of data and regulation of devices is the possibility of criminal activity. This subsection will first discuss their perceptions of IoT threats as covert and unknowable. It will then discuss different cyber-physical threats named by interviewees. Finally, it will note some limited examples of such threats being taken seriously, given by interviewees.

Interviewees across the studied countries differed in opinion in terms of whether they most feared legal government overreach or illegal access to their data, although they agreed that their own governments were unlikely to be perpetrators of cyber-physical attacks.[798] On this, P25, a Taiwanese lawyer with expertise in information technology, communications and telecoms, and technology law and policy, intimated a generational divide in Taiwan: older generations are afraid of what the government will do with data collected, while the younger generation is afraid of what other adversaries will do if the government cannot protect the data that they retain.[799] This may be because of the memories of martial law held by the older generation, which P25 and P63, an investigative reporter, felt may have influenced the Taiwanese public to be more tolerant of commercial data collection as opposed to government power concentration.[800] Comparatively, P58, who works for a Taiwanese public news broadcaster, and P63 stated that societal worry regarding government intrusion has increased since 2018, but the public is divided less along generational lines than into groups such as those who prioritise IoT-enabled domestic convenience versus those with privacy considerations, as is the case in Australia.[801]

Further, one US interviewee acknowledged that the former general counsel of the Federal Bureau of Investigation (FBI) is now an advocate for strong encryption on the basis that weak commercial encryption benefits criminals more than any other party.[802] US interviewees hoped that raising awareness of the types and quantities of data collected by the IoT would be sufficient to make government legal and policy responses more comprehensive.[803] UK interviewees noted that, for journalists to trust the safeguards in place through the IPT, they must rely on both judicial understanding of emerging technologies, ignoring the historic lack of technical knowledge, and on technical experts from the IPCO being sufficiently

[796] Banasiński C and Rojszczak M (2021) Cybersecurity of consumer products against the background of the EU model of cyberspace protection. *Journal of Cybersecurity* 7(tyab011). DOI: 10.1093/cybsec/tyab011.
[797] Interviewees: P30, P33
[798] Interviewee: P14
[799] Interviewee: P25
[800] Interviewees: P25, P63, P39
[801] Interviewees: P58, P63
[802] Interviewee: P48; Baker J (2019) Rethinking Encryption. Lawfare, 22 October. Available at: https://www.lawfareblog.com/rethinking-encryption (accessed 1 January 2021).
[803] Interviewee: P17

committed to press protections.[804] All these considerations influenced the protections and mitigations detailed in Chapter 8's framework of IoT threat countermeasures.

The predominant reason for concern regarding IoT risk to journalists given by interviewees was the clandestine nature of exploitation of the devices' many vulnerabilities and the prevalence of ambient devices such as voice assistants, which leads to a widespread lack of awareness of whether attacks have occurred or are even possible.[805] US and Australian interviewees argued that as a result, very few consumer IoT threats that come to fruition are reported, either in the media or to the authorities, despite the ease with which some attacks can be carried out, which has contributed to the societal sense that IoT-related threats are "black swan events."[806]

P6, an expert in IoT security and privacy in the US, suggested that the popular uptake of consumer IoT devices in the US has occurred in spite of a common lack of comprehension regarding how the devices function, what data they collect or with whom they communicate, due to a lack of specialist technical knowledge required to investigate these behaviours.[807] P6 recognised that there are some open-source tools available to parse this information and make it accessible to the public, such as 'IoT Inspector,'[808] which has been used by journalists at NPR and the Washington Post. However, overall, US interviewees felt that while the market for IoT devices is expanding, security knowledge amongst consumers is still inchoate,[809] and two Australia interviewees noted even highly aware members of the public are unlikely to be able to identify the passive surveillance capabilities of IoT devices in public spaces. They posited that this makes regulation and education much harder and could even lead to gaslighting[810] because of the difficulty of forensics.[811]

On a national level, in 2022, after interviews had concluded, the UK's National Cyber Security Centre began scanning all UK-based internet-connected devices for vulnerabilities, to prompt remediation and also log identifiers for devices that might become part of a widespread cyber-attack on the country.[812] While this could limit the number of targets for an attacker, and thus the scale of damage, the fact that this scanning scheme requires individuals to opt out by emailing the NCSC with a list of IP addresses that they do not want to be scanned may prevent less technologically-savvy journalists and sources from refusing to participate, and could contribute to a feeling of being constant surveilled. A 2022 report by Daly *et al.* found that their journalist interviewees were aware of the potential of technological surveillance, but that "they were not always aware if they had actually been under that surveillance."[813] Situating this finding within the context of the thesis more broadly, this uncertainty is exacerbated by the number and variety

[804] Interviewee: P4
[805] Interviewees: P34, P35, P9, P37, P17, P23, P8, P55, P52, P5, P39, P29, P58, P22, P12, P25
[806] Interviewees: P34, P35, P36, P9, P37, P17, P23, P8
[807] Interviewee: P6
[808] Huang DY, Apthorpe N, Li F, et al. (2020) IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 4(2): 1–21. DOI: 10.1145/3397333.
[809] Interviewee: P6
[810] Abramson K (2014) TURNING UP THE LIGHTS ON GASLIGHTING. *Philosophical Perspectives* 28. [Ridgeview Publishing Company, Wiley]: 1–30.
[811] Interviewees: P55, P52
[812] Levy I (2022) Scanning the internet for fun and profit. Available at: https://www.ncsc.gov.uk/blog-post/scanning-the-internet-for-fun-and-profit (accessed 15 November 2022); National Cyber Security Centre (NCSC) (2022) NCSC Scanning information. Available at: https://www.ncsc.gov.uk/information/ncsc-scanning-information (accessed 15 November 2022).
[813] Daly A, Robinson E and McMenemy D (2022) Cyber security, surveillance and journalism in Scotland. Science, Policy and Law Series 1, Leverhulme Research Centre for Forensic Science, 27 September. Dundee, Scotland: University of Dundee. Available at: https://discovery.dundee.ac.uk/ws/files/81462869/CyberSecurity_DigitalReport_1.0.pdf.

of ways in which the IoT can collect data (see: Chapter 5). Further, Mills and Sarikakis discussed self-censorship as a well-documented "chilling effect" consequence of laws enabling surveillance and the consequences of reporting against the interests of influential decision makers.[814]

Similarly, multiple Taiwan interviewees also disclosed a lack of awareness of IoT threats either among the press or in society.[815] P39, an academic specialising in Asia, noted that there was very little discussion of the security issues of consumer IoT devices on the popular online forum "Bulletin Board PTT", where people air their scepticism about goods and services.[816] With respect to smart doorbells specifically, P39 mentioned that a series of historical murders in Taiwan had caused a "moral panic" that led to many households putting bars on their windows, so IoT doorbells may have mass appeal if they enter the Taiwanese markets.[817] P5, who has 25 years of experience working on press freedom in Taiwan, also suggested that there is a cultural propensity in Taiwan to overlook technological security concerns unless a user is likely to be specifically targeted by China.[818]

Despite this lack of societal awareness, interviewees explicitly recognised multiple different kinds of cyber-physical threats from the IoT to journalists. Many of these have been discussed in Chapter 5, in the models presented assessing and conceptualising IoT risk to journalists. A few examples are detailed here, specifically those notable for being shared across countries. One threat model that was named as possibly used to target individuals was remote hacking of internet-connected cars. For example, investigative reporter P63 noted the popularity of the company Tesla among the Taiwanese public,[819] and recalled a 2020 incident in which a Tesla car in autopilot mode crashed into another vehicle,[820] while US interviewees mentioned the provision of erroneous information by a GPS device to lead a journalist astray[821] and the abuse of location sensors.[822] Another IoT threat to journalists and news organisations that was named is the creation and use of botnet armies,[823] as there are legal issues with takedown considering jurisdictional restrictions and bulletproof hosting.[824] P40, an investigative journalist with eight years of experience, including working on multiple international collaborative investigations, acknowledged that the Australian Signals Directorate had released a manual on device hardening,[825] but this does not cover novel IoT devices.[826]

---

[814] Mills A and Sarikakis K (2016) Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism. Big Data & Society 3(2): 2053951716669381. DOI: 10.1177/2053951716669381.
[815] Interviewees: P5, P39, P29, P58, P22, P12, P25
[816] Interviewee: P39
[817] Interviewee: P39
[818] Interviewee: P5
[819] CommonWealth Magazine (2020) Taiwan's Tesla Boom, and Looking for More. Available at: https://topics.amcham.com.tw/2020/10/taiwan-tesla-boom/ (accessed 31 December 2020).
[820] Interviewee: P63; Templeton B (2020) Tesla In Taiwan Crashes Directly Into Overturned Truck, Ignores Pedestrian, With Autopilot On. Available at: https://www.forbes.com/sites/bradtempleton/2020/06/02/tesla-in-taiwan-crashes-directly-into-overturned-truck-ignores-pedestrian-with-autopilot-on/ (accessed 31 December 2020).
[821] Interviewee: P37
[822] Interviewee: P6
[823] Interviewees: P14, P48, P6
[824] Interviewee: P48
[825] Interviewee: P40
[826] Australian Cyber Security Centre and Australian Signals Directorate (2020) *Australian Government Information Security Manual (October 2020)*. October. Australia: Australian Signals Directorate. Available at: https://www.cyber.gov.au/sites/default/files/2020-10/Australian%20Government%20Information%20Security%20Manual%20%28October%202020%29.pdf (accessed 31 December 2020).

However, interviewees acknowledged evidence that some actors are aware of the dangers presented by the consumer IoT and are taking these issues seriously. Hopeful initiatives include a new Australian Federal Police forensics hub with the expertise and capabilities to analyse potentially compromised IoT devices.[827] As discussed in Chapter 2, Australia has a research niche looking at IoT threats in domestic violence situations, which may be what this hub is primarily focusing on, although some threat models for these two communities overlap.[828] Further, the Australian Office of the eSafety Commissioner is now responsible for collating information on the realities of these threats,[829] which could alleviate the pervasive lack of knowledge about what is possible and what is happening. Additionally, P36, an expert in Australia's national cyber security strategy, noted that the 2016 national cyber security strategy has created the post of Ambassador for Cyber Affairs, enabling a more coordinated global projection of Australia's cyber security capabilities.[830] Relatedly, in the US, there have been class action lawsuits filed relating to poorly secured IoT baby monitors[831] and high-profile botnets that included IoT devices (such as Mirai),[832] suggesting that the public are starting to become more aware of IoT threats in general.

6.4 Conclusion

This chapter compared and contrasted the legal and policy challenges that increase IoT risk to the media industries and to journalists in Taiwan, Australia, the UK, and the US. Across the countries examined, interviewees were clear that there is a clear dearth of IoT-specific policy and legislation that effectively regulates the security or privacy provisions of the consumer IoT or addresses the potential for serious threats enacted through adversarial use of these devices.[833] This is primarily because of the recent and rapid development of the consumer IoT market, its fragmentation and poor privacy and security by design, and particularly the massive amounts of data collected by heterogeneous devices.[834] Interviewees expressed that this last factor is exacerbated by the high value placed upon intelligence by national governments, and a post-9/11 surveillance culture, which signal growing authoritarian tendencies even in democratic states and contribute to attacks on freedom of the press globally.[835]

This chapter therefore demonstrates that there is not just more risk to manage on an individual, organisational and industry level because of poor IoT regulation nationally, but also that it is harder for

[827] Interviewee: P60; Australian Federal Police (2016) What We Do: Operational Support: Forensics. Available at: https://www.afp.gov.au/what-we-do/operational-support/forensics (accessed 31 December 2020).
[828] Interviewees: P48, P3, P30
[829] eSafety Commissioner (2020) eSafety Commissioner. Available at: https://www.esafety.gov.au/homepage (accessed 31 December 2020).
[830] Interviewee: P36
[831] Interviewees: P35, P24; Castillo R (2011) Jamison v. Summer Infant (Usa), Inc., 778 F. Supp. 2d 900. No. 09 C 7513-778 F. Supp. 2d 900 (N.D. Ill. 2011) 74 U.C.C. Rep. Serv. 2d 408. Available at: https://casetext.com/case/jamison-v-summer-infant-usa (accessed 1 January 2021).
[832] Interviewee: P6
[833] DeNardis L and Raymond M (2017) The Internet of Things as a Global Policy Frontier. UC Davis Law Review 51(2): 23; Sicker DC (2019) The Breadth of Policy and Regulatory Issues Facing IoT. IEEE Internet of Things Magazine 2(1): 4–5. DOI: 10.1109/MIOT.2019.8835416.
[834] Tusikov N (2019) Precarious Ownership of the Internet of Things in the Age of Data. In: Haggart B, Henne K, and Tusikov N (eds) Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century. International Political Economy Series. Cham: Springer International Publishing, pp. 121–148. DOI: 10.1007/978-3-030-14540-8_6.
[835] Reporters without borders (2019) Only nine percent of humankind lives in a country where press freedom is good. Available at: https://rsf.org/en/news/only-nine-percent-humankind-lives-country-where-press-freedom-good (accessed 1 January 2021); Reporters Without Borders (RSF) (2017) #SPOILERSFORFREEDOM: Exiled journalists warn democracies about decline in media freedom. Available at: https://rsf.org/en/news/spoilersforfreedom-exiled-journalists-warn-democracies-about-decline-media-freedom (accessed 1 January 2021).

the media to manage this risk because of other priorities that limit their resources. These domestic factors are exacerbated by geopolitical concerns and combine to create challenging gaps in existing protection and mitigation methods used by journalists, all of which will be discussed in Chapter 7.

Chapter 7: Additional IoT risks perceived by interviewees: Geopolitical and Organisational Considerations

7.1 Introduction

This chapter aims to understand the extent of IoT risk journalists face from geopolitical and organisational factors, and the extent to which they are able to combat these risks. Specifically, it utilises unique qualitative data to compare and contrast journalistic experiences in these two thematic areas in Taiwan, Australia, the United Kingdom, and the United States. The methodology underpinning this chapter including methods of country selection, interviewee selection criteria, recruitment methods, interview procedures, and thematic analysis can be found in Chapter 3 (sections 3.2.4.2, 3.3, and 3.5.1.1). Details about the presentation of this chapter as an integrated findings and discussion focused chapter,[836] and how these two chapters relate to Chapter 5's findings can also be found in the introduction of Chapter 6.

This chapter builds on the contributions of the previous chapter and contributes to this thesis's overall research question by understanding the geopolitical context of each case study country to help clarify which aspects of IoT risks are beyond the scope for mitigation attempts by journalists and media organisations. Additionally, this chapter determines which existing methods are being used for protection in order to improve the recommendations for journalists and the media, to finish addressing the research question with Chapters 8 and 9. As with Chapter 6, this chapter is organised thematically, categorising the responses of 63 interviewees and their perceptions of threats posed by the IoT to journalists into overarching themes and corroborating them using up-to-date literature. Chapter 6 focused on the most prevalently reported themes: legal threats; this chapter presents geopolitical challenges and organisational gaps that while less feared than legal threats, were nevertheless consistently reported by interviewees across the four case study countries.

By assessing journalists' knowledge and behaviours regarding perceived IoT threats, this chapter's objective is to establish the implications of the consumer IoT for journalists in each country, and particularly the elements that maximise IoT risk for the media. This bridges the gap between the IoT's theoretical capabilities and associated threats (see: Chapter 5) and the legal challenges that exist for journalists in practice (see: Chapter 6). This information about gaps in current media security knowledge and practices enables Chapter 8's framework to fill in the stated user needs. This enhances the feasibility of implementation and increases opportunities for this thesis to have real-world impact.

Additionally, this chapter highlights the importance of formal media threat intelligence sharing mechanisms, which may enhance the roles of news organisations' executives, security teams and lawyers.

[836] Hesse-Biber, SN, & Johnson, RB (eds) 2015, The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry, Oxford University Press, Incorporated, Oxford. Available from: ProQuest Ebook Central: pp. 84, 198-200; Seidman I (2006) Interpreting The Material. In: *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. Third. New York: Teachers College Press, Columbia University, pp. 128–131; Hancock B, Ockleford E and Windridge K (2009) *An Introduction to Qualitative Research: Presenting Qualitative Research*. UK: The NIHR Research Design Service for Yorkshire & the Humber. Available at: https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/5_Introduction-to-qualitative-research-2009.pdf (accessed 21 December 2022); Erlingsson C and Brysiewicz P (2017) A hands-on guide to doing content analysis. *African Journal of Emergency Medicine* 7(3): 93–99. DOI: 10.1016/j.afjem.2017.08.001; Braun V and Clarke V (2013) Successful Qualitative Research: A Practical Guide for Beginners. London, UK: SAGE Publications Ltd; Yin RK (2009) *Case Study Research: Design and Methods*. Fourth. Applied Social Research Methods Series. California, USA: SAGE Publications, Inc; Hartley J (2004) Case Study Research. In: Cassell C and Symon G (eds) *Essential Guide to Qualitative Methods in Organizational Research*. London: SAGE Publications Ltd., pp. 323–333. DOI: 10.4135/9781446280119; Eisenhardt KM (1989) Building Theories from Case Study Research. *The Academy of Management Review* 14(4). Academy of Management: 532–550. DOI: 10.2307/258557.

Interviewees discussed the necessity of newsroom security to coordinate protections against a number of contemporary threats, as well as the need to lobby for policy changes that could mitigate emerging threats. Finally, journalists themselves may find these chapters relevant as they present a holistic view of the myriad strategic and tactical considerations that affect their ability to protect their work, wellbeing and sources from threats associated with the consumer IoT.

This chapter will therefore first detail geopolitical risk factors, including supply chain concerns. It will then document the status of existing protections and mitigations for journalists, focusing on risk assessments and training, as well as whether and how media organisations and journalists share threat intelligence.

7.2 Theme 3: Geopolitical risk factors

Geopolitical risk was a major theme of interviewees' responses regarding the significance of IoT threats to the media in each country. This section will thus first discuss interviewees' thoughts on how the threat from China manifests in each country, then interviewees' concerns about Chinese information warfare using IoT devices in Taiwan, then Taiwan's shifting economic ties to China. It will follow those topics with interviewees' descriptions of Taiwan's increasing alliances with other countries to limit the influence of China, juxtaposed with their perceptions of Taiwan's push for smart cities and Big Data, then their fears of supply chain threats from China. The section will then explore other, more general supply chain considerations that interviewees recognised, but that are not specific to China. After that, it will discuss interviewees' worries about the impact of convoluted supply chains on IoT regulation, and finally, their thoughts on supply chain localisation attempts.

Specifically, interviewees' perceived threats to press freedom and threats through IoT devices from China in all four countries, which is corroborated by Reporters Without Borders.[837] However, interviewee responses made it clear that the countries differ in their relationship with China and thus in the extent to which they feared Chinese IoT threats. For example, Taiwan is a major flashpoint for China, and is "strategically important" to the US,[838] which views China as the other side in an international technological competition that "replaced the Cold War".[839] Notwithstanding Taiwan's unique concerns, interviewees perceived Australia as caught between the West and Chinese spheres of influence, which contributes to its decision to align its security policies with the UK and US and perhaps Australia's decision to base its IoT regulatory regime on the UK's, to ensure the West's long-standing support without compromising the country's necessary trading partnership with China.[840]

In addition to direct ways in which laws, or a lack thereof, create risks for journalists and press freedom via the IoT, interviewees acknowledged additional contextual factors that inhibit the media as a sector from best protecting itself. These are not specific to the IoT but are wider challenges interviewees stated

[837] Reporters Without Borders (2019) RSF Report: 'China's Pursuit of a New World Media Order' | Reporters without borders. Available at: https://rsf.org/en/reports/rsf-report-chinas-pursuit-new-world-media-order (accessed 9 November 2021).
[838] Interviewee: P39
[839] Interviewee: P61
[840] Hurst (2020) UK and US lock in behind Australia in China row. Available at: http://www.theguardian.com/australia-news/2020/dec/02/uk-and-us-lock-in-behind-australia-in-china-row (accessed 1 January 2021); Layton P (2017) As China's Sphere of Influence Expands, Australia Has a Choice. In: War on the Rocks. Available at: https://warontherocks.com/2017/06/as-chinas-sphere-of-influence-expands-australia-has-a-choice/ (accessed 1 January 2021); White H (2005) The limits to optimism: Australia and the rise of China. Australian Journal of International Affairs 59(4). Routledge: 469–480. DOI: 10.1080/10357710500367273; Weber V (2020) Strategic Update: Making Sense of Technological Spheres of Influence. LSE IDEAS, April. London, UK: London School of Economics. Available at: http://eprints.lse.ac.uk/107791/1/LSE_IDEAS_Technological_Spheres_of_Influence_April_2020.pdf (accessed 1 January 2021).

the media faces that impede journalistic work. In particular, interviewees saw Taiwan's situation as notable because the lack of enforced regulation stems from a reluctance of political and legislative decision-makers to intervene in issues relating to the press due to Taiwan's history of authoritarianism and juxtaposition with Chinese oppression of journalists.[841] Given Taiwan's history as an authoritarian country (martial law only lifted in 1989), and the resultant societal taboo of government interference in press activities, interviewees argued that media outlets have developed polarised political positions that align with either one of the two political parties.[842] They also recognised that this has led to calls for media literacy programmes that educate the public about disinformation and propaganda and greater legal protection of the editorial independence of journalists, to avoid conflicts of interest with media owners who are, for example, pro-China.[843]

One area in which China concerns interviewees regarding IoT threats to the Taiwanese media is through information warfare. Combining findings from the interviews with existing academic literature, it is clear that this could result from military invasion, and is likely to be occurring already as part of existing action against Taiwan. Interviewees suggested that the consumer IoT has not yet fully penetrated Taiwanese society, nor is it recognised by journalists as a tangible threat vector. However, they said that the threat of asymmetric warfare tactics employed against Taiwan's Internet and electrical infrastructure by China has been considered during hackathons[844] and possibly during the 2019 cyber war game held with the US.[845]

Even without escalations in military action, P63, an investigative journalist, discussed the Chinese Advanced Persistent Threat, including frequent DDoS attacks against Taiwanese institutions and coordinated disinformation attacks constituting an "information war" that undermined public trust in the media.[846] P5, who has 25 years of experience working on press freedom in Taiwan, speculated that device backdoors could be activated to spread disinformation further in the event of a military attack: "If China attacked Taiwan, they could hack journalists' devices and make them release statements on social media or false articles to simultaneously tell the public that China has won."[847]

Another area in which interviewees recognised that China threatens the Taiwanese press is through economic interaction, including via investment. According to P38 and P29, both foreign correspondents in Taiwan, part of the motivation for Taiwan's 2020 Anti-infiltration Act was concern over the political influence "seeping into the Taiwanese media" through Chinese business connections and Chinese government bodies that operate in Taiwan.[848] Relevant literature suggests that information politics and journalistic transparency are central to Taiwan's image overseas and at home,[849] and corroborates a

[841] Interviewees: P5, P39, P22, P58
[842] Interviewee: P5
[843] Interviewees: P5, P39, P58
[844] Woodhouse A (2015) Taiwan launches hackathon to help make itself an impregnable fortress against cyber criminals from China as attacks proliferate. Available at: https://www.scmp.com/tech/apps-gaming/article/1861116/taiwan-launches-hackathon-help-make-itself-impregnable-fortress (accessed 31 December 2020).
[845] Interviewee: P29; Hille K (2019) US and Taiwan host security exercise to boost cyber defence. Financial Times, 4 November. Available at: https://www.ft.com/content/7d6c78cc-fec8-11e9-b7bc-f3fa4e77dd47 (accessed 31 December 2020).
[846] Interviewee: P63
[847] Interviewee: P5
[848] Interviewees: P38, P29; Lee Y (2019) Taiwan has 'urgent' need for infiltration law in face of China - president. *Reuters*, 27 December. Available at: https://uk.reuters.com/article/uk-taiwan-election-idUKKBN1YV141 (accessed 31 December 2020).
[849] Brysk A (2020) Constructing rights in Taiwan: the feminist factor, democratization, and the quest for global citizenship. *The Pacific Review* 0(0). Routledge: 1–33. DOI: 10.1080/09512748.2020.1784985.

historically negative correlation between Taiwan's press freedom and economic ties to China.[850] For example, Huang has argued that there is a danger of closer commercial relations with China affecting Taiwan's own relationship with its press, as the former is openly hostile to journalists, and there is a risk of economic influence spilling into the political and social spheres. This view of Taiwan's economic interactions with China within the China-dominated geopolitical status quo as being dangerous was shared by Magcamit, who said this has decreased Taiwanese autonomy generally.[851] P58, who works for a public news broadcaster, stated that Taiwanese businesses continue to collaborate with Chinese IoT companies, from manufacturers to vendors such as Alibaba and Taobao, both to promote products and boost sales.[852]

Similarly, the greatest perceived threat by interviewees to Taiwanese press freedom was Chinese state-affiliated ownership of news outlets in Taiwan, which erodes public trust in both the media and democratic systems more broadly.[853] For example, multiple interviewees named the controversial Want media group, which came under scrutiny during the 2019 presidential campaign for purveying pro-Chinese propaganda through its various news outlets.[854] They noted that this is indicative of a trend of large entertainment corporations merging with or absorbing media outlets and financially outcompeting independent news organisations and public broadcasters.[855] They also felt that a dearth of funding keeps public broadcasters from being able to rival private media, both in terms of advertising power and because it prevents public news organisations from competing in the Chinese language news market.[856] This kind of systemic threat explains why Chapter 8 presents legislative actions as potential threat mitigations, although political legacies, such as in Taiwan, can present barriers to this recommendation.

Interviewees for all four countries expressed particular concerns about the Chinese Cybersecurity Law (2017),[857] which requires telecoms operators in China to provide the Chinese authorities with full access to data collected in the interest of national security.[858] P25, a Taiwanese lawyer with expertise in information technology, communications and telecoms, and technology law and policy, disclosed that legal clients require advice on which products are manufactured by Chinese companies. They said this is because the Taiwanese government bans the use of certain products in critical infrastructure due to the likelihood that data will be transmitted to China.[859] Similarly, a 2023 report advising the UK government

[850] Huang J-N (2016) *Liberalization, Economic Dependence, and the Paradox of Taiwan's Press Freedom*. UC Riverside, California, USA. Available at: https://escholarship.org/uc/item/3j53d4r1 (accessed 23 April 2021).
[851] Magcamit MI and Tan AC (2015) Crouching tiger, lurking dragon: understanding Taiwan's sovereignty and trade linkages in the twenty-first century. *International Relations of the Asia-Pacific* 15(1): 81–112. DOI: 10.1093/irap/lcu013; Magcamit MI (2015) Games, Changes and Fears: Exploring Taiwan's Cross-Strait Dilemma in the Twenty-first Century. *Journal of Asian Security and International Affairs* 2(1). SAGE Publications India: 92–115. DOI: 10.1177/2347797014565297.
[852] Interviewee: P58
[853] Interviewee: P5
[854] Interviewees: P5, P38, P39, P63; Aspinwall N (2019) Taiwan Shaken by Concerns Over Chinese Influence in Media, Press Freedom. Available at: https://thediplomat.com/2019/07/taiwan-shaken-by-concerns-over-chinese-influence-in-media-press-freedom/ (accessed 31 December 2020); Kurlantzick J (2019) *In Brief: How China Is Interfering in Taiwan's Election*. 7 November. New York, NY, USA: Council on Foreign Relations (CFR). Available at: https://www.cfr.org/in-brief/how-china-interfering-taiwans-election (accessed 31 December 2020).
[855] Interviewee: P5
[856] Interviewee: P5
[857] Interviewees: P29, P25
[858] Wagner J (2017) China's Cybersecurity Law: What You Need to Know. Available at: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ (accessed 31 December 2020).
[859] Interviewee: P25

on threats from China explicitly flagged the national security risk associated with Chinese-manufactured IoT device components akin to spyware.[860]

Investigative reporter P63 recalled that Chinese hackers had already been accused of causing Taiwanese data breaches and that Chinese IoT manufacturer Xiaomi had come under fire for "collect[ing] personal information without the user's permission and transmit[ting] it to Alibaba's servers in China."[861] P55, who has thirteen years of experience as a cyber security journalist, noted that Australia was one of the first countries to ban some Chinese-owned companies, such as Huawei and ZTE, from national telecommunications networks.[862] The risk of peer-to-peer networks that are regularly contacted by IoT devices from all over the world is well established in literature,[863] justified using maintenance reasons by Chinese manufacturers.[864] Given these risks, there have been reports of the US government putting pressure on Taiwanese companies such as TSMC to cease business with Huawei,[865] and concerns that this may enable journalists to be spied on.[866] The similarity of these threats against individual journalists and the concerns of the whole US and Australian governments underscore the importance of protecting against IoT threats at both the individual and institutional levels (see: Chapter 8).

P40, an investigative journalist with eight years of experience, including working on multiple international collaborative investigations, noted that China's presence in supply chains and its potential use for surveillance is "the most substantial geopolitical issue at the moment in Australia."[867] Two interviewees pointed out a strategic pivot in Australia's diplomatic cyber policy, recognising that politicians as high-profile as Prime Minister Scott Morrison have openly discussed the threat of foreign interference, while trying to balance these concerns with the fact that China is Australia's biggest trade partner.[868] Relatedly, multiple interviewees noted that the US government had expressed concern over the prominent role of Chinese manufacturers in the US electronics market.[869] Interviewees posited that Australia, the UK and US all consider both the value of blended supply chains and the costs of splintering mutual dependence to be geopolitical factors in their discussions about how to manage supply chain threats and IoT regulation.[870] The latter factor includes the precarity of diplomatic relations with China.

---

[860] Rayner G (2023) China can use people's fridges and laptops to spy on them, UK warned. *The Telegraph*, 23 January. Available at: https://www.telegraph.co.uk/news/2023/01/23/china-could-spy-millions-britons-household-objects-like-fridges/ (accessed 7 February 2023).
[861] Interviewee: P63
[862] Interviewee: P55
[863] Smith S (2017) The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.: p. 129; Krebs B (2016) This is Why People Fear the 'Internet of Things'. In: Krebs on Security. Available at: https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/comment-page-1/#comments (accessed 31 December 2020).
[864] Krebs B (2016) This is Why People Fear the 'Internet of Things'. In: Krebs on Security. Available at: https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/comment-page-1/#comments (accessed 31 December 2020); Smith S (2017) The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.: p. 129.
[865] Wu D (2020) Apple Chipmaker TSMC Raises Outlook in Sign of Tech's Resilience. Available at: https://www.bloomberg.com/news/articles/2020-07-16/tsmc-s-profit-beats-as-virus-drives-demand-for-datacenter-chips (accessed 31 December 2020).
[866] Interviewee: P5
[867] Interviewee: P40
[868] Interviewees: P60, P55
[869] Interviewees: P8, P37, P21, P34, P47, P6
[870] Interviewees: P36, P56; Weber V (2020) Strategic Update: Making Sense of Technological Spheres of Influence. LSE IDEAS, April. London, UK: London School of Economics. Available at: http://eprints.lse.ac.uk/107791/1/LSE_IDEAS_Technological_Spheres_of_Influence_April_2020.pdf (accessed 1 January 2021).

However, interviewees were concerned that convoluted supply chains make IoT regulation almost prohibitively difficult.[871] UK interviewee P43, an expert in data rights, technology, surveillance, and press freedom in the UK, argued that the IoT supply chain involves too many actors to establish responsibility, foster accountability or stop data aggregation.[872] This is substantiated by literature on the topic. For example, Haner and Knake noted that improving the security of every device in the US would not have an effect on attacks from botnets, over 96% of which are located outside the country.[873]

Further, Tanczer *et al*. evaluated the utility of the nascent IoT policy landscape in the United Kingdom, acknowledging the difficulty of regulating devices produced globally and with complex chains of custody of data.[874] For example, given the extensive supply chain for even one consumer IoT device, from "manufacturers, software developers, retailers, to third parties,"[875] it is unclear as to who would be responsible for implementation of a self-regulatory Code of Practice, such as the one in the UK, which interviewees confirmed.[876] Interviewees mentioned that this is challenging because entities in the IoT supply chain can be based anywhere in the world and sell through online vendors, and this is the case unless standards are simultaneously adopted internationally.[877] P20, who has 11 years of experience in regulation of emerging technologies, including the IoT, noted that safety considerations have been an ingrained part of global supply chains for decades, but manufacturers who built purely physical devices are not accustomed to thinking about multifaceted security concerns that include software vulnerabilities.[878]

Interviewees saw few realistic options to have fully domestic or regionally localised supply chains for IoT devices, however to combat supply chain threats, they still offered recommendations such as commercial transparency reports and national data localisation.[879] Taiwan interviewees suggested that demand for local manufacturers will grow as awareness and concern about Chinese access to data grows, especially as Taiwan's own technology companies are so well-known and robust.[880] Due to fears over foreign interference through device backdoors and the risk of reliance on foreign manufacturing, interviewees mentioned that some countries have attempted supply chain localisation. For example, there was talk of a desire to prevent Australia from being a data colony, to ensure more reliable product safety and relevant legal frameworks that do not pose a threat to national security.[881] However, participants acknowledged that Australia does not have the manufacturing or storage capacity to compete with Chinese

[871] Interviewee: P28
[872] Interviewee: P43
[873] Haner JK and Knake RK (2021) Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity. *Journal of Cybersecurity* 7(tyab003). DOI: 10.1093/cybsec/tyab003.
[874] Tanczer L, Brass I, Elsden M, et al. (2019) The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In: *Rewired: Cybersecurity Governance*. Hoboken, NJ: Social Science Research Network, pp. 37–56. Available at: https://papers.ssrn.com/abstract=3385548 (accessed 22 April 2021).
[875] Interviewee: P20
[876] Interviewee: P20
[877] Interviewees: P31, P50, P20
[878] Interviewee: P20
[879] Interviewee: P21, P47
[880] Interviewees: P25, P29, P39, P38; TSMC (2020) About TSMC - Taiwan Semiconductor Manufacturing Company Limited. Available at: https://www.tsmc.com/english/aboutTSMC (accessed 31 December 2020); Bloomberg Business Wire (2019) Electronic Manufacturing Services Industry Procurement Intelligence Report | Evolving Opportunities with Foxconn Electronics and PEGATRON in the Electronic Manufacturing Services Market. Bloomberg, 9 December. London. Available at: https://www.bloomberg.com/press-releases/2019-12-09/electronic-manufacturing-services-industry-procurement-intelligence-report-evolving-opportunities-with-foxconn-electronics-and (accessed 31 December 2020).
[881] Interviewees: P3, P60

infrastructure without driving up prices dramatically,[882] likely explaining the relative lack of IoT manufacturing in Australia.[883]

In comparison, President Biden signed into law the CHIPS and Science Act in August 2022, earmarking $52.7 billion for domestic semiconductor manufacturing in the US.[884] Additionally, in October 2022, he implemented heavy restrictions on manufacturing equipment, components, and US talent in China that would stymy the Chinese semiconductor industry and associated IoT supply chains.[885]

7.3 Theme 4: Status of existing protections and mitigations for journalists

7.3.1 Risk assessments and training

This subsection builds on the literature discussed in Chapter 2 regarding cyber security processes, tools, and practices available to the media, by documenting the cyber security protections employed by journalists and news organisations in the four studied countries, per interviewee responses. First, it describes the threat modelling, reporting and policy work done by media organisations, then it discusses the tools taken up by journalists, before exploring newsroom security training, and security education and awareness.

Newsroom security is often neglected, with interviewees in all countries unable to name any large news organisations investing in journalist-specific threat assessments and security expertise in addition to organisational security teams.[886] They reported that this has resulted in low reported awareness among journalists of emerging technological threats, as evidenced by the fact that Di Salvo's 2022 paper does not mention the IoT at all. [887] Interviewees named encrypted channels as their primary protective measure when communicating with sources or other members of their editorial team.[888] However, many interviewees also expressed concern over attempts to weaken encryption by the state.[889] Participants noted that policies for how media organisations must model, report and manage threats differ, with Taiwan's media organisations following a process prescribed by the government, while news outlets in the UK, the US and Australia must determine how to deal with cyber-threats on an institution-by-institution basis.

In Taiwan, interviewees claimed that risk assessments are "first determined by a journalist or an office clerk and then reviewed by the relevant unit to be discussed by various departments to discuss how to

[882] Interviewees: P3, P60

[883] Interviewee: P55; Braue D (2020) Mathematically-secure Australian seL4 microkernel gains global boost. Available at: https://www.csoonline.com/article/3537589/mathematically-secure-australian-sel4-microkernel-gains-global-boost.html (accessed 31 December 2020).

[884] House TW (2022) FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/ (accessed 27 October 2022).

[885] Sheehan M (2022) *Biden's Unprecedented Semiconductor Bet*. 27 October. Washington DC: Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2022/10/27/biden-s-unprecedented-semiconductor-bet-pub-88270 (accessed 27 October 2022).

[886] See, for example, interviewee: P57

[887] Di Salvo P (2022) Information security and journalism: Mapping a nascent research field. Sociology Compass 16(3). John Wiley & Sons, Ltd: e12961. DOI: 10.1111/soc4.12961; Holcomb J and Mitchell A (2015) Adoption of Digital Security Tools. In: *Pew Research Center's Journalism Project*. Available at: https://www.pewresearch.org/journalism/2015/02/05/adoption-of-digital-security-tools/ (accessed 9 December 2022).

[888] Interviewees: P44, P32, P6, P35

[889] Interviewees: P59, P4, P15, P51, P34, P30

tackle the issue."[890] This suggests clear bureaucratic processes that occur within at least Taiwanese public broadcasting organisations, perhaps as an extension to formal government threat reporting procedures. P49, who has five years of experience relating to Taiwan's technology policy and semiconductor industry, posited that any attacks are divulged to the National Communication and Cyber Security Centre or the National Communication Commission, to be reviewed and handled with state assistance.[891] This was reinforced by P58, who works for a public news broadcaster and who stated that every media organisation in Taiwan is mandated to have a cyber security task force.[892]

According to interviewees, the UK has a less standardised landscape.[893] Examples they gave included that centralised organisations such as the BBC apply their policies across the board, while broadcasters like Channel 4 commission material and therefore each contracted production company has flexibility in their risk assessment and security training processes.[894] Interviewees discussed that following threats relating to a number of global data leaks investigations, large organisations such as the Guardian have teams of technical information security and systems experts, either on staff or contracted as consultants.[895] They noted that there are long-established risk assessments and security processes relating to physical threats,[896] but that the rapid shifts in journalists' digital threat landscape make keeping training up to date difficult,[897] something with which US interviewees agreed.[898]

Threat modelling across all four countries appeared to interviewees to rely on institutional practices, regardless of whether the organisations' processes are established and well-communicated. P52, an investigative data journalist and member of Hacks/Hackers, noted that journalism-specific threat modelling is rarely carried out in Australia, and almost exclusively at an organisational level but that this does not filter through to editorial policies or a "systematic approach to educating and maintaining awareness around threat modelling for journalists."[899] P42, a journalist of 30 years, asserted that "in Australia, we don't have a culture of risk assessments because Australians generally don't feel that there is a risk."[900] As in Australia, US interviewees noted that most US news organisations are underfinanced and therefore cannot afford to invest in up-to-date security tools and training or in-house consultants.[901] Still, they noted that there are some civil society and news organisations that are able to sporadically hire independent experts or entire security teams to conduct threat modelling.[902]

Interviewees noted discrepancies between the threat intelligence generation work done by domestic organisations compared to foreign ones based in each country. For example, P42, a journalist of 30 years, made the point that threat intelligence and protection measures at Australian news outlets are notably worse than at foreign news organisations, as there is an acute lack of understanding of risk assessments in the Australian media.[903] In contrast, intra-organisational threat intelligence channels for international

[890] Interviewee: P58
[891] Interviewee: P49
[892] Interviewee: P58
[893] Interviewees: P45, P11, P22, P44
[894] Interviewees: P45, P22
[895] Interviewees: P12, P15
[896] Interviewees: P22, P44
[897] Interviewees: P44, P15, P11
[898] Interviewees: P44, P47, P57
[899] Interviewee: P52
[900] Interviewee: P42
[901] Interviewees: P34, P47, P12
[902] Interviewees: P47, P12, P17
[903] Interviewee: P42

news organisations with journalists in Taiwan were reported by interviewees to be well-developed, relative to domestic media organisations.[904]

Although media organisational cyber security training materials and processes differ across the countries, no interviewees mentioned the inclusion of IoT risk in training.[905] This was partially justified by some interviewees as being due to financial and time constraints.[906] According to interviewees, these financial constraints arose in part because of large layoffs of journalists and media consolidation, such that remaining news outlets cannot compete financially, nor can they afford to invest in resources to protect them against IoT risks.[907] P42, a journalist of 30 years, noted that the financial crisis facing journalism around the world has had dire repercussions for small Australian news organisations who are so preoccupied with staying afloat that they cannot afford to fight proposals for more restrictive national security legislation.[908] As noted by McGregor and corroborated by multiple interviewees, additional constraints include the individualised nature of determining necessary mitigation methods, relating to a journalist's beat (the topics on which they report) and their attack surface (i.e. which technologies they interact with and the security of their work practices).[909] Further, multiple interviewees recognised high-level political denigration of the media in Australia, the US and the US inhibits journalists from seeking support and protection, including by sharing cyber-attack information, from and with the state.[910]

For cyber security training more broadly, interviewees reported that Australian news outlets tend to minimise the number of staff who are required to receive high-risk training due to their policy of drawing on foreign correspondents employed at other organisations rather than deploying their own people overseas.[911] In contrast, in Taiwan, P38, an Asia correspondent based in Taipei, mentioned that "every few years, we need to take a risk course" that focuses on high-risk environments such as warzones, as well as cyber security lessons, although these do not cover the IoT.[912] P46, a security researcher with nine years of expertise in technology-related threats to press freedom in the US, noted that US journalists who are at high-risk of being attacked by governments, cartels or other very well-resourced adversaries tend to be abstractly aware of the risks but may not know how threats would manifest or know of recommended mitigations.[913] This is relevant to IoT threat protections, as US interviewees noted that the consumer IoT is so prolific that warning journalists to avoid devices would provide them with insufficient protection.[914] Further, multiple UK interviewees believed that journalists are not cognisant of the range of ways in which IoT devices can threaten their security or privacy.[915] Another difficulty of updating journalists' education to reflect emerging technological threats perceived by interviewees is that devices

[904] Interviewee: P29
[905] Berdan K (2021) CLTC Report: An Evaluation of Online Security Guides for Journalists. 20 January. California, USA: CLTC UC Berkeley Center for Long-Term Cybersecurity. Available at: https://cltc.berkeley.edu/2021/01/20/cltc-report-an-evaluation-of-online-security-guides-for-journalists/ (accessed 1 March 2021).
[906] Interviewees: P61, P23, P30, P5, P22, P12, P16
[907] Interviewees: P61, P23, P22, P30, P56, P42, P12
[908] Interviewee: P42
[909] Interviewees: P46, P57, P41; McGregor SE (2021) *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.
[910] Interviewees: P42, P52, P40, P9, P61, P47, P22, P23, P12, P44; Mauldin W (2020) Voice of America Director Resigns After Clashing With Trump Administration. Wall Street Journal, 15 June. Available at: https://www.wsj.com/articles/voice-of-america-director-resigns-after-clashing-with-trump-administration-11592259031 (accessed 1 January 2021);
[911] Interviewee: P42
[912] Interviewee: P38
[913] Interviewee: P46
[914] Interviewees: P17, P12, P47, P57
[915] Interviewees: P44, P12, P22

can combine several sensors and collect sensitive information disclosed within variable distances, which literature suggests even lawyers may not have recognised as a possibility.[916]

In terms of common security tools and techniques, interviewees named some encrypted apps for messaging (Signal, but not WhatsApp), email (Protonmail), and document transfers (SecureDrop) as gaining traction in both UK and US journalistic communities, the same that have been mentioned in journalism studies literature to date.[917] UK and US interviewees also noted that traditional advice such as meeting sources in secluded spaces, not carrying devices and limiting the technological means of access to both journalists and their information remain applicable,[918] though not always possible.[919] Comparatively, Taiwan journalist interviewees disclosed that neither local journalists[920] nor foreign correspondents[921] undertake significant additional personal security provisions to supplement those implemented by news organisations when in Taiwan, unless working on sensitive stories which does lead to more protective measures being used.[922]

As is clear from literature reviewed for Chapter 2 and interviewee responses, security education and awareness for journalists require constant iteration,[923] in ways that address the needs of journalists. US interviewee P46, a security researcher with nine years of expertise in technology-related threats to press freedom in the US, stated that reiteration is necessary "to make the newsroom comfortable with cyber security being a part of the work that they're doing" and to ensure that they are intended to protect "a combination of [journalists'] physical, digital, legal and emotional well-being."[924] Interviewees across countries agreed that this is difficult as it involves both making lessons as concise and informative as possible, without overloading journalists, and while ensuring that the information is tailored to the threat profile of individual journalists and their sources.[925] Additionally, UK interviewees noted that news organisations face so many demands that training often receives insufficient attention.[926]

US interviewees noted that, to their knowledge, there has only been one US news organisation that invested in securing the newsroom beyond generic infrequent training and that this organisation had stopped doing so.[927] P46, a security researcher with nine years of expertise in technology-related threats to press freedom in the US, noted that typical security training for journalists covers "passwords, two-factor [authentication] and social engineering in the context of phishing."[928] Likewise in Australia, P52, an investigative data journalist and member of Hacks/Hackers, and P40, an investigative journalist with eight years of experience, including working on multiple international collaborative investigations, described media organisations' cyber protection policies as "fairly immature." [929]

---

[916] Interviewee: P17; Tse C and Browning J (2020) Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls. Bloomberg.com, 20 March. Available at: https://www.bloomberg.com/news/articles/2020-03-20/locked-down-lawyers-warned-alexa-is-hearing-confidential-calls (accessed 1 January 2021).
[917] Interviewees: P1, P44; Henrichsen JR (2021) Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice* 0(0). Routledge: 1–20. DOI: 10.1080/17512786.2021.1927802.
[918] Interviewees: P12, P15, P26
[919] Interviewee: P47
[920] Interviewees: P63, P58
[921] Interviewees: P29, P38
[922] Interviewees: P38, P63, P29
[923] Interviewee: P46
[924] Interviewee: P46
[925] Interviewees: P46, P17, P54, P12, P41
[926] Interviewees: P44, P12, P22
[927] Interviewees: P57, P46
[928] Interviewee: P46
[929] Interviewees: P52, P40

Although Taiwan has a progressive threat reporting regime, interviewees indicated that threat management is still difficult. P5, who has 25 years of experience working on press freedom in Taiwan, re-stated the gulf between independent Taiwanese news outlets and those that are extensions of large entertainment corporations regarding the cyber security protection methods employed by journalists and news organisations.[930] They suggested that smaller organisations require individual journalists to manage the bulk of their personal and professional cyber security, while commercial entities have in-house specialists.[931] Similarly, research by Watkins in 2017 and by Henrichsen in 2021 illustrates that individual "security champions" have long shouldered the responsibility for advancing the information security of their newsroom, with ad-hoc attempts to fill the gap left by an absence of institutionalised security practices as media organisations add tools to their repertoire rather than amending behaviours and practices.[932] [933]

Interviewees noted that some tools and guidance materials can even be inaccessible to members of the media. P13, a researcher with expertise in journalists' experiences in the US, Europe and the UK, postulated that cyber security in those contexts has an "anti-institutionalist" rhetoric that make tools difficult to adopt by journalists without experience of decentralised hacker communities.[934] They claimed that such communities are often insular and so cutting-edge tools may not be shared with the journalists who most need them.[935] In contrast, both digital safety trainer P12 and foreign correspondent P29 noted that Taiwan has an active information security "scene" catering to the media.[936] Further, interviewees and literature read for Chapter 2 claimed that freelance journalists do not have the same level of access to any training that might exist,[937] meaning that they lag behind even the limited security knowledge available to staff reporters. This is critical: Crete-Nishihata *et al.* argue that freelancers are more likely to need support, training and threat intelligence sharing from their peers.[938]

Regarding the development of cyber protection processes for at-risk populations such as journalists, interviewees recognised a gap between policy research and implementation. This is because they foresaw that the process would require minimisation of overhead costs while still employing effective security procedures, which cannot always scale down to smaller organisations.[939] However, this does not have to be the case, as P54, who has expertise in the impact of technological threats on civil liberties in the US, relayed their experience that media cyber security training can be effective if it is framed as enabling them to do their job, rather than on protecting them.[940] They gave the example of teaching journalists that a VPN could help protect their identity and information from hostile forces and that it can "give them access to a different view of the internet because your IP address looks like it's coming from a different country, then that can mean better reporting". According to P54, this prevented journalists from worrying that

[930] Interviewee: P5
[931] Interviewee: P5
[932] Watkins EA (2017) Workers' Sensemaking for Information Security: a Research Agenda for the Future of Work. ACM. Available at: https://drive.google.com/file/d/1llLwRsXCSqnPxuRueHk2M1cYD2x4U1BZ/edit? (accessed 9 September 2019).
[933] Henrichsen JR (2021) Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". Journalism Practice 0(0). Routledge: 1–20. DOI: 10.1080/17512786.2021.1927802.
[934] Interviewee: P13
[935] Interviewee: P13
[936] Interviewees: P12, P29
[937] Interviewee: P55
[938] Crete-Nishihata M, Oliver J, Parsons C, et al. (2020) The Information Security Cultures of Journalism. Digital Journalism 0(0). Routledge: 1–24. DOI: 10.1080/21670811.2020.1777882.
[939] Interviewees: P54, P47
[940] Interviewee: P54

these protective measures will hinder their reporting or harm their sources, which interviewees noted is a particular concern for journalists.[941] Similarly, Tsui and Lee, whose research was reviewed for Chapter 2, found that journalists who conceptualise security as "opportunity" and proactively improve their security stance are able to report on a more diverse range of topics, without feeling impeded from covering more sensitive stories that may engender more attacks and surveillance.[942]

Similarly, P40, an investigative journalist with eight years of experience, discussed training sessions they have run for the Australian Broadcasting Corporation and the Guardian. These are aimed at making threat modelling and security topics, such as surveillance, accessible to journalists by fostering scenario-based discussions.[943] They argued that this kind of practical information sharing is crucial for ensuring that threats stemming from abstract concepts such as the IoT are matched to the journalistic process so that journalists take them seriously.[944] This feedback in particular was important for the development of the framework of mitigations and countermeasures (see: Chapter 8) in order to ensure they were framed in a useful way for the specific user group of journalists.

7.3.2 Sharing threat intelligence between media organisations and journalists

One response to IoT risk that interviewees acknowledged could expand the media sector's ability to identify threats and collectively respond to them would be the expansion of threat intelligence sharing networks. However, across all four countries, formal threat intelligence sharing mechanisms appear nonexistent, with few exceptions from civil society organisations,[945] groups of media lawyers[946] or independent security experts.[947] Interviewees suggested that this may be because of a desire for security through obscurity,[948] but also because lax ownership regulations allow media consolidation,[949] leading to political polarisation and financial competition between news outlets, which makes organisations less likely to collaborate.[950] International collaborative investigations were considered by interviewees to be the main examples of news organisations developing and sharing security and threat knowledge. For example, UK interviewees named high-profile collaborative journalistic investigations (e.g. the Paradise Papers, the Panama Papers, the Snowden revelations and Wikileaks).[951] This subsection will therefore first discuss the current state of threat intelligence sharing in each of the four countries, per interviewee responses, and then make a case regarding the importance of threat intelligence sharing networks as an asset against IoT threats for journalists.

Regarding threat intelligence sharing between journalists and news organisations in the UK, interviewees mentioned a number of established informal[952] and formal[953] mechanisms, although both appear to

[941] Interviewees: P54, P47, P12
[942] Tsui L and Lee F (2019) How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. Journalism 00(0). SAGE Journals: 1–23. DOI: 10.1177/1464884919849418.
[943] Interviewee: P40
[944] Interviewee: P40
[945] Interviewees: P44, P61, P15, P16, P12, P22
[946] Interviewees: P45, P15
[947] Interviewees: P12, P46
[948] Interviewee: P35
[949] Interviewees: P61, P22
[950] Interviewees: P56, P61, P52, P42, P63, P29
[951] Interviewees: P1, P15
[952] Interviewees: P45, P53, P1, P16, P15
[953] Interviewees: P45, P15

unwittingly exclude freelancers and citizen journalists.[954] Informal methods, which interviewees noted involve a social network of journalists, are possible because of a historical concentration of news outlets in certain geographical locations, which enables staff to mingle socially.[955] This is in contrast to Australia, where interviewees recognised the country's low population density means there is no single location with a high concentration of news outlets. Therefore, interviewees thought that informal threat intelligence sharing mechanisms, such as social events that attract journalists from different organisations, are less likely,[956] although P40, an investigative journalist with eight years of experience, including working on multiple international collaborative investigations, noted that they have experience of an informal channel spanning different organisations.[957]

From interviewee responses, Australian and US media threat intelligence sharing appeared to be the least developed. Four Australia interviewees divulged that media threat intelligence is rarely promulgated across the entire industry,[958] as the level of partisanship and fierce financial competition between news organisations decreases their incentive to cooperate.[959] Additionally, the interviews revealed no consistent or comprehensive threat intelligence networks between organisations or individuals,[960] and it is difficult to determine to what extent these structures are adequate even within the largest media corporations. Although interviewees recognised that the Australian journalists' union (the Media, Entertainment and Arts Alliance) does organise information sessions on risk assessments, they named no formal or government-ordained mechanisms for threat intelligence sharing within the media industry.[961]

US interviewees noted that formal communication of this kind between media outlets was rare because of the partisanship of most news organisations.[962] Still, while US interviewees could not name any formal or systematic threat intelligence sharing processes between news organisations, P46, a security researcher with nine years of expertise in technology-related threats to press freedom in the US, started an informal information sharing group for the security teams of news organisations to discuss asset management and incident detection.[963]

In contrast, P58, who works for a public news broadcaster, disclosed that threat intelligence sharing systems in Taiwan include informal discussions between managers of different news stations, and quasi-formal through seminars and workshops.[964] However, there was notable disparity between accounts by different journalist interviewees in Taiwan, indicating insufficient communication of threat intelligence sharing channels across the breadth of the media in Taiwan. For example, P29, a foreign correspondent in Taiwan, noted that, to their knowledge, "there are no formal mechanisms sort of between the different media organisations and bureaus in Taiwan that inform me of the journalistic risks." [965] However, P29 acknowledged that inter-organisational sharing of this intelligence is likely done by high-level representatives based at regional hubs,[966] and P58, who works for a public news broadcaster,

[954] Interviewees: P15, P22
[955] Interviewees: P53, P15
[956] Interviewee: P52
[957] Interviewee: P40
[958] Interviewees: P52, P42, P55, P40
[959] Interviewees: P42, P52
[960] Interviewees: P42, P52, P55, P40
[961] Interviewees: P42, P52, P55, P40
[962] Interviewee: P61
[963] Interviewee: P46
[964] Interviewee: P58
[965] Interviewee: P29
[966] Interviewee: P29

corroborated that there are formal meetings arranged by the National Communications Commission or organisations within Taiwan's media and civil society space, including the "Commercial Radio Broadcasting Association, Media Watch, [and the] Association of Taiwan Journalists."[967]

UK interviewees reported that formal methods of threat intelligence sharing include channels of communication between different news organisations' legal teams,[968] including the Society of Editors, the Media Lawyers Association, and the Media Legal Defence Initiative. They remarked that these conversations regarding legal threats occur both between in-house legal advisors and within news organisations every three months[969] and on a case-by-case basis.[970] They also noted that this has led to the creation of the Press Association's central database of reporting restrictions,[971] but these focused on legal threats sharing, not just cyber threats. In fact, UK interviewees could not recall an industry-wide formal mechanism for non-legal cyber threat intelligence sharing.[972]

Most semi-formal cyber threat intelligence sharing appeared to interviewees to be conducted by civil society organisations in the media space. UK interviewees praised civil society organisations, such as the Committee to Protect Journalists, the International News Safety Institute and Reporters without Borders, for maintaining awareness of potential threats, although noted that they lack the resources to proliferate training widely.[973] US interviewees also noted that threat intelligence sharing occurs via word of mouth or via civil society advisories online.[974] Relevant non-governmental organisations that were named as being prominent in the US include the Electronic Frontier Foundation (EFF) and the Reporters Committee for Freedom of the Press (RCFP), although one interviewee stated that the protocols used by these organisations are not published externally.[975]

Although interviewees noted few established and well-maintained threat intelligence sharing processes within the media industry in each country, and none internationally, they were able to recognise the benefits of such networks. For example, P46, a security researcher with nine years of expertise in technology-related threats to press freedom in the US, noted the significance of accurate threat intelligence, recommending that "the point here is not to teach everyone about the doom and gloom world of Internet-connected devices, but just to make people aware of the potential impact that it could have in a worst case scenario."[976] They compared cyber security threats to news organisations to legal risk, pointing out that "if we were to constantly talk about the potential legal risk associated with reporting on a sensitive story, we wouldn't get anything done." [977] They also noted the importance of a team of journalistic security experts, analogous to in-house lawyers, to help journalists to navigate their own evolving threat landscapes, and to ensure that they are empowered to continue reporting because their risk level is tolerable.[978] Relatedly, P48, a cyber security and threat intelligence expert, noted the significance of increasing Australian cognisance of a shared supply chain and similar threat landscape.[979]

[967] Interviewee: P58
[968] Interviewees: P45, P15
[969] Interviewee: P15
[970] Interviewee: P45
[971] Interviewee: P45
[972] Interviewees: P53, P45, P15, P16
[973] Interviewees: P15, P22
[974] Interviewees: P54, P47, P44, P23, P35
[975] Interviewee: P35
[976] Interviewee: P46
[977] Interviewee: P46
[978] Interviewee: P46
[979] Interviewee: P48

They said that this could lead to the recognition that more cooperation between news outlets would be beneficial for the whole country's media industry.[980] According to P56, an international law expert, "collaborative buy-in" would result in an overarching threat intelligence sharing model in the media industry.[981] However, interviewees claimed that the aforementioned factors have created a combative tension that precludes the press from feeling like they can share information.[982]

7.4 Conclusion

In conclusion, this chapter consolidated and discussed the geopolitical and organisational challenges that affect the media industry's ability to combat IoT threats in Taiwan, Australia, the UK, and the US. This chapter also recorded contemporary journalist and source protections, and identified gaps in these methods. This allows the content of the framework presented in Chapter 8 to take into account existing methods, channels and supporting institutions, to ensure that the framework is tailored to the reality of journalists' environment in each country and therefore can be feasibly implemented.

This chapter's contemporary cyber protections and threat mitigations employed by journalists and news organisations demonstrated a common lack of resources available to devote to security. It further showed low levels of comprehension of emerging technological threats and how they compound existing legal challenges. Notably, interviewees did not know of any instances of integration of IoT-specific knowledge, mitigation processes or behaviours into news organisational or journalistic security training in any of these countries or in any countries at all. This gap was clearly illustrated by P27, who has 26 years of experience in technological threats to the press in Australia, who said of the IoT threat landscape for journalists: "it's fractal in a way, there are so many facets and details and intricate interrelationships between the different kinds of risks."[983] This is especially true when this chapter is considered in conjunction with the patchwork of existing and emerging legal threats that were explored in Chapter 6.[984]

Additionally, interviewees noted the cultural hegemony of the US and the UK and the pervasive role of Murdoch-owned media globally. Further, while Taiwan's perceived threat from China is the most extreme,[985] it was seen as shared to a considerable degree by interviewee experts for the other three countries as well. This may signify that these four media environments are representative of media organisations in democracies more broadly.[986] Further, secondary literature, such as from Reporters without Borders,[987] indicates that the similarities found in these four cases extend to other democratic countries. For example, financial crises and inadequate regulation of media ownership is causing

[980] Interviewee: P48
[981] Interviewee: P56
[982] Interviewee: P56
[983] Interviewee: P27
[984] Interviewees: P27, P3, P40, P42, P60, P14, P28, P33, P55, P36, P48, P52, P56
[985] Rawnsley GD and Rawnsley M-Y (2018) Critical Security, Democratisation and Television in Taiwan. 2nd ed. UK: Taylor and Francis.
[986] Paterson C (2003) Prospects for a democratic information Society: The news agency stranglehold on global political discourse. In: Presented to the EMTEL: New Media, Technology and Everyday Life in Europe Conference, London, UK, 23 April 2003. London School of Economics and Political Science. Available at: https://www.lse.ac.uk/media@lse/research/EMTEL/Conference/papers/Paterson.pdf; Hermann E and McChesney RW (2001) Global Media: The New Missionaries of Global Capitalism. United Kingdom: Bloomsbury Academic.
[987] Reporters without borders (2019) Only nine percent of humankind lives in a country where press freedom is good. Available at: https://rsf.org/en/news/only-nine-percent-humankind-lives-country-where-press-freedom-good (accessed 1 January 2021); Reporters Without Borders (RSF) (2017) #SPOILERSFORFREEDOM: Exiled journalists warn democracies about decline in media freedom. Available at: https://rsf.org/en/news/spoilersforfreedom-exiled-journalists-warn-democracies-about-decline-media-freedom (accessed 1 January 2021).

increasing conglomeration and thus both decreasing media plurality and growing news deserts in many countries.[988] While it is impossible to achieve comprehensive applicability of the findings of this study and of the forthcoming framework for IoT threat mitigation across all democracies, there is therefore some generalisability, given the depth and quantity of the expert interviews upon which Chapters 6 and 7 are based.

The interviews underpinning this chapter and Chapter 6 highlighted the need for practical tools and guidance for protections and mitigations that can be flexible depending on circumstance, and are specific to the media. These two chapters demonstrated that "the individual doesn't have the base capacity to make individual good policy decisions that are going to carry out to every other individual around them, because it only takes one person to make a not-good decision to compromise everyone in their circle."[989] This emphasises the importance of spreading out responsibility for assessing and managing IoT risk to the media between different decision-makers and key stakeholding organisations. This is the main premise of the IoT device categorisation in Chapter 5, and the reason why the IoT protection framework in Chapter 8 addresses various media roles, rather than just journalists. Chapter 9 will discuss how the contextual analysis in Chapters 6 and 7 can be combined with the conceptual models in Chapter 5 and the countermeasures framework in Chapter 8, to be incorporated into journalistic security strategies to mitigate IoT emerging IoT threats to journalists and sources.

[988] UNESCO (2018) Trends in media pluralism - UNESCO Digital Library. In: World Trends in Freedom of Expression and Media Development: Global Report 2017/2018. Paris: UNESCO, pp. 66–100. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000261370 (accessed 1 January 2021).
[989] Interviewee: P57

Chapter 8: Framework

8.1 Introduction

This chapter combines and analyses elements from the previous three chapters to form a framework of possible countermeasures for the consumer IoT. The objective of the framework was to create a practical tool that combined two objectives. First, it matches threats from Chapter 5 to appropriate countermeasures. Second, it allows users in the media industry to personalise their risk management process through filtering of relevant countermeasure attributes (e.g. relative benefits and disadvantages) and elements specific to journalism (e.g. media roles and journalistic workflow phases).

Such a tool is necessary because of the overwhelming range of advice available regarding securing consumer IoT devices,[990] but none of which is specific to the media. A literature review (see: Chapter 2) demonstrated a clear knowledge gap: a lack of resources relevant to IoT protection for the specific population of journalists. To close this gap, this chapter presents a novel countermeasures framework.

The framework builds on two important elements of the IoT journalistic security toolkit from Chapter 5. First, the conceptual IoT model acts as a basic educational stimulus for journalists with little to no knowledge of IoT risk, to demonstrate to them where to look for IoT devices so that they can understand the scale of these technologies and their networks. Second, the threats categorisation has its own section of the framework (the column "Threats addressed by each countermeasure"), so that users can decide which countermeasures are best implemented based on their risk profile and anticipated threats.

In addition to building on work from previous chapters, this framework was populated and refined through online questionnaires sent to media, cyber security and IoT, and states' capabilities experts. For details on the definitions used, survey creation, analytical methods, and other methodological questions, see Chapter 3.

8.2 Framework overview

The framework is structured with recommended countermeasures at its centre. Each recommendation has noted disadvantages, and is matched to relevant threats that it addresses, followed by an assessment of the function of the countermeasure. Then, to assist with categorising the recommendations according to their relevance to different levels of the press, each protection is given a "beneficiary," i.e. whether the countermeasure is intended to help an individual journalist and source, a news organisation as a business, or the news media existentially. To ensure that protections are suited to the practical needs of the press as a whole, they are also assigned to phase(s) of the editorial workflow to which this countermeasure is most relevant. They are further matched to categories of media roles that are most likely to be responsible for implementation. Finally, the framework includes a feasibility label to demonstrate ease of implementation of each countermeasure.

The core of this framework is its threats-countermeasures matching. This framework attempts to offer protections and mitigations for the threats modelled in Chapter 5, without resorting to only prescriptive technical solutions. Rather, the countermeasures in this framework range from technical suggestions to strategic recommendations for collective action to push for policy changes, as well as for organisational

[990] Turner S, Nurse J and Li S (2021) When Googling It Doesn't Work: The Challenge of Finding Security Advice for Smart Home Devices. In: *15th International Symposium on Human Aspects of Information Security & Assurance (HAISA)* (eds S Furnell and N Clarke), Cham, 2021, pp. 115–126. IFIP Advances in Information and Communication Technology. Springer International Publishing. DOI: 10.1007/978-3-030-81111-2_10.

and behavioural shifts. The imagined users of this framework are members of the media, including both those who seek to protect themselves, their sources, and their work, and those who seek to influence governments to implement policies that protect the industry existentially. This combination of individual, organisational and community-based measures addresses the social and emotional elements of journalistic security, by removing the responsibility for all protective actions from individual members of the media, and through the inclusion of secondary psychological threats. This framework is intended for use as part of a toolkit that includes the threats-focused resources in Chapter 5, and the idea of structuring the framework around threats was discounted as too theoretical and therefore possibly less instructive for the target user community. Therefore, whilst the traditional approach in risk identification, assessment, and mitigation is to open with a consideration of threats, this framework deliberately begins with countermeasures as part of its user-centric focus to avoid repeatedly bombarding users with a threats-first perspective that may result in a sense of helplessness.

Users are also encouraged to consider the implementation of these countermeasures as part of their workflow. This framework allows any members of the media to use the framework interactively from several different perspectives to identify threats and protections, as well as immediately visualise implementation considerations such as countermeasures' functions and feasibility.[991] To ensure that users do not view countermeasures as infallible, and to enable effective risk assessment, experts added to a list of disadvantages that were then standardised and used in the framework. Further, by including "beneficiaries" within this multifaceted analysis,[992] this framework moves beyond the dichotomy of "individual" versus "organisational" in recognising how threats and protections can impact different actors. This chapter therefore bridges the gap between knowledge held by IoT security experts and the press, the latter who have specific practical needs that are currently not adequately addressed by the security community.

As is common in cyber security doctoral research,[993] representation of the framework is in the form of a prototype showing proof of concept, validated by different groups of stakeholder experts. The utility of the framework for this thesis is therefore best considered as an intellectual tool, rather than as a product optimised for ideal user experience. While the framework is portrayed as an Excel spreadsheet, as discussed in section 8.3, its presentation could change depending on the needs of the user group and the technology available. If the tool were being deployed to a news organisation, then it would likely require a different interface technology to make it easier to sort/filter, but this current conceptual model fits the intended purpose here.

8.2.1 Framework definitions

In the following subsections, definitions for the various components of the framework will be stated and clarified. The columns of the framework are (as seen from left to right in the supplementary spreadsheet document submitted with this dissertation):

[991] Chen J and Urquhart L (2021) 'They're all about pushing the products and shiny things rather than fundamental security': Mapping socio-technical challenges in securing the smart home. *Information & Communications Technology Law* 0(0). Routledge: 1–24. DOI: 10.1080/13600834.2021.1957193.

[992] Pierce J, Fox S, Merrill N, et al. (2018) Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. Proceedings of the ACM on Human-Computer Interaction 2(CSCW): 139:1-139:24. DOI: 10.1145/3274408.

[993] Nthala N (2019) *Home data security decisions*. http://purl.org/dc/dcmitype/Text. University of Oxford, Oxford, United Kingdom. Available at: https://ora.ox.ac.uk/objects/uuid:72401f07-d923-4448-af20-f99ecb677e3a (accessed 9 August 2022); Carvalho R (2019) *Enhancing the investigation of malware-related crimes using semantic technologies*. http://purl.org/dc/dcmitype/Text. University of Oxford, Oxford, United Kingdom. Available at: https://ora.ox.ac.uk/objects/uuid:5abeb135-ff33-42b4-8847-0aefe8e82c8f (accessed 9 August 2022).

1. Countermeasure indicator (e.g. “A”) (column 1)
2. Countermeasures (Protections & Mitigations) (column 2)
3. Disadvantages to each countermeasure (column 3)
4. Threats addressed by each countermeasure (from the threats categorisation) (column 4)
5. How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure) (column 5)
6. Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?) (column 6)
7. Phase(s) of the editorial workflow to which this countermeasure is most relevant (column 7)
8. Category of media roles that is most likely to be responsible for implementation of this countermeasure (column 8)
9. Feasibility of the countermeasure (column 9)

Columns 2, 3, 5, 6, 7, 8 and 9 are defined in this section; however, column 4 will not be defined in this section as it consists of IoT threats to the press that were taken directly from the threats categorisation (explained in detail in Chapter 5).

8.2.1.1 Defining “Countermeasures” (column 2)

The primary organising method for the framework centres around countermeasures that address threats detailed in Chapter 5. Countermeasures are defined in NIST SP 800-53 Rev. 5 from FIPS 200 as “actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. [They are] synonymous with security controls and safeguards.”[994] This definition was chosen because of the level of detail in its recommended security controls and for consistency throughout this dissertation (see: Chapter 1).

Other NIST definitions mention “information systems” and “confidentiality, integrity and availability” more explicitly. An example is: “the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information” from CNSSI 4009-2015 under security controls from FIPS 199.[995] However, this kind of definition was not used because these particular characteristics do not reflect the key objectives of the countermeasures framework. Further, the term “prescribed” is incongruous with the tone intended to be conveyed by this framework, which is less normative and more informative.

NIST’s countermeasures definition was also chosen to ensure clarity that the framework’s recommended countermeasures do not presume full immunity against IoT threats, but rather that they both limit the likelihood and severity of attacks.[996] This latter aspect is in line with NIST’s definition for protection:

> *“[...] The solution to the problem is optimized through a balanced proactive strategy and a reactive strategy that is not limited to prevention. The strategy also encompasses avoiding asset loss and*

[994] National Institute of Standards and Technology (2006) *Minimum security requirements for federal information and information systems.* NIST FIPS 200, March. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.FIPS.200; National Institute of Standards and Technology (NIST) (2021) *countermeasures - Glossary | CSRC.* Available at: https://csrc.nist.gov/glossary/term/countermeasures (accessed 13 October 2021).
[995] National Institute of Standards and Technology (2004) *Standards for security categorization of federal information and information systems*. NIST FIPS 199, February. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.FIPS.199.
[996] National Institute of Standards and Technology (NIST) (2021) *mitigate - Glossary | CSRC.* Available at: https://csrc.nist.gov/glossary/term/mitigate (accessed 13 October 2021).

consequences; detecting asset loss and consequences; minimizing (i.e., limiting, containing, restricting) asset loss and consequences; responding to asset loss and consequences; recovering from asset loss and consequences; and forecasting or predicting asset loss and consequences."[997]

The emphasis in this definition on both prevention and reaction is aligned with this thesis' overall argument and intent, and thus neatly encapsulates the definitional need in this instance.

The criteria for each countermeasure were: (1) That it could be conveyed in clear and simple language, (2) that it was directly relevant to specific IoT threats from Chapter 5's threat categorisation system, and (3) that an individual could work toward it. However, regarding the third criterion, certain countermeasures will be more usefully implemented by people working together. All three of these criteria were assessed through the validations study (see: section 8.2.3.2), and countermeasures were determined to have achieved these three criteria if over 50% of validators agreed with the assessment. Over 50% was chosen as this represented a majority, but did not try to achieve impossible standards, i.e. countermeasures on which a diverse range of security experts could unanimously agree. No single countermeasure is expected to be completely effective in either prevention or mitigation of IoT threats. This said, all stated countermeasures can be used against an IoT threat. Factors that affect the level of efficacy of each countermeasure include which individual role is implementing the countermeasure, and when in the workflow this is being done.

8.2.1.2 Defining "Disadvantages" (column 3)

Column 3, focused on the disadvantages of the countermeasures proposed in column 2, was validated by both journalists and cyber security experts (see: sections 8.2.3.2 and 8.3.2.2.2). It is necessary to include disadvantages associated with each countermeasure because these recommended protections all have downsides, so it is a matter of giving the target user group of this framework enough information that they can make decisions based on their own needs and concerns. None of these protective techniques are infallible, and each should only be attempted with the knowledge that experts surveyed in the exploratory study (see: Chapter 4) unanimously felt that threats from IoT devices could no longer be avoided even with the most rigorous protection methods.

8.2.1.3 Defining "Function of countermeasure," i.e. "How is it estimated that this protection will help against a given threat?" (column 5)

There are multiple potential perspectives on how to explain a countermeasure's function of protection or mitigation. This framework builds on the work of Ahmad *et al.* by grouping countermeasures into categories by functionality.[998] Ahmad *et al.* also looked at resources from diverse security fields (e.g. information security and military affairs), which aligned well with the different kinds of threat categories used in the framework. This paper was chosen because of its clearly defined and well-sourced categories, as well as its intention that the different categories of protection would be layered for optimal effect.

Functions 1-6 (PREV to DECEP) are temporal, while 7-9 (PERI to LAYER) are spatial:

1. *"Prevention (PREV): Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure*

[997] National Institute of Standards and Technology (NIST) (2021) *protection - Glossary | CSRC.* Available at: https://csrc.nist.gov/glossary/term/protection (accessed 13 October 2021).

[998] Ahmad, A., Maynard, S.B. & Park, S. Information security strategies: towards an organizational multi-strategy perspective. J Intell Manuf 25, 357–370 (2014). https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/s10845-012-0683-0.

2. *Deterrence (DETER): Deterrence employs disciplinary action to influence human behavior and attitude*
3. *Surveillance (SURV): Surveillance is the systematic monitoring of the security environment towards developing situational awareness to assist in adapting to fast-changing circumstances and threats*
4. *Detection (DETECT): Detection is an operational-level strategy aimed at identifying specific security behavior*
5. *Response (RESP): Response takes appropriate corrective actions against identified attacks*
6. *Deception (DECEP): Deception distracts an attacker's attention from critical information assets using decoys thereby leading the attacker to waste time and resources*
7. *Perimeter defense (PERI): Perimeter defense creates a boundary around information assets that is secured by regulating traffic at every incoming and outgoing information channel (choke points)*
8. *Compartmentalization (COMP): Compartmentalization reduces an attacker's opportunities by dividing the intended area of attack into zones that are secured separately*
9. *Layering (LAYER): Layering uses multiple countermeasures that function independently but increases the effectiveness of the defense when working together thereby posing a series of challenges to the attacker. The defensive system is designed to be resilient by overlapping the series of countermeasures, whereby each countermeasure complements the next so that if one fails another will back it up."*[999]

Using the function of a countermeasure as an organising principle does have downsides, including the fact that it is derived from research on organisational countermeasures to threats. Further, it is not a ranking/scale, which means it may be slightly less intuitive to use. However, the categories are also applicable to individual countermeasures and less arbitrary and subjective than if the creation of a scale for ranking countermeasures. Further, ranking protections, or assigning them quantitative values, would be rapidly outdated, because as threats develop the utility of each protection is likely to fluctuate.

Other methods considered include one inspired by a NIST SP 800-30 Guide for Conducting Risk Assessments, which discussed the futility of trying to establish or control effectiveness of a countermeasure because of the likelihood of decreasing efficacy over time. The guide noted that mitigation of this challenge requires continual risk assessments and a flexible organisational security posture. Acknowledgement of this uncertainty is helpful for users, and the resource notes that this can be communicated in various ways, including "[1.] by expressing results qualitatively, [2.] by providing ranges of values rather than single values for identified risks, or [3.] by using a visual representations of fuzzy regions rather than points."[1000] The first of these options was chosen for this research, as the latter two methods are too dependent on the exact nature of the threat scenario, and would change too rapidly for the framework to remain useful in its first iteration.

Another method that was considered was to change the column to "time frame within which the protection is effective" (i.e. immediate, mid-term, long-term), but this would be both variable and subjective. There was also the potential for looking at the column in terms of likelihood of materialisation of an exact worst-case scenario threat from the threats categorisation, but this seemed too inflexible. To maximise utility to lay users, these alternatives informed the structure of the feasibility column, separate from the functions column.

[999] Ahmad, A., Maynard, S.B. & Park, S. Information security strategies: towards an organizational multi-strategy perspective. J Intell Manuf 25, 357–370 (2014). https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/s10845-012-0683-0.
[1000] NIST Joint Task Force Transformation Initiative (2012) *Guide for conducting risk assessments*. 0 ed. NIST SP 800-30r1. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-30r1.

8.2.1.4 Defining "Beneficiaries of these countermeasures" (column 6)

Column five identifies the most likely beneficiary of a given protection, i.e. whether the protection/mitigation is intended to help an individual, a news organisation (both newsroom and business sides), or the news media existentially. Given the overwhelming amount of negatively-phrased cyber security advice available for journalists[1001], it was important for this toolkit to be as encouraging as possible in its wording to increase its likelihood of use. The framework therefore refers to "beneficiaries," as these can be more broadly classified and clearly denote a positive outcome for those affected by the protection. This column was included in the framework because sources such as SANS have noted that the first step of practical risk analysis is to make a list of what needs to be protected.[1002] While it is difficult for all members of the media to be able to identify and list technological assets, there is a higher likelihood that they will recognise the importance of improving the security status of the beneficiaries in the framework. By identifying what needed to be protected, the beneficiaries of each countermeasure were inferred, which was considered to be more useful information for members of the media than enumerating possible assets. As will be discussed in Chapter 9, recognising beneficiaries should help to increase buy-in from the industry.

In deciding on this language, other cyber security frameworks that focus on the identification of vulnerabilities and assets were considered.[1003] However, given the specific needs of the user population discussed above and in Chapter 7, the word beneficiaries was chosen to distinguish between three options: First, "vulnerabilities" which may not be exploited. Second, "assets" which may not be relevant[1004]. Third, "targets" which have connotations relating to external threats[1005], thus linking the protections back to the threats categorisation's content but not focusing enough on the potential benefits of the protections.

Some of the countermeasures aim to change legislation and/or policy (through collective action)[1006] so their scope covers the future of press freedom, thus the final level (the news media) was chosen as the beneficiary in these instances. Further, Bellman and van Oorschot note that actions that would affect the existential status of a target community (such as legal and policy recommendations) are important inclusions in best practice proposals, particularly low-cost, highly protective practices that could easily be mandated through government regulation.[1007]

[1001] Berdan K (2021) *CLTC Report: An Evaluation of Online Security Guides for Journalists*. 20 January. California, USA: CLTC UC Berkeley Center for Long-Term Cybersecurity. Available at: https://cltc.berkeley.edu/2021/01/20/cltc-report-an-evaluation-of-online-security-guides-for-journalists/ (accessed 1 March 2021); Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies, Henrichsen, Jennifer R, Routledge, Digital journalism, 2020-03-15, Vol.8 (3), p.328-346

[1002] SANS Institute (2009) Practical Risk Analysis and Threat Modeling Spreadsheet. In: *SANS Cyber Defense*. Available at: https://www.sans.org/blog/practical-risk-analysis-and-threat-modeling-spreadsheet/ (accessed 13 October 2021).

[1003] Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 2020, 12, 157. https://doi.org/10.3390/fi12090157.

[1004] Chen J and Urquhart L (2021) 'They're all about pushing the products and shiny things rather than fundamental security':Mapping socio-technical challenges in securing the smart home. *Information & Communications Technology Law* 0(0). Routledge: 1–24. DOI: 10.1080/13600834.2021.1957193.

[1005] Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies, Henrichsen, Jennifer R, Routledge, Digital journalism, 2020-03-15, Vol.8 (3), p.328-346

[1006] Chen J and Urquhart L (2021) 'They're all about pushing the products and shiny things rather than fundamental security': Mapping socio-technical challenges in securing the smart home. *Information & Communications Technology Law* 0(0). Routledge: 1–24. DOI: 10.1080/13600834.2021.1957193.

[1007] Bellman C and van Oorschot PC (2020) Best Practices for IoT Security: What Does That Even Mean? arXiv:2004.12179 [cs]. Available at: http://arxiv.org/abs/2004.12179 (accessed 7 June 2021).

8.2.1.5 Defining "Workflow phases" (column 7)

Including journalistic workflow phases as a filtering feature of the framework adds a novel and industry-specific element to this thesis and avoids repeating the threats-structure of Chapter 5 or case-study organisation of Chapters 6 and 7. Instead, it allows those insights to be combined in new ways. As a consequence, it clearly highlights the specific threats this population faces, as distinct from the general citizenry.

To ensure this framework is tailored to be more usable by the press, it was important to use a workflow that is consistent with journalistic practice.[1008] The workflow stages may occur simultaneously or discretely, depending on the organisation, the news story and the structure of the piece (e.g. long form/print, daily news, online). This approach was particularly informed by Chapter 5's conceptual IoT environment model, which demonstrates the ubiquity of the IoT without making it seem insurmountably immense by splitting it into the various locations in which devices may be found by journalists. Similarly, the intention behind the workflow phases of the framework is to allow members of each role umbrella to prioritise according to the relevant phase of the workflow,[1009] without becoming overwhelmed by the fact that IoT threats influence every stage of journalistic work.

In collaboration with the Association for International Broadcasting (AIB), a trade organisation that works with the global press, the author of this thesis (in her capacity as an analyst with the AIB) co-created a generic but flexible editorial workflow that incorporates relevant media roles at each phase. This was done by soliciting organisation-specific workflows from AIB members (news organisations around the world) and conducting thematic analysis (see: section 8.5.1) to identify key stages, core roles and the order in which these are most likely to occur. The construction of a standardised journalistic workflow was necessary because neither an academic literature search, nor leveraging professional contacts, revealed any overarching journalistic workflows. Academic literature that mentions workflows and journalism often refers to workflow as something that is specific to an individual, without noting commonalities across the industry.[1010] The AIB, which is run by former BBC executives, noted that overarching workflows were compiled by large traditional news organisations (e.g. the BBC) in the late 1980s and early 1990s. However, use of these was discontinued for various reasons, including the rise of online journalism and the perception that this rendered workflow models outdated. As a result, on 14th June 2021, the AIB asked its member organisations for their specific workflow diagrams, to compile them into an overarching industry workflow. Their final product (as-yet unpublished) is the basis of the workflow phases element of the framework, as shown below in Figure 7:

[1008] Berdan, K. (2021). CLTC Report: An Evaluation of Online Security Guides for Journalists (p. 48). CLTC UC Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/2021/01/20/cltc-report-an-evaluation-of-online-security-guides-for-journalists/; Attfield, S., & Dowell, J. (2003). Information seeking and use by newspaper journalists. Journal of Documentation, 59(2), 187–204. https://doi.org/10.1108/00220410310463860; the Finnish Lifelong Learning Foundation (KVS), Birzeit University Media Development Center (MDC), & the Finnish Ministry for Foreign Affairs. (2021). The journalistic work process. Media Guide. https://mediaguide.fi/mediaguide/the-journalistic-work-process/

[1009] Reeder, R. W., Ion, I., & Consolvo, S. (2017). 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. IEEE Security Privacy, 15(5), 55–64. https://doi.org/10.1109/MSP.2017.3681050

[1010] Attfield, S., & Dowell, J. (2003). Information seeking and use by newspaper journalists. Journal of Documentation, 59(2), 187–204. https://doi.org/10.1108/00220410310463860; the Finnish Lifelong Learning Foundation (KVS), Birzeit University Media Development Center (MDC), & the Finnish Ministry for Foreign Affairs. (2021). The journalistic work process. Media Guide. https://mediaguide.fi/mediaguide/the-journalistic-work-process/

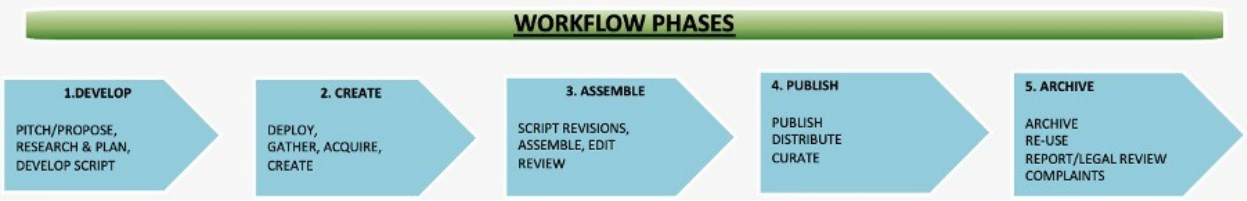


Figure 7: Editorial workflow diagram, co-created with the AIB

8.2.1.6 Defining "Role Umbrellas" (column 8)

A high-level view of media sector roles was necessary in order to assign protection considerations to the actors within the media industry to which they were most relevant. As the industry is incredibly diverse and different roles will be applicable depending on the size of the news organisation, its location and other factors, examples of common roles were grouped by their primary functionality (e.g. "Risk Management Personnel"), to ensure applicability of the framework.

As a first step towards constructing these role umbrellas, a literature search was conducted, using keywords including "role," "journalism", "media", "news organisation." These search terms were used in databases of academic literature, specifically. Google Scholar, JSTOR, and the university's SOLO search system. Each umbrella was then searched as a keyword on the publisher sites for major journalism-specific journals (SAGE, Taylor & Francis, Springer), to identify any other categories or individual roles. This search revealed that while there was some academic literature delving into the specifics of media roles, there was no agreed over-arching model this framework could draw on. For example, Lewis and Westlund explore three categories - editorial, business, technology - but they do not mention risk management,[1011] possibly because this has become much more pressing for all news organisations since their article was published in 2014.

The interviewees for the country profiles in Chapters 6 and 7 highlighted the multifaceted societal functions of news organisations. Therefore, these role umbrellas are intended to balance the need for both editorial news work roles and news organisational (business-oriented) roles (including tech/infrastructure-related roles).[1012] Further, to reflect the diversity of the journalistic ecosystem, the example roles for each umbrella must not necessarily relate to staff positions at traditional media organisations, but also germane positions at civil society organisations in this space.

Therefore, existing relationships with the AIB (mentioned above) allowed this thesis to draw on their network of journalists and media organisations around the world to collect examples of workflows used by different news institutions (see previous section) and role umbrellas for this research and other work. While individual roles may be specific to the kind of news organisation (e.g. sub-editors for print journalism, producers for broadcast journalism), through this work done by the AIB, these roles can be grouped into "role umbrellas" (e.g. "editorial/narrative producers").

There are some caveats to be considered regarding role umbrellas: for example, freelancers and citizen journalists likely come under multiple primary role umbrellas, so may be able to choose which role they are primarily inhabiting at a given time. The division of labour (and thus of primary responsibilities) will

[1011] Lewis, S. C., & Westlund, O. (2015). Actors, Actants, Audiences, and Activities in Cross-Media News Work. Digital Journalism, 3(1), 19–37. https://doi.org/10.1080/21670811.2014.927986

[1012] Cornia, A., Sehl, A., & Nielsen, R. K. (2020). 'We no longer live in a time of separation': A comparative analysis of how editorial and commercial integration became a norm. Journalism, 21(2), 172–190. https://doi.org/10.1177/1464884918779919

vary across different organisations. Still, these groupings are useful for assigning general actions to different groups, without overwhelming any one member of the media with information about security challenges and recommendations.

The role umbrellas are as follows, with the footnotes indicating literature that supports the idea of this as a role category that is relevant to journalism:

- Risk Management Personnel[1013] [1014]
    - Examples of specific roles under this umbrella include: media lawyers, technical security specialists, information security technologists, digital and physical security trainers, crisis response managers, CISOs, risk assessors.
- Editorial/Narrative Producers[1015] [1016]
    - Examples of specific roles under this umbrella include: Sources (including news agencies (although these are external suppliers to the process)), journalists, editors (including programme editors), producers, heads of development, researchers, directors, social media managers.
- Business/Corporate/Commercial/Organisational Stakeholders[1017] [1018]
    - Examples of specific roles under this umbrella include: Media organisation owners, CEOs, CFOs, CIOs, accountants, advertisers, audiences, technologists such as Cloud and back-end developers, content distributors, platform agents, financial staff, corporate lawyers (e.g. mergers and acquisitions).
- Technical Operators[1019] [1020]
    - Examples of specific roles under this umbrella include: directors of photography, satellite and communications engineers, picture editors, camera operators, sound recorders, vision and sound mixers, digital media technologists, archivists (stills and video tech library managers), production staff (e.g. floor management, gallery production assistants, other technical operators).

8.2.1.7 Defining "Feasibility" (column 9)

Feasibility can help members of the press to make the decision about which countermeasures to implement first, or at all. According to Saltzman and Stevens *et al.*, feasibility is "operationalised in terms of the time it took to use the tool [here, to implement a countermeasure], as well as the perceived ease of use."[1021]

[1013] Henrichsen, J. R. (2021). Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". Journalism Practice, 0(0), 1–20. https://doi.org/10.1080/17512786.2021.1927802

[1014] Mythen, G. (2010). Reframing risk? Citizen journalism and the transformation of news. Journal of Risk Research, 13(1), 45–58. https://doi.org/10.1080/13669870903136159

[1015] Duffy, A. (2021). Out of the shadows: The editor as a defining characteristic of journalism. Journalism, 22(3), 634–649. https://doi.org/10.1177/1464884919826818

[1016] Lewis, S. C., & Westlund, O. (2015). Actors, Actants, Audiences, and Activities in Cross-Media News Work. Digital Journalism, 3(1), 19–37. https://doi.org/10.1080/21670811.2014.927986

[1017] Cornia, A., Sehl, A., & Nielsen, R. K. (2020). 'We no longer live in a time of separation': A comparative analysis of how editorial and commercial integration became a norm. Journalism, 21(2), 172–190. https://doi.org/10.1177/1464884918779919

[1018] Milosavljević, M., & Vobič, I. (2019). 'Our task is to demystify fears': Analysing newsroom management of automation in journalism. Journalism, 1464884919861598. https://doi.org/10.1177/1464884919861598

[1019] Witschge, T., Anderson, C. W., Domingo, D., & Hermida, A. (2016). The SAGE Handbook of Digital Journalism. SAGE.

[1020] Westlund, O., & Krumsvik, A. H. (2014). Perceptions of Intra-Organizational Collaboration and Media Workers' Interests in Media Innovations. The Journal of Media Innovations, 1(2), 52–74. https://doi.org/10.5617/jmi.v1i2.858

[1021] Saltzman DL (2014) *Examining the Feasibility of the Nisonger Outcome Assessment Tool*. PhD thesis. The Ohio State University, Ohio, USA. Available at: https://etd.ohiolink.edu/apexprod/rws_olink/r/1501/10?clear=10&p10_accession_num=osu1397221453 (accessed 19 January

Regarding the framework of countermeasures, ease of use relates to both potential confusion and difficulty associated with the task, i.e. both cost and knowledge.[1022] Time taken can vary depending on the function of the countermeasure and its beneficiaries. Estimated feasibility of countermeasures used in this framework follows Saltzman's 1-5 numbered scale, but adds written descriptors to each number to assist user interpretation.[1023] This decision to include categories that can be used to alter the structure of the framework through filtering, in addition to a numbered scale, was informed by the SANS CIS Controls emphasis on effective prioritisation.[1024] For this thesis, countermeasures were therefore grouped according to estimated feasibility and each category was matched to a point on this scale. The assigned feasibility values were validated through Likert Scale questions in the surveys sent to both media experts and cyber security experts (see section 8.2.3.2), because feasibility is a relative concept.

For this framework, these categories are:

1. "Quick win" (i.e. controls that can be swiftly* implemented)
2. "Mid-term effort" (i.e. takes months)
3. "Long-term effort" (i.e. this work is unlikely to ever be finished)
4. "Collective win" (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat)
5. "Unicorn" (i.e. unlikely to be worth time and effort in most circumstances). Although the toolkit in this thesis advocates for individualised risk assessments, this method of filtering enables perpetually useful actions to be undertaken regardless of the specific risk model.

*There is an implication, given the next level up is "takes months," that the "Quick win" category refers to countermeasures that can be implemented within a month. Although the word "swiftly" can be interpreted subjectively, experts were asked what they would change (both in the pilot study and in the final validation study), and they did not contest this phrasing, or ask for more specificity. See also the discussion of feasibility and benefit in section 9.5 of Chapter 9.

8.3 Framework contents

The framework itself is submitted alongside this thesis as a supplementary document in the form of an Excel spreadsheet. It can also be found here and in Appendix L (as a static version). This section will describe in detail the process by which each column was filled, and the content options. Table 16 (below) shows the top part of the framework, demonstrating all columns and the first row of content as a visual aid for how the information is organised:

2022); Stevens A, Beurskens A, Köke A, van der Weijden T (2013) The use of patient-specific measurement instruments in the process of goal-setting: a systematic review of available instruments and their feasibility. *Clinical Rehabilitation* 27(11): 1005–1019. DOI: 10.1177/0269215513490178.

[1022] Saltzman DL (2014) *Examining the Feasibility of the Nisonger Outcome Assessment Tool*. PhD thesis. The Ohio State University, Ohio, USA. Available at: https://etd.ohiolink.edu/apexprod/rws_olink/r/1501/10?clear=10&p10_accession_num=osu1397221453 (accessed 19 January 2022).

[1023] Saltzman DL (2014) *Examining the Feasibility of the Nisonger Outcome Assessment Tool*. PhD thesis. The Ohio State University, Ohio, USA. Available at: https://etd.ohiolink.edu/apexprod/rws_olink/r/1501/10?clear=10&p10_accession_num=osu1397221453 (accessed 19 January 2022).

[1024] Tunggal AT (2021) What are the CIS Controls for Effective Cyber Defense? In: *UpGuard*. Available at: https://www.upguard.com/blog/cis-controls (accessed 13 October 2021).

#	Countermeasures (Protections & Mitigations)	Disadvantages to each countermeasure	Threats addressed by each countermeasure	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?)	Phase(s) of the editorial workflow to which this countermeasure is most relevant	Media roles that are most likely to be responsible for implementation of this countermeasure	Feasibility of implementation of the countermeasure
A	**Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.**	Relies on ability to opt-out of interaction with the IoT Resource-intensive and time consuming Increases likelihood of successful physical theft of information Device functionality and so benefits of the IoT will be lost when the countermeasure is in force	Warrantless bulk data purchase Abusing health and biometric information Third party supply chain actors accessing data Abuse of data and privacy laws SOCMINT and IoT interrogation by law enforcement Data linkage and aggregation Informal additions to state surveillance networks Data manipulation as a result of consent requirements Sensor-level attacks on data confidentiality or integrity Predictive analysis of location data to facilitate physical attacks Continuous surveillance Weaponisation of financial penalties Hijacking connected social	Prevention (PREV)	Individual members of the press and their sources	Stage 2: Deploy, Gather, Acquire, Create	Editorial/Narrative Producers (inc. Programme Editors)	1. “quick win” (i.e. controls that can be swiftly implemented)

			media and communications accounts Botnet creation Denial of Service attacks Manipulation of devices' physical activities Data harvesting from decommissioned devices Altering user-facing device and data attributes Voice stealing					

Table 16: Demonstration of the first two rows of the framework

8.3.1 Column 2: Countermeasures (and their assigned letter label in column 1)

Qualitative data used to populate the countermeasures column were contributed by participants across all four validation surveys, as the experts were asked for their thoughts on each countermeasure and how they could/should be amended to make them more useful to journalists. The suggested edits and any relevant comments relating to countermeasures by respondents from all the surveys were consolidated, so that they could be collectively reviewed and contrasted in order to decide what to change about each countermeasure. For more details on data collection and expert recruitment for the content of this framework, see Chapter 3.

Additionally, the states' capabilities survey asked experts to assign each countermeasure scores reflecting its current and future utility. The decision was made to find the median of these scores because the response options on these topics were not open-ended but were instead a numbered scale of discrete responses (1-5, where each number had an assigned qualitative value, see Appendix K for details). The label accompanying the number 3 was always "Not sure/don't know", with 4 and 5 being more confident positive responses. The median score was used to determine which countermeasures, if any, fell to 3 or below. A value below this threshold meant that the countermeasure needed to be reconsidered and/or rewritten to make it clearer and/or more useful against the states' capabilities that could be used to enact IoT threats against journalists. This method was also used to analyse expert responses for other columns in the framework, see sections 8.3.3, 8.3.5, and 8.3.6.

The median was chosen, rather than the mean, to avoid outliers skewing data and therefore to prevent any single expert's knowledge or perspective from disproportionately influencing the results of the survey. Medians also simplify any further analysis. This latter reason was chosen because using the mean could have created fractional values from the 1-5 number scale used, and interpreting the difference between a 3.4 and a 3.8 would have been more speculative than assessing the difference between integer values. As there was an odd number of states' capabilities survey participants, the median countermeasure values were always integers. The modal value was not used as the mode is particularly useful for summarising categorical variables.[1025]

Based on the responses relating to countermeasures across all four surveys, one countermeasure (the original countermeasure #4) was cut, two countermeasures (originally #5 and #10) were consolidated into one new countermeasure (D), the phrasing of 11 countermeasures were amended and six remained unchanged. In order to ensure clarity through the analytical process, the revised countermeasures that now comprise the framework have alphabetical designations, to differentiate from the numbers used in the initial list of countermeasures (see: Table 17).

The original countermeasure 4 was "Travelling without local storage: Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control." Media expert responses noted that the countermeasure needed to take account of flaws in this plan, such as: "availability of secure internet could make this impossible in some countries",

[1025] Government of Canada (2021) Measures of central tendency: Calculating the mode. Available at: https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch11/mode/5214873-eng.htm (accessed 13 September 2022).

“some people might assume it's BETTER to store something locally to avoid Internet threats”, and the level of feasibility of this idea “in situations where the Internet isn't available”. This countermeasure was deleted because, in addition to these critiques by media experts, only two threats were matched to this countermeasure by two cyber security experts. This showed that it was neither a particularly relevant countermeasure from a cyber security perspective, nor from a media user point of view.

The new countermeasure D was created by merging two old countermeasures. These were: “Network segmentation: Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices” and “Wi-Fi security: Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.” States’ capabilities experts gave both countermeasures the same scores regarding current and future utility. Further, three different media expert answers indicated that participants found it hard to comprehend the technical nuances of these countermeasures, with suggestions such as “Explain the reason for the countermeasure” and “Eventually it would be helpful to include a step-by-step guide for how to carry out the countermeasure, for cases in which editorial staff might have to do it themselves”. Therefore, these two were consolidated into one new countermeasure, D: “Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).”

One example of how a countermeasure was amended to take into account expert feedback was countermeasure A. The original countermeasure 1 was: “Limit connectivity: Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.” One media respondent said “Rely[ing] primarily on analogue methods of journalism [...] is not possible in this day and age,” while another said “Define ‘interaction’ and add the option of using digital voice recorders that aren't connected to the Internet. (Recording interviews is a legal/ethical requirement for some newsrooms.)” As a result, this countermeasure was updated to: “Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.”

Another notable amendment was the original countermeasure 19: “Legal scrutiny: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.” Although no media experts said that this needed changing, one cyber security expert noted that “legal scrutiny doesn't necessarily result in more favourable laws. Just as possible that more restrictive/opaque clauses are brought in instead.” Further, the Media Freedom Coalition legal panel group of 52 countries is working to draw up proforma media freedom legislation.[1026] To encourage more use of such proforma legislation and similar work, this has become countermeasure Q: “Legal scrutiny in favour of press freedom: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of

[1026] Media Freedom Coalition (2022) Coalition Objectives. Available at: https://mediafreedomcoalition.org/about/objectives/coalition-objectives (accessed 13 September 2022).

Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc. A motivating factor behind the scrutiny should be the risk posed by these clauses to press freedom."

A third example of an amended countermeasure is the original #20, which was clarified per requests from both media and cyber security expert respondents. This was: "No clear countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities." However, media experts noted, for example, that "It's unclear here who the journalist is reporting to -- their own tech team? Outside research orgs? Tweeting about it?" The cyber security experts seemed to view #20 as "non-IoT-specific cyber security", rather than no cyber security at all, as evidenced by the comment "With no specific countermeasure, it may be hard to target threats and mitigate them". This was changed to countermeasure R: "No clear IoT-specific countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. With no specific countermeasure, it may be hard to target threats and mitigate them. However, it is important that journalists draw attention to these threats as much as possible, so that there is a sense of urgency to address them."

See Table 17 (below) for comparison of old and new countermeasures:

Old countermeasures used in surveys (see: Appendices H, I, J, and K for full details)	**New countermeasures (after survey analysis)**
(1) Limit connectivity: Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.	(A) Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.
(2) IoT-free contingency plans: Push for media stakeholders (e.g. news organisations) to create emergency/contingency plans that do not involve Internet of Things devices. These plans should acknowledge the risks associated with reliance on such devices to, for example, keep track of correspondents in dangerous environments.	(B) IoT-free contingency plans: Encourage media stakeholders (e.g. news organisations) to ensure that their emergency/contingency plans do not rely on Internet of Things devices.
(3) Transparency reporting: Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices about device purchasing and can warn their sources about these devices.	(C) Transparency reporting: Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices and can warn their sources. This countermeasure could also include

	news organisations reporting on these lists so that their audiences, including their sources, can also make informed decisions.
(4) Travelling without local storage: Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control.	NONE
(5) Network segmentation: Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices. *AND* (10) Wi-Fi security: Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.	(D) Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).
(6) Aesthetic disguises: Consider employing some methods of hiding one's face in ambient settings, through make-up, masks, clothing choices, etc.	(E) Aesthetic disguises: Consider employing some methods of hiding one's face to protect against video-equipped devices in public spaces. For example, this can be done through make-up, masks, and/or clothing choices. If this is done, consider other ways of verifying one's identity when meeting with sources.
(7) Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces. [UNCHANGED]	(F) Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.
(8) Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities. [UNCHANGED]	(G) Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.
(9) Stronger passwords: Internet of Things devices should not have default passwords (this is both an individual responsibility to change passwords upon purchase of a device, and also a necessary legislative shift to make sure that devices all have	(H) Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by

distinct default passwords)	a legislative shift to make sure that devices all have distinct default passwords.
(11) Collaborative technology design: News organisations and media-related civil society organisations could fund and collaborate with cyber security researchers and designers on the creation of cutting-edge intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become mandatory within press institutions.	(I) Collaborative technology design: News organisations and media-related civil society organisations could collaborate with cyber security researchers and designers on the creation of cutting-edge, open and transparent standards for IoT protection. For example, developing intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become adopted within press institutions.
(12) Firewalls: If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines. [UNCHANGED]	(J) Firewalls: If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.
(13) Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device. [UNCHANGED]	(K) Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.
(14) Block the signal: Faraday bags can be used to transport devices or temporarily block Internet of Things device capabilities.	(L) Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).
(15) Research device security: As with smartphones, if an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. If an individual member of the press must frequently use or be in spaces where Internet of	(M) Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. They should research communications protocols and vulnerabilities of these devices, and should

Things devices exist, they should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.	attempt to change or remove these devices as soon as public vulnerabilities become known.
(16) Intelligence sharing: Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). Their goal is to share information on topics from best practices to threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.	(N) Intelligence sharing: Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). These groups can share information on topics including best practices and threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.
(17) Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours. [UNCHANGED]	(O) Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.
(18) IoT-specific risk assessments: Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats. [UNCHANGED]	(P) IoT-specific risk assessments: Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.
(19) Legal scrutiny: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.	(Q) Legal scrutiny in favour of press freedom: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc. A motivating factor behind the scrutiny should be the risk posed by these clauses to press freedom.
(20) No clear countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as	(R) No clear IoT-specific countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. With no specific countermeasure, it may be hard

possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.	to target threats and mitigate them. However, it is important that journalists draw attention to these threats as much as possible, so that there is a sense of urgency to address them.

Table 17: Conversion of old countermeasures to new countermeasures

8.3.2 Column 3: Disadvantages to each countermeasure

From the survey results, a spreadsheet was created that cross-referenced the list of countermeasures with the range of disadvantages participants could choose from. These disadvantages were from the survey questions and from write-in responses by participants.

Using these results, the individual comments about disadvantages were grouped into categories to enable filtering of results in the framework. For example, relating to countermeasure J (formerly #12), disadvantages suggested by cyber security experts included: "This doesn't stop determined attackers from hijacking PCs in the US or Canada to carry out their work", "Relatively easy to rent server time, or make use of botnet hosts, in specific countries that are permitted through the firewall block", and "North Korea operates out of every country but NK". These suggested disadvantages were grouped and renamed "Geofencing is generally considered weak protection against attacks launched via proxy."

Similarly, the disadvantages "The purpose of some IoT technologies, such as fitness trackers, is to continually collect data. Therefore, disconnecting them and disabling their function would ultimately render them less useful" and "Some functionality might be lost if the network is segmented" were consolidated under the new label: "Device functionality and so benefits of the IoT will be lost when the countermeasure is in force", thereby enabling this disadvantage to be assigned to multiple countermeasures (A and D). As original countermeasures 5 and 10 were merged, their individual disadvantages were allocated to the new combined countermeasure. These refined disadvantages became column 3 of the framework, see below for a list of disadvantages:

- Relies on ability to opt-out of interaction with the IoT
- Resource-intensive and time consuming
- Increases likelihood of successful physical theft of information
- Relies on people obeying the law
- Difficulty enforcing for all necessary users.
- Ad hoc solution that requires training for sustained use
- Increased information available for attackers about which companies hold specific data types
- Deleted data can be recovered
- Device functionality and so benefits of the IoT will be lost when the countermeasure is in force
- Not possible for every type of IoT device
- Works against (some) machines, but unlikely to slip past human analysts
- Under-researched technology, not proven to work
- More passwords for individuals to manage
- Companies are only beginning to provide this service
- Geofencing is generally considered weak protection against attacks launched via proxy.
- Requires technical skills
- You cannot know all the scanners/websites that are indexing your devices
- Not possible for bystanders

- Long-term goal
- Risk assessments are administrative burdens

8.3.3 Column 4: Threats addressed by each countermeasure

For the threats column, cyber security expert participants were asked to match countermeasures to a list of threats. This was necessary to enable users to build upon the knowledge in Chapter 5, moving from risk assessment to risk management. States' capabilities experts were also asked to rate threats in terms of their current and future realism, in the same manner as they rated the current and future utility of the countermeasures, see section 8.3.1.

However, due to the time needed to recruit participants to these intensive validation surveys, by the time of data collection, the threats included in the survey questions were outdated, as they were forms of threats created as part of an old draft of Chapter 5's threats categorisation (see: Appendix D). The new threats categorisation was peer reviewed and published during the period when the surveys were open, so the analysis of these survey results first included converting the threats into the new threats from the new categorisation (see Table 18).

If there was a change of wording between the old threats and their new threat, this change did not affect the meaning of the survey questions for three reasons. First, some threats did not change their title wording at all, and had minimal updates to description wording. Second, some threats had new titles (e.g. "Peer-to-peer networks" became "Third party supply chain actors accessing data"), and had more information added to the description, but retained their original meaning.

Third, some threats became combinations of different old threats: e.g. the survey had Threat A, Threat B, and Threat C, but they were all combined in the new threats categorisation as Threat 1. For example, "Poor encryption" and "Botnet creation and use" were combined under the new threat title "Botnet creation" because of overlaps in their original descriptions, namely that lax encryption can lead to botnet creation. Other elements of the "Poor encryption" description were used to build the new "Networked Device Threats" category description. Additionally, "Poor encryption" can be the result of a "Regulatory gap" (a new category), and is the basis for multiple different threats, so having a single threat named "Poor encryption" seemed unnecessary. Table 18 demonstrates the conversion from old threats (see: Appendix D) to new threats (see: Chapter 5).

Alternatively, some threats ("Computer Network Exploitation by state agencies," "Elevation of Privilege attacks", and "Exploitation of multiple devices to start and escalate an attack") were also combined into the new "Networked Device Threats" category description, rather than into individual threat examples. Their scores were therefore ignored because each individual new threat has its own cumulative score.

Old threat title used in survey (see: Appendix D for full details)	**New threat title (see: Chapter 5)**
Peer-to-peer networks	Third party supply chain actors accessing data
Weak authorisation protocols facilitating third party data manipulation AND Consent requirements that include data manipulation	Data manipulation as a result of consent requirements

Visual displays AND Involuntary data access AND Device seizure AND Dumpster diving	Data harvesting from decommissioned devices
Poor encryption AND Botnet creation and use	Botnet creation
Legitimate interest clauses	Abuse of data and privacy laws
Data breach financial repercussions AND Ransomware	Weaponisation of financial penalties
Warrantless bulk data purchase AND Using historical datasets for identification and financial gain	Warrantless bulk data purchase
Eavesdropping for identification and profiling AND Doxxing and stalking	Continuous surveillance
Altering health data AND Using health information to cause psychological pressure	Abusing health and biometric information
Profiling to cause identity theft and financial damage AND Data linkage and aggregation AND Pattern of life recognition and predictive analysis	Data linkage and aggregation
Informal additions to state surveillance networks	Informal additions to state surveillance networks
SOCMINT and IoT interrogation by law enforcement	SOCMINT and IoT interrogation by law enforcement
Predictive analysis of location data to facilitate physical attacks AND Real-time vehicular hacking and tracking	Predictive analysis of location data to facilitate physical attacks
Information Damage Level attacks against data confidentiality or integrity AND Sybil attacks against data integrity	Sensor-level attacks on data confidentiality or integrity
Falsifying timestamps to impede forensics AND Altering user-facing device and data properties to put psychological pressure on journalists AND Clock skewing AND Spoofing to stop device actions	Altering user-facing device and data attributes
Hijacking connected accounts AND Restrictive laws relating to ‘fake news’	Hijacking connected social media and communications accounts
Malware-induced kinetic attacks AND Aggressive vehicular takeover AND Changing the settings of essential devices	Manipulation of devices' physical activities

Rerouting attacks AND Replay attacks to manipulate devices with audio activation	Voice stealing
Restricting internet access AND Denial of Service attacks	Denial of Service attacks

Table 18: Conversion of old threats to the new threats categorisation

Additional changes were made to the threats following the expert validations. For example, "Laser modulation to cause device activity" was cut from the final list of threats because it was deemed to be too niche and more akin to a hypothetical consequence than a threat, and because states' capabilities respondents assigned it an average of 3 in both current and future threats, indicating that they did not know if it was realistic. "5G and increased portability of devices" was also cut because this is a detail about the IoT market that is discussed briefly in the country profiles in Chapters 6 and 7, but is more of an overarching factor affecting threats than a threat itself. Finally, "Normalisation of monitoring of employees causing a decrease in reporting quality" was cut because it is a threat that is easily conducted via multiple non-IoT methods, and has a specified consequence in the threat that makes it more rigid than other descriptions.

States' capabilities expert scores were assigned, and the decision was taken to use the median of the participant scores for each threat for the same reasons as were stated in the Countermeasure column subsection (see: section 8.3.1). This did not significantly alter the overall realism score of each threat, either in terms of the current or the future perception. For the new countermeasure D that merged #5 and #10, the medians of their threats matching scores were taken individually, and then the median of those two results was taken in order to produce a combined result.

As some new threats were composites of even numbers of old threats, some of the new threats' realism scores were not integers but instead had a decimal of 0.5 (i.e. 4.5). Changes between current and future scores were only considered significant if there was an integer difference (1 or greater). This is done instead of rounding up the decimals because rounding up the decimals would cause a change from 4 in current to 4.5 in future to appear to be an increase from 4 to a 5, while a change from 4.5 in current to 5 in future would appear to be stable from 5 to 5, and it is inconsistent to have the 0.5 difference mean two different things.

Any threats that received votes from at least half of the cyber security experts (i.e. two or more votes) were matched to their relevant countermeasures and were used to populate the Threats column.

8.3.4 Column 5: Function of countermeasure

One of the cyber security expert surveys explained that there are lots of potential angles to take in determining how to best explain how a countermeasure will mitigate a specific threat: one way is to group countermeasures into categories by similar functionalities. To build on existing research as a foundation for these categorisations, the functions assigned to each countermeasure are categories created by Ahmad *et al.*[1027] Functions 1-6 (PREV to DECEP) are temporal, while 7-9 (PERI to LAYER) are spatial. See section 8.2.1.3 for a full discussion of this choice, as a reminder the list is:

[1027] Ahmad, A., Maynard, S.B. & Park, S. Information security strategies: towards an organizational multi-strategy perspective. J Intell Manuf 25, 357–370 (2014). https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/s10845-012-0683-0.

1. “Prevention (PREV): Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure
2. Deterrence (DETER): Deterrence employs disciplinary action to influence human behavior and attitude
3. Surveillance (SURV): Surveillance is the systematic monitoring of the security environment towards developing situational awareness to assist in adapting to fast-changing circumstances and threats
4. Detection (DETECT): Detection is an operational-level strategy aimed at identifying specific security behavior
5. Response (RESP): Response takes appropriate corrective actions against identified attacks
6. Deception (DECEP): Deception distracts an attacker’s attention from critical information assets using decoys thereby leading the attacker to waste time and resources
7. Perimeter defense (PERI): Perimeter defense creates a boundary around information assets that is secured by regulating traffic at every incoming and outgoing information channel (choke points)
8. Compartmentalization (COMP): Compartmentalization reduces an attacker’s opportunities by dividing the intended area of attack into zones that are secured separately
9. Layering (LAYER): Layering uses multiple countermeasures that function independently but increases the effectiveness of the defense when working together thereby posing a series of challenges to the attacker. The defensive system is designed to be resilient by overlapping the series of countermeasures, whereby each countermeasure complements the next so that if one fails another will back it up.”[1028]

Respondents were asked to assign each countermeasure the function that they considered to be most accurate and were given an opportunity at the end of this survey to provide feedback on these function categories and the countermeasures themselves. No experts chose to comment on function categorisations at the end of the survey, suggesting their approval of the categories.

The functions used to populate the column were assigned according to the modal vote per countermeasure, i.e. if a category got two or more votes, that was the assigned function type for the given countermeasure. If there was not a single modal response, then the most common tied responses were input. The modal response was chosen because the answer options were largely qualitative and so could not be averaged.

Two of the original countermeasures (#15 and #18) got four different votes for types of function. One countermeasure (#10) got two different votes for types of function. However, countermeasures #5 and #10 were merged and the clear modal outcome was assigned to the new countermeasure (D). For these three countermeasures, all functions that were given by respondents became the assigned functions.

8.3.5 Column 6: Beneficiary

Media experts were asked to assign a beneficiary of each countermeasure from a multiple choice list. The question was: “Which of the following options is this countermeasure intended to help?” The available options were: an individual; a news organisation as a business; and/or the news media existentially.

When analysing the raw data, the first of the options was amended to better reflect survey feedback, as a respondent repeatedly insisted that “sources” are potential beneficiaries of journalistic security

[1028] Ahmad, A., Maynard, S.B. & Park, S. Information security strategies: towards an organizational multi-strategy perspective. J Intell Manuf 25, 357–370 (2014). https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/s10845-012-0683-0.

measures. One piece of survey feedback was: “To me, if the beneficiary is the journalist, it's also the source since that is who we are required to protect.” This caused the “individual members of the press” beneficiary option to be changed to “individual members of the press and their sources.”

For this column, as with the workflow phases and media roles columns, the content used to populate the framework was comprised of the beneficiaries that had the most votes from respondents for each countermeasure. For countermeasure D, the median of the results for #5 and #10 was taken in order to produce a result for each beneficiary.

8.3.6 Column 7: Phase(s) of the editorial workflow to which this countermeasure is most relevant

For the workflow phases column of the framework, scores were given based on how many media expert respondents assigned each workflow phase to each countermeasure. Again, countermeasure D required taking the median of the scores assigned to countermeasures #5 and #10. The column was filled out using the workflow phases that had the most votes from respondents for each countermeasure.

Three countermeasures (old 1, 6 and 7) had top votes for “Stage 2: Deploy, Gather, Acquire, Create”. However, for the majority of countermeasures, the response with the most votes was "All of the above/This countermeasure is an action that exists in parallel with the editorial workflow". To make the column more effectively searchable, this label was removed and instead the relevant cells just listed all stages for each relevant countermeasure. See section 8.2.1.5 for details on how the workflow stages were created, with the Association for International Broadcasting. They are as follows:

1. Develop: Pitch/propose, research & plan, develop script
2. Create: Deploy, gather, acquire, create
3. Assemble: Script revisions, assemble, edit, review
4. Publish: Publish, distribute, curate
5. Archive: Archive, re-use, report/legal review complaints

8.3.7 Column 8: Category of media roles that is most likely to be responsible for implementation of this countermeasure

Role umbrella categories can be found in section 8.2.1.6 of this chapter. For this column, each role umbrella was given scores based on how many media expert respondents assigned the roles to different countermeasures. As before, countermeasure D took the median of the scores assigned to countermeasures #5 and #10. The content of this column was formed of the role umbrellas that had the most votes per countermeasure.

Three countermeasures had a tie for the most votes for different role umbrellas, so all tied options were included in the framework. First, old countermeasure #9 (which became H) had three votes each for “Editorial/Narrative Producers (inc. Programme Editors); Technological Editorial Contributors”. Similarly, old countermeasure #15 (which became M) had 3 votes each for “Risk Management Personnel; Business/Corporate/Commercial/Organisational Stakeholders”. Finally, countermeasure D had two votes each for three options (“Risk Management Personnel; Business/Corporate/Commercial/Organisational Stakeholders; Technological Editorial Contributors”).

8.3.8 Column 9: Feasibility of the countermeasure

The categories of feasibility given in the framework are as in section 8.2.1.7. Both cyber security and media experts were asked their opinions of the level of feasibility of each countermeasure. These two sets of responses were combined, because the media experts were expected to best know what would be feasible in their own industry, and the cyber security experts were expected to best know how feasible such countermeasures are in general.

As with the "function of countermeasures" column, feasibility of countermeasures options are qualitative and so the column is also populated with modal responses. Some countermeasures had multiple modal responses. For example, two countermeasures (#16 and #20) got two different votes for which category of feasibility they should fall into. Another countermeasure (#1) got four different votes for the category of feasibility. For these three countermeasures, all feasibility categories that were given by respondents became the assigned feasibility.

One countermeasure (#20) did not have a decisive outcome; the modal votes overall were for: "2. "mid-term effort" (i.e. takes weeks to months), 3. "long-term effort" (i.e. this work is unlikely to ever be finished), and 4. "collective win" (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat)". For this countermeasure, modal votes within both types of experts were also conflicted. Cyber security experts tied on "3. long-term effort (i.e. this work is unlikely to ever be finished)" and "5. unicorn" (i.e. unlikely to be worth time and effort in most circumstances)". Media experts tied on "2. mid-term effort (i.e. takes weeks to months) and "4. collective win (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat)".

For other tied modal responses, the response used to populate the column was chosen to be the modal option said by the media experts, as they are the framework's target audience. However, the modal response given by the cyber security experts (3) was chosen because it is true that the work of finding all IoT countermeasures is unlikely to ever be completed. Further, the cyber security experts were likely to have a more accurate idea of how long it takes to develop these countermeasures.

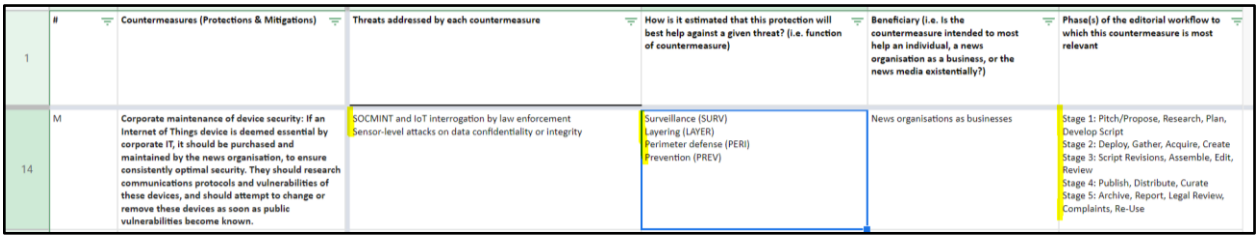
8.4 Using the framework

The structure of the framework, linked here, is as follows:

1. Countermeasures (Protections & Mitigations) (column 2)
2. Disadvantages to each countermeasure (column 3)
3. Threats addressed by each countermeasure (from the threats categorisation) (column 4)
4. How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure) (column 5)
5. Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?) (column 6)
6. Phase(s) of the editorial workflow to which this countermeasure is most relevant (column 7)
7. Category of media roles that is most likely to be responsible for implementation of this countermeasure (column 8)
8. Feasibility of the countermeasure (column 9)

This tool was designed to be used online, with interactive features, in order to address the diverse needs of journalists. For ease of observation, however, given the requirements of this thesis, the framework has also been supplied in full in static form in Appendix L. In its online, dynamic, interactive, and multi-use

form, this framework spreadsheet uses filters. Some countermeasures were assigned multiple answers in the same column. To ensure that these are still filterable by each individual answer, all answers were put into the same cell, as demonstrated in Figure 8.



	#	Countermeasures (Protections & Mitigations)	Threats addressed by each countermeasure	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?)	Phase(s) of the editorial workflow to which this countermeasure is most relevant
1						
14	M	**Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.**	SOCMINT and IoT interrogation by law enforcement Sensor-level attacks on data confidentiality or integrity	Surveillance (SURV) Layering (LAYER) Perimeter defense (PERI) Prevention (PREV)	News organisations as businesses	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use

Figure 8: Demonstration of multiple options within the same cell

Each column is topped with a filter icon that opens a menu, which allows filtering by “values” (the default) and “condition.” Choosing “filter by condition” and then selecting “text contains” allows filtering for a specific answer. For example, the countermeasure “IoT-specific risk assessments” has four assigned functions (“Surveillance (SURV), Prevention (PREV), Response (RESP), Layering (LAYER)”); searching for all answers containing LAYER ensures that this cell is included in the search results. However, if “filter by value” was used, that countermeasure wouldn't show up because there is more than one answer in the same cell.

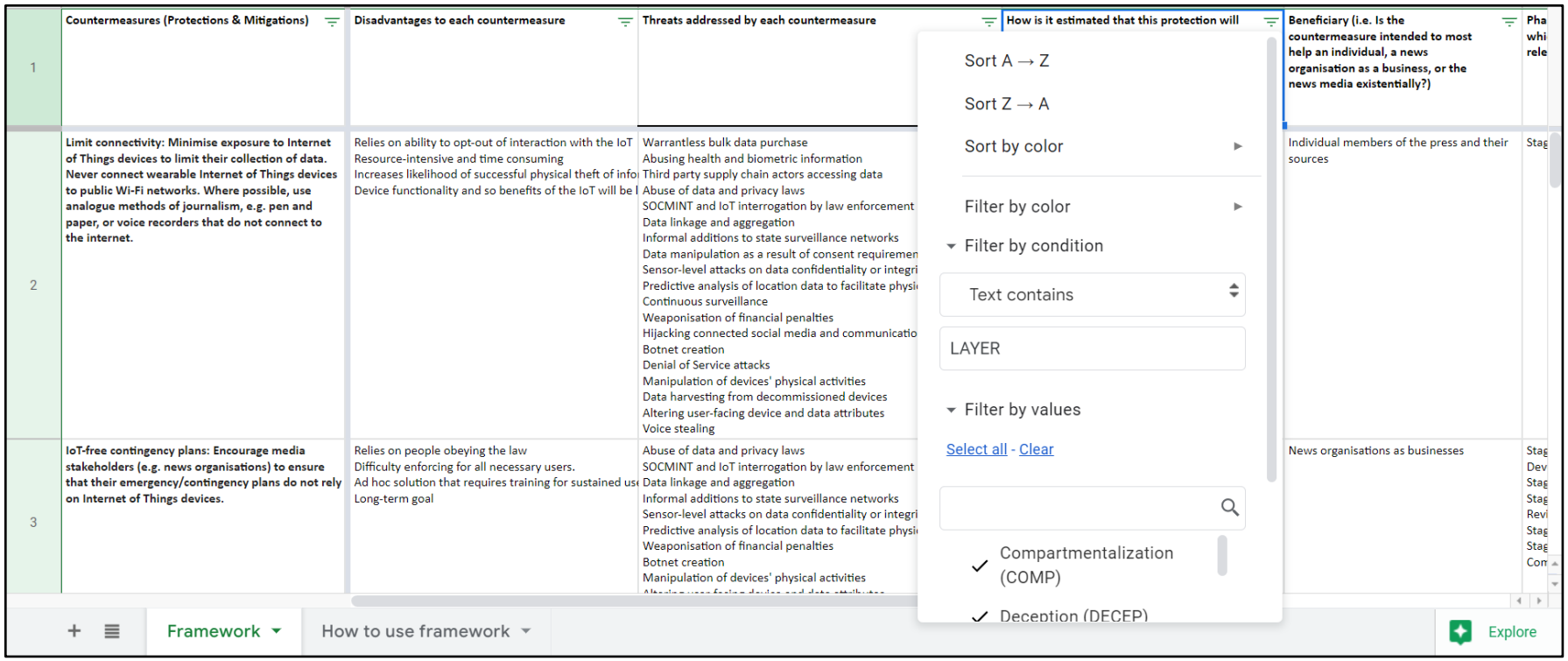


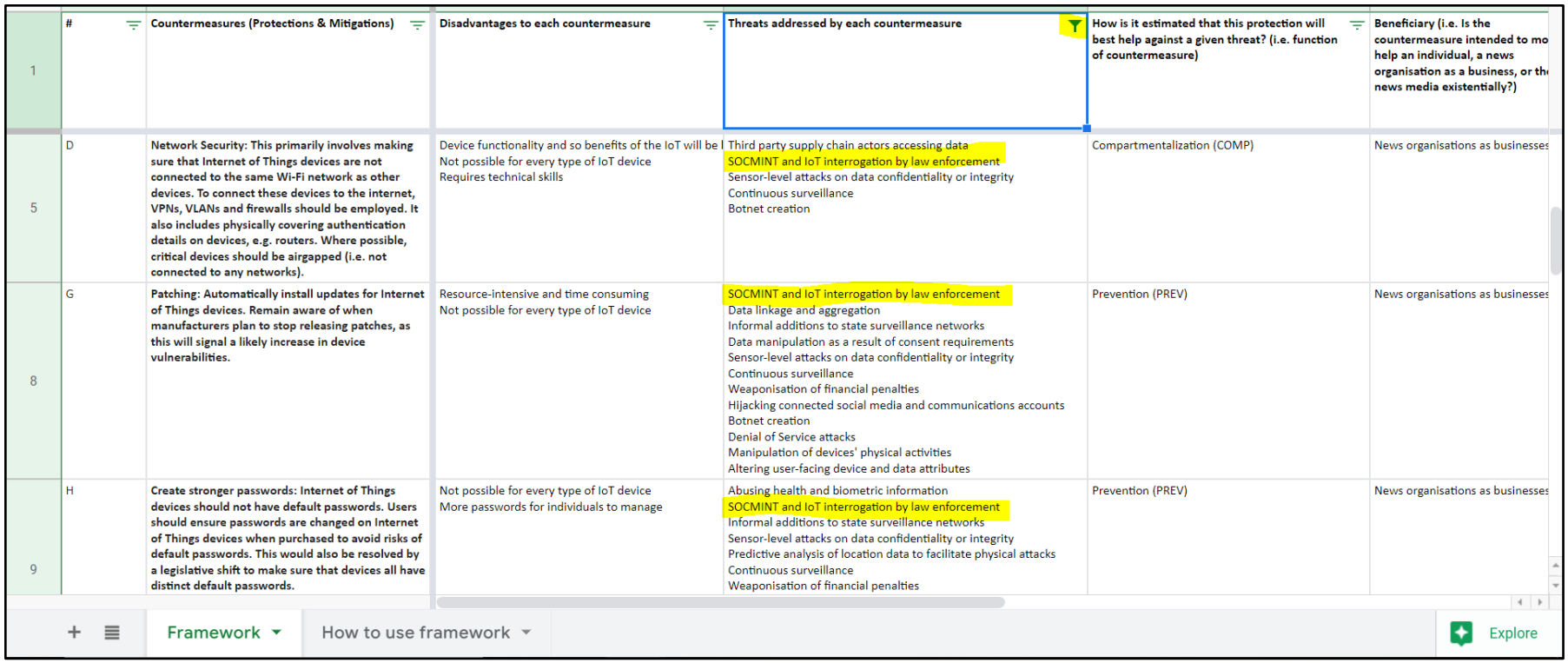
Figure 9: Demonstration of filtering process

(Figures 9 and 10 are rotated and maximised in size, to give readers a clear picture of what is included in this process. After the next figure, the subsequent figures will be smaller and integrated with text).

A spreadsheet with filters was chosen as the approach to present this information because the framework as a PhD research output is intended to be a prototype of a journalism-centric tool. It was therefore more important to choose an interface that was recognisable to its target audience rather than a fully optimised and visually novel commercial product. To this end, Excel was chosen as it is a widely used application, both generally and for risk assessment and management.[1029] Further, the framework compiled a large amount of information to demonstrate various perspectives on different elements of IoT risk management, which required a tool that allowed reorientation according to the priorities or level of knowledge of each user. The ability to filter this information increases the utility of the framework, as it can be used and amended in different ways and so is useful for a variety of roles and scenarios across the media industry.

As shown in Figure 10, users may begin by deciding their immediate priority, for example the threat that they want to tackle. They can filter column 4 to show only the rows that mention that threat (e.g. "SOCMINT and IoT interrogation by law enforcement"), giving them a list of countermeasures against it (e.g. "countermeasures A, B, D, G, H, I, L, M, N, O, P and Q").

[1029] SANS Institute (2009) Practical Risk Analysis and Threat Modeling Spreadsheet. In: *SANS Cyber Defense*. Available at: https://www.sans.org/blog/practical-risk-analysis-and-threat-modeling-spreadsheet/ (accessed 13 October 2021); Cronk RJ and Shapiro SS (2021) Quantitative Privacy Risk Analysis. In: *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, September 2021, pp. 340–350. DOI: 10.1109/EuroSPW54576.2021.00043.

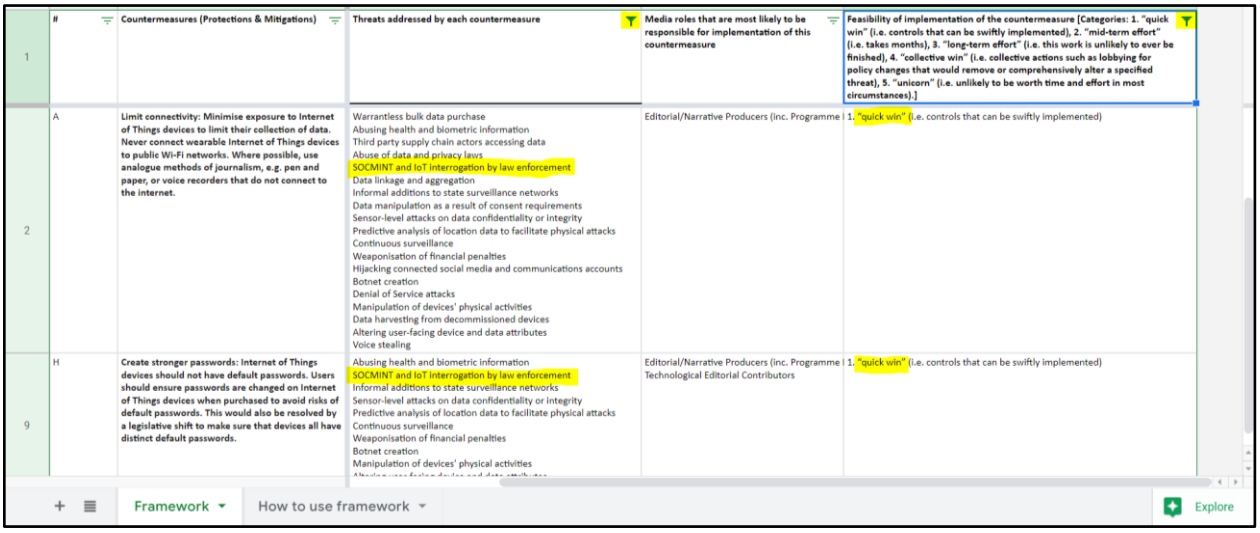


	#	Countermeasures (Protections & Mitigations)	Disadvantages to each countermeasure	Threats addressed by each countermeasure	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to mo help an individual, a news organisation as a business, or th news media existentially?)
5	D	**Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).**	Device functionality and so benefits of the IoT will be l Not possible for every type of IoT device Requires technical skills	Third party supply chain actors accessing data SOCMINT and IoT interrogation by law enforcement Sensor-level attacks on data confidentiality or integrity Continuous surveillance Botnet creation	Compartmentalization (COMP)	News organisations as businesses
8	G	**Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.**	Resource-intensive and time consuming Not possible for every type of IoT device	SOCMINT and IoT interrogation by law enforcement Data linkage and aggregation Informal additions to state surveillance networks Data manipulation as a result of consent requirements Sensor-level attacks on data confidentiality or integrity Continuous surveillance Weaponisation of financial penalties Hijacking connected social media and communications accounts Botnet creation Denial of Service attacks Manipulation of devices' physical activities Altering user-facing device and data attributes	Prevention (PREV)	News organisations as businesses
9	H	**Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.**	Not possible for every type of IoT device More passwords for individuals to manage	Abusing health and biometric information SOCMINT and IoT interrogation by law enforcement Informal additions to state surveillance networks Sensor-level attacks on data confidentiality or integrity Predictive analysis of location data to facilitate physical attacks Continuous surveillance Weaponisation of financial penalties	Prevention (PREV)	News organisations as businesses

Framework | How to use framework | Explore

Figure 10: Demonstration of filtering by a specific threat

Then, as displayed in Figure 11, they may decide that they are only willing to implement the countermeasures with a specific feasibility label (e.g. “quick win”), and additionally filter for this feature in column 9 (which would highlight countermeasures A, H and L).

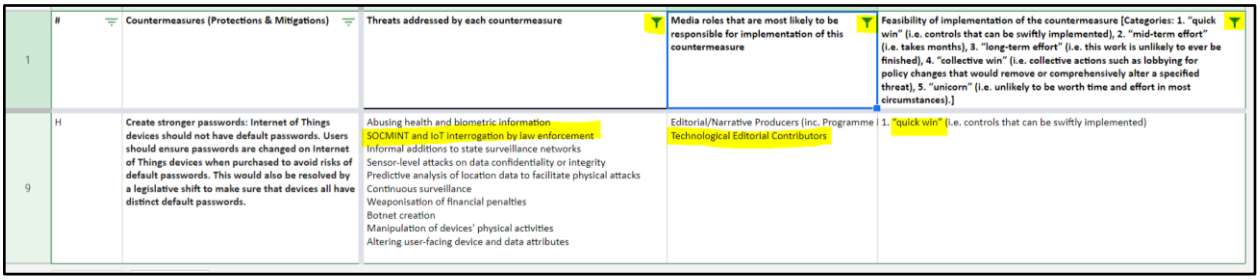


	#	Countermeasures (Protections & Mitigations)	Threats addressed by each countermeasure	Media roles that are most likely to be responsible for implementation of this countermeasure	Feasibility of implementation of the countermeasure [Categories: 1. “quick win” (i.e. controls that can be swiftly implemented), 2. “mid-term effort” (i.e. takes months), 3. “long-term effort” (i.e. this work is unlikely to ever be finished), 4. “collective win” (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat), 5. “unicorn” (i.e. unlikely to be worth time and effort in most circumstances).]
1					
2	A	Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.	Warrantless bulk data purchase Abusing health and biometric information Third party supply chain actors accessing data Abuse of data and privacy laws SOCMINT and IoT interrogation by law enforcement Data linkage and aggregation Informal additions to state surveillance networks Data manipulation as a result of consent requirements Sensor-level attacks on data confidentiality or integrity Predictive analysis of location data to facilitate physical attacks Continuous surveillance Weaponisation of financial penalties Hijacking connected social media and communications accounts Botnet creation Denial of Service attacks Manipulation of devices' physical activities Data harvesting from decommissioned devices Altering user-facing device and data attributes Voice stealing	Editorial/Narrative Producers (inc. Programme I	1. “quick win” (i.e. controls that can be swiftly implemented)
9	H	Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.	Abusing health and biometric information SOCMINT and IoT interrogation by law enforcement Informal additions to state surveillance networks Sensor-level attacks on data confidentiality or integrity Predictive analysis of location data to facilitate physical attacks Continuous surveillance Weaponisation of financial penalties Botnet creation Manipulation of devices' physical activities	Editorial/Narrative Producers (inc. Programme I Technological Editorial Contributors	1. “quick win” (i.e. controls that can be swiftly implemented)

Framework | How to use framework | Explore

Figure 11: Demonstration of simultaneous filtering using two columns

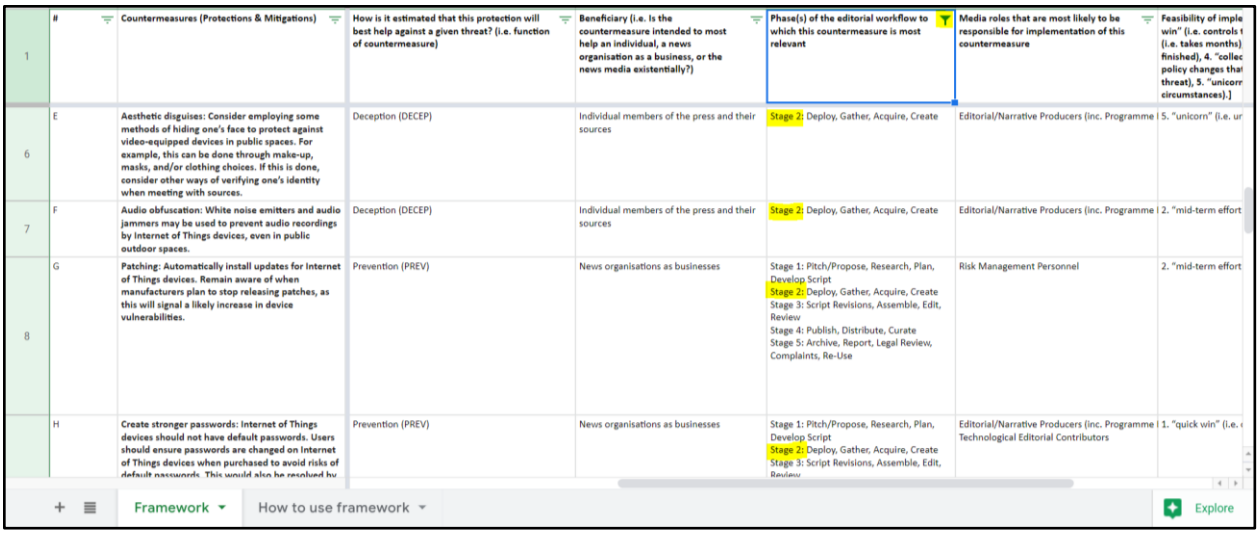
This may be as far as they are willing to narrow down their countermeasures. Alternatively, they may wish to further specify. For example, they could just search for countermeasures that are best assigned to their own media role umbrella (e.g. “Technological Editorial Contributors”). This third level of filtering would narrow down the results to one countermeasure. Figure 12 demonstrates simultaneous filtering using three columns.



	#	Countermeasures (Protections & Mitigations)	Threats addressed by each countermeasure	Media roles that are most likely to be responsible for implementation of this countermeasure	Feasibility of implementation of the countermeasure [Categories: 1. “quick win” (i.e. controls that can be swiftly implemented), 2. “mid-term effort” (i.e. takes months), 3. “long-term effort” (i.e. this work is unlikely to ever be finished), 4. “collective win” (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat), 5. “unicorn” (i.e. unlikely to be worth time and effort in most circumstances).]
1					
9	H	Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.	Abusing health and biometric information SOCMINT and IoT interrogation by law enforcement Informal additions to state surveillance networks Sensor-level attacks on data confidentiality or integrity Predictive analysis of location data to facilitate physical attacks Continuous surveillance Weaponisation of financial penalties Botnet creation Manipulation of devices' physical activities Altering user-facing device and data attributes	Editorial/Narrative Producers (inc. Programme I Technological Editorial Contributors	1. “quick win” (i.e. controls that can be swiftly implemented)

Figure 12: Demonstration of simultaneous filtering using three columns

Alternatively, users could decide to narrow the selection based on a specific workflow stage about which they are concerned, using the options in column 7, as in Figure 13.

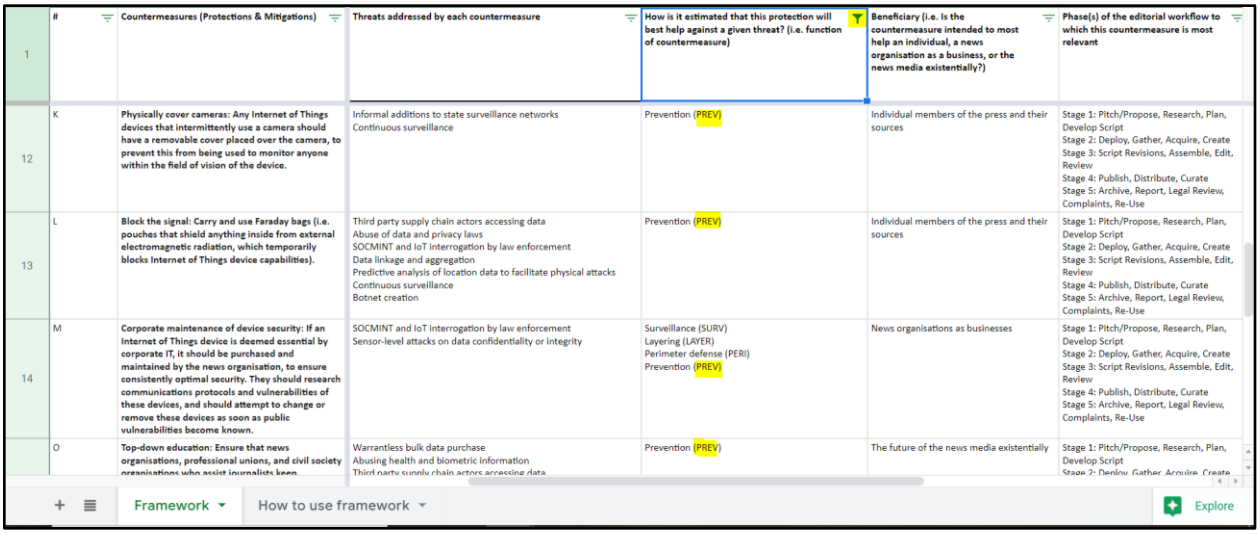


	#	Countermeasures (Protections & Mitigations)	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?)	Phase(s) of the editorial workflow to which this countermeasure is most relevant	Media roles that are most likely to be responsible for implementation of this countermeasure	Feasibility of imple win" (i.e. controls t (i.e. takes months) finished), 4. "collec policy changes that threat), 5. "unicorn circumstances).]
6	E	**Aesthetic disguises: Consider employing some methods of hiding one's face to protect against video-equipped devices in public spaces. For example, this can be done through make-up, masks, and/or clothing choices. If this is done, consider other ways of verifying one's identity when meeting with sources.**	Deception (DECEP)	Individual members of the press and their sources	Stage 2: Deploy, Gather, Acquire, Create	Editorial/Narrative Producers (inc. Programme	5. "unicorn" (i.e. ur
7	F	**Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.**	Deception (DECEP)	Individual members of the press and their sources	Stage 2: Deploy, Gather, Acquire, Create	Editorial/Narrative Producers (inc. Programme	2. "mid-term effort
8	G	**Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.**	Prevention (PREV)	News organisations as businesses	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel	2. "mid-term effort
	H	**Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by**	Prevention (PREV)	News organisations as businesses	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review	Editorial/Narrative Producers (inc. Programme Technological Editorial Contributors	1. "quick win" (i.e.

Framework | How to use framework | Explore

Figure 13: Demonstration of filtering by a specific workflow phase

As shown in Figure 14, they may also filter for function, for example whether they are aiming for prevention of a future threat versus various forms of mitigation of a current one, in column 5.

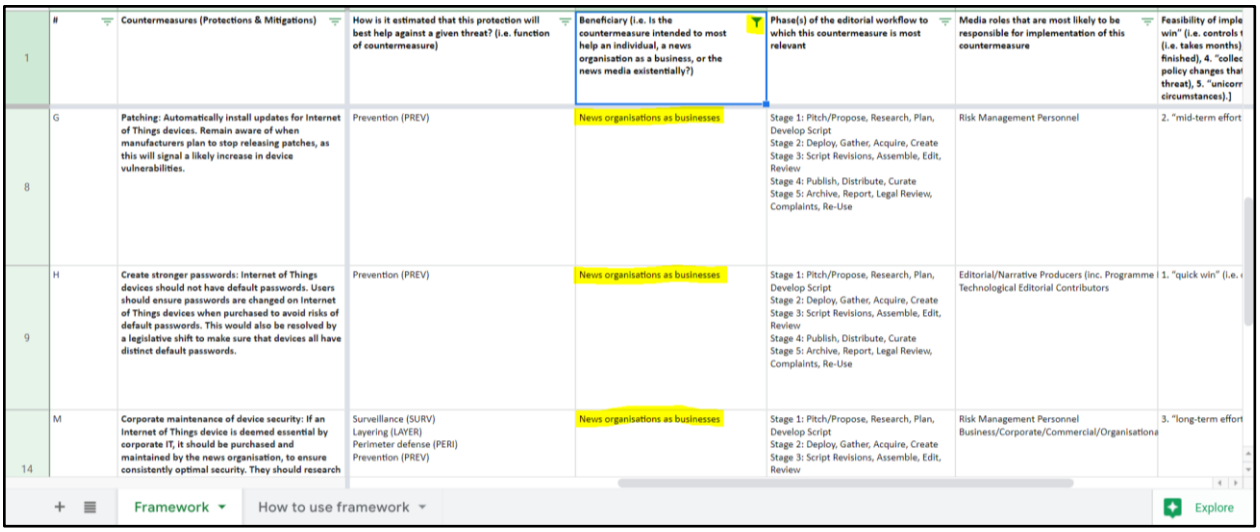


	#	Countermeasures (Protections & Mitigations)	Threats addressed by each countermeasure	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?)	Phase(s) of the editorial workflow to which this countermeasure is most relevant
12	K	**Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.**	Informal additions to state surveillance networks Continuous surveillance	Prevention (PREV)	Individual members of the press and their sources	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use
13	L	**Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).**	Third party supply chain actors accessing data Abuse of data and privacy laws SOCMINT and IoT interrogation by law enforcement Data linkage and aggregation Predictive analysis of location data to facilitate physical attacks Continuous surveillance Botnet creation	Prevention (PREV)	Individual members of the press and their sources	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use
14	M	**Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.**	SOCMINT and IoT interrogation by law enforcement Sensor-level attacks on data confidentiality or integrity	Surveillance (SURV) Layering (LAYER) Perimeter defense (PERI) Prevention (PREV)	News organisations as businesses	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use
	O	**Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep**	Warrantless bulk data purchase Abusing health and biometric information Third party supply chain actors accessing data	Prevention (PREV)	The future of the news media existentially	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create

Framework | How to use framework | Explore

Figure 14: Demonstration of filtering by a specific function

Further, as exemplified by Figure 15, they could focus on the key beneficiary they want to protect, filtering options in column 6, for example to only show organisational level countermeasures.



	#	Countermeasures (Protections & Mitigations)	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?)	Phase(s) of the editorial workflow to which this countermeasure is most relevant	Media roles that are most likely to be responsible for implementation of this countermeasure	Feasibility of imple win" (i.e. controls t (i.e. takes months) finished), 4. "collec policy changes that threat), 5. "unicorn circumstances).]
8	G	Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.	Prevention (PREV)	News organisations as businesses	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel	2. "mid-term effort
9	H	Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.	Prevention (PREV)	News organisations as businesses	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Editorial/Narrative Producers (inc. Programme Technological Editorial Contributors	1. "quick win" (i.e.
14	M	Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. They should research	Surveillance (SURV) Layering (LAYER) Perimeter defense (PERI) Prevention (PREV)	News organisations as businesses	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review	Risk Management Personnel Business/Corporate/Commercial/Organisationa	3. "long-term effort

Framework | How to use framework | Explore

Figure 15: Demonstration of filtering by a specific beneficiary

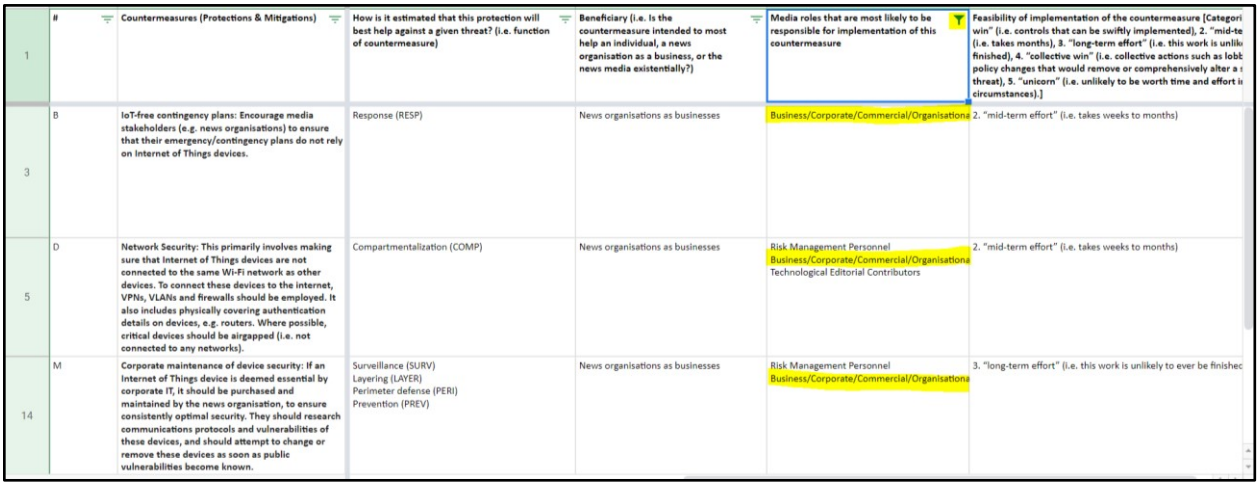
As another example, a journalist who is particularly concerned about "Continuous surveillance" could filter by this label. Then, of the listed countermeasures that combat this threat, they could decide whether the disadvantages of implementing these countermeasures constitute acceptable risk. Figure 16 demonstrates filtering by threat and reviewing countermeasure disadvantages.

	#	Countermeasures (Protections & Mitigations)	Disadvantages to each countermeasure	Threats addressed by each countermeasure
12	K	Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.	Not possible for every type of IoT device Not possible for bystanders	Informal additions to state surveillance networks Continuous surveillance
13	L	Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).	Not possible for bystanders	Third party supply chain actors accessing data Abuse of data and privacy laws SOCMINT and IoT interrogation by law enforcement Data linkage and aggregation Predictive analysis of location data to facilitate physical attacks Continuous surveillance Botnet creation
15	N	Intelligence sharing: Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). These groups can share information on topics including best practices and threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.	Resource-intensive and time consuming Long-term goal	Warrantless bulk data purchase Abusing health and biometric information Third party supply chain actors accessing data Abuse of data and privacy laws SOCMINT and IoT interrogation by law enforcement Data linkage and aggregation Informal additions to state surveillance networks Data manipulation as a result of consent requirements Sensor-level attacks on data confidentiality or integrity Predictive analysis of location data to facilitate physical attacks Continuous surveillance Weaponisation of financial penalties

Figure 16: Demonstration of filtering by threat and reviewing countermeasure disadvantages

The journalist can also assess the feasibility of implementing these countermeasures, given what is possible to implement as an individual in their professional capacity, and on which workflow stage(s) they are focusing. To view simultaneous filtering, see Figure 12.

The journalist can then make an informed decision about how best to protect their work and wellbeing from IoT threats for that part of their work. If they are part of a media organisation, the journalist can also check the column for "media roles that are most likely to be responsible for implementation of this countermeasure" (see: Figure 17), and approach the relevant person within their organisation.



	#	Countermeasures (Protections & Mitigations)	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?)	Media roles that are most likely to be responsible for implementation of this countermeasure	Feasibility of implementation of the countermeasure [Categori win" (i.e. controls that can be swiftly implemented), 2. "mid-te (i.e. takes months), 3. "long-term effort" (i.e. this work is unlik finished), 4. "collective win" (i.e. collective actions such as lobb policy changes that would remove or comprehensively alter a t threat), 5. "unicorn" (i.e. unlikely to be worth time and effort i circumstances).]
1						
3	B	IoT-free contingency plans: Encourage media stakeholders (e.g. news organisations) to ensure that their emergency/contingency plans do not rely on Internet of Things devices.	Response (RESP)	News organisations as businesses	Business/Corporate/Commercial/Organisationa	2. "mid-term effort" (i.e. takes weeks to months)
5	D	Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).	Compartmentalization (COMP)	News organisations as businesses	Risk Management Personnel Business/Corporate/Commercial/Organisationa Technological Editorial Contributors	2. "mid-term effort" (i.e. takes weeks to months)
14	M	Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.	Surveillance (SURV) Layering (LAYER) Perimeter defense (PERI) Prevention (PREV)	News organisations as businesses	Risk Management Personnel Business/Corporate/Commercial/Organisationa	3. "long-term effort" (i.e. this work is unlikely to ever be finishec

Figure 17: Demonstration of filtering by role umbrella to highlight tasks for corporate actors

8.5 Discussion

This section will cross-reference and highlight some of the most interesting responses provided by experts via the validation study that populated the framework.

8.5.1 Assessment of cyber security and states capabilities experts' validations of countermeasures

In this section, notable feedback from expert participants in the framework study is discussed, to draw out key observations that validate the utility of the framework and its countermeasures. For example, each countermeasure was seen to be able to combat at least two threats. Those that counter the fewest threats (i.e. two threats each) are E, F, K and M. The ones that cyber security experts believed would be most widely applicable are A, N, O and P (with 19 out of 19 threats each). Disappointingly, none of these overlap with the countermeasures voted by states' capabilities experts as being the most realistic and useful both now and in the future, which are D, H, J, K and L. All five of these countermeasures received votes of "Totally realistic [now]/this is already being effectively implemented by some people" and "5 Totally realistic [in the future]/this is already being implemented". This lack of overlap could be because the latter group (D, H, J, K and L) can all be implemented by individuals and were assigned immediate or mid-term feasibility, while the former group (A, N, O and P) are explicitly about educating journalists on IoT threats and restricting IoT risk, rather than specifically intended to counter one kind of threat. The inclusion of individual controls differentiates the framework from a recent Atlantic Council report on IoT risk to industries and government, which solely focuses on recommended policy shifts.[1030]

[1030] Mitchell P, Rowley L, Sherman J, et al. (2022) Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem. 26 September. Washington, D.C.: The Atlantic Council's Cyber Statecraft Initiative, under the Digital Forensic Research Lab (DFRLab). Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/ (accessed 24 October 2022), figure 4.

Further, only A, H, K and L were considered to be “quick wins,” while M, P and R (No IoT-specific countermeasure yet) were assigned “long-term effort”, indicating that this work is unlikely to ever be finished. There were five mid-term and five collective wins, which makes sense because most IoT protections likely require either some time taken (i.e. not immediate) or large-scale lobbying changes. Of the “quick wins,” all but A were assigned the highest possible realistic utility scores both now and in the future by states’ capabilities experts. Of the rest of the “quick wins,” H counters the most threats (10/19), so creating stronger passwords may be the most useful countermeasure for all three levels of implementation (individual action, organisational decree, and lobbying efforts) as a starting point for IoT risk management.

The view of A as being a widely effective “quick win” was unanticipated, as the cyber security experts surveyed for Chapter 4’s exploratory study in 2019 noted that limiting connectivity (“interaction with the IoT”) would be less possible within five years. In contrast, however, the median states’ capabilities experts scores for current and future realistic utility of countermeasure A were 4 (“Somewhat realistic/this is likely to be already in the process of development”) and 5 (“Totally realistic/this is already being implemented”) respectively, when answered in 2022. This could be for a number of factors, for example increased public concerns about privacy and device access due to political and pandemic events that have occurred since 2019.

Cyber security experts assigned all countermeasures at least one disadvantage, with the most common one being that a countermeasure is “Resource-intensive and time consuming.” The least prolific disadvantages were specific to countermeasures, such as “Risk assessments are administrative burdens” for countermeasure P. Overall, E was considered the least useful threat as it gained the only “unicorn” rating (i.e. unlikely to be worth time and effort in most circumstances). This seems reasonable, given that its listed disadvantages are that applying aesthetic disguises is “resource-intensive and time consuming” and “works against (some) machines, but is unlikely to slip past human analysts.” In contrast, states’ capabilities experts gave E a realism of utility rating of 4 both now and in the future, which is possibly a result of the pandemic normalising face coverings in public.

8.5.2 Assessment of media experts’ validations of countermeasures

In the media experts’ survey, respondents were asked to match countermeasures to the workflow stages to which they are most relevant. For the majority of countermeasures, the response with the most votes was "All of the above/This countermeasure is an action that exists in parallel with the editorial workflow". However, three countermeasures (A, E and F) had top votes for “Stage 2: Deploy, Gather, Acquire, Create”. It was decided that the workflow column would still be included in the framework and, to make it more effectively searchable, the all-encompassing label used in the survey would be removed. Instead, all stages are listed for each relevant countermeasure (i.e. all but the three previously named). One reason to keep this in the framework was to facilitate users who want to filter by a workflow phase other than stage 2, in which case then three countermeasures (and “No countermeasure”) will be highlighted. While this may be considered a limitation for the framework as a tool, as it means that this column is not as useful for filtering as some of the others, it does validate the general applicability of all countermeasures for the media.

All four options for media role umbrellas were assigned to different countermeasures, with the most common being “Editorial/Narrative Producers (inc. Programme Editors)” (assigned eight times), closely followed by “Risk Management Personnel” (assigned seven times). The least common was “Technological Editorial Contributors,” which was assigned only twice. It is particularly interesting that

"Business/Corporate/Commercial/Organisational Stakeholders" were assigned only four times, given that "News organisations as businesses" were considered the primary beneficiary of six different countermeasures, tied for the most votes with "Individual members of the press and their sources." The two countermeasures that did not have executive stakeholders assigned as the main enactors despite news organisations being the beneficiary were G and H.

Regarding function, "prevention" was assigned ten times, including to both of the countermeasures that had four modal functions each. In comparison, of the nine options for function (column 5), none of the countermeasures were classed as having the main intention of "deterrence" or "detection" of threats. Individual cyber security experts did vote for both these function options, but they were outvoted in the modal score that was used for the framework. It may be that none of these countermeasures are primarily deterrents, but some, such as Q, are "layered," and certainly include deterrence in their likely outcomes. Further, the lack of modal votes for "detection" may be because most cyber-threat detection mechanisms require technical expertise or software, while this is a list of countermeasures that can be implemented by a lay user group and do not include specific technological recommendations (to avoid giving rapidly out-of-date advice).

Encouragingly for the longevity of the framework, all but one countermeasure gained realistic utility ratings of 4 and 5 currently and in the future, and all but two stayed the same or increased in utility in the future. The exception to both of these is I, which decreased by one point to a 3 (i.e. "Not sure/don't know"), which may be because it is not the area of expertise of states' capabilities experts to say whether this kind of collaboration would be realistic. However, one expert noted that "It would be difficult to segregate global press infrastructure rules and requirements as this would be at odds with open standards and would eventually lead to compatibility issues with wider more commonly accessible technologies which in turn would lead to a less secure press infrastructure overall. We must continue to develop technology and improve the security of devices using open and transparent standards that ensure that everyone has access to or knowledge of technologies that can help or impede security." This feedback enabled the refinement of the countermeasure. One other notable countermeasure in this regard is G which, like I, was anticipated to decrease in realistic utility (but from a 5 to a 4). For G, this is possibly because there is a growing number of old devices that are unlikely to be supported with new patches.

8.5.3 Implications of countermeasures for the media sector

The framework highlights changes that require investment of time and resources by the entire media sector to contribute to combatting a range of IoT threats. Some of these countermeasures involve coordinated shifts across the media sector regarding security behaviours and technological ventures to try to improve protections specifically for the press. The former includes G and H, which are possible as actions on an individual level, or a media organisational level, but would be more powerful if the sector decided to lobby as a bloc to force tech companies to make patching and authentication easier, more transparent, and more secure. An example of the latter is countermeasure I, which encourages organisations within the media space to collaborate with technologists to design and implement standards and tools that would flag and possibly combat IoT threats as they happen. Although, as noted above, countermeasure I was seen to decrease in realism/perceived utility in the future, this kind of collaboration has precedent. One such widely-used software is SecureDrop, which was developed by Freedom of the Press Foundation to facilitate secure anonymous communication between journalists and sources.[1031]

[1031] SecureDrop (2022) About SecureDrop. Available at: https://securedrop.org/faq/about-securedrop/ (accessed 13 September 2022).

Additionally, some countermeasures specifically address the need for legislative and policy shifts to act against legal threats to the press. The need for this kind of countermeasure has been noted as a persistent concern by participants at every stage of this research, and in literature on both threats to journalists and IoT threats to democracy as a whole.[1032] For example, countermeasure C is intended to increase the amount of information available to journalists and the public about which companies share their data with the authorities. Adding to this, countermeasure Q's goal is to increase scrutiny of the legal clauses that allow this flow of individuals' information from private corporations to state agencies, and to raise awareness of the ways in which this access chills independent reporting. These countermeasures tackle a similar problem to that solved by SecureDrop, demonstrating that there are various elements to threats that can be neutralised from both tactical and strategic perspectives, as well as by combining legal and technical knowledge and protections.

As highlighted by interviewee responses for Chapter 7, other work needed to build the media industry's internal resilience to IoT threats includes inter-organisational schemes such as countermeasure N, which would establish threat intelligence sharing networks across the media. These could formalise and build upon the unofficial systems that were disclosed by interviewees, such as discussions between media lawyers during breaks, and journalists' unplanned post-work drinks (see: Chapters 6 and 7). Cyber security experts assigned this countermeasure as an effective response to all 19 threats, illustrating the utility of industry-wide efforts. Countermeasure O is likewise a comprehensive countermeasure. However, unlike N, O would not be focused on communally acknowledging and responding to current active problems. Rather, O would be a preventative way of raising the industry's level of awareness of all potential IoT threats to the press and guiding public communication on this topic. Similarly, countermeasure B would address the industry's dependence on networked devices and enable swift and unified responses to attacks on, for example, broadcasting infrastructure, such as the TV5Monde incident mentioned in Chapter 5.[1033] Countermeasure B is related to and informed by countermeasures M and P, which respectively minimise and manage IoT risk over time, but can be done by each organisation independently. This overlapping influence of countermeasures creates a layering effect, which contributes to a multifaceted protection of the press against IoT threats.

8.6 Conclusion

This chapter presents a novel framework that aims to guide members of the media through IoT-specific risk management decision-making as an addition to existing security processes. The framework functions as a tool that matches countermeasures to threats (see: Chapter 5). For each countermeasure, it also details: disadvantages, function and feasibility, most relevant phases of the media workflow, groups of media roles most likely to be responsible for implementation, and parts of the field that would most benefit. The chapter itself begins with an overview of the framework, before describing the content of each column and how it was created, and then explaining how users may interact with the tool, and finally discussing key findings.

[1032] Lashmar P (2020) Spies, Spin and the Fourth Estate: British Intelligence and the Media. Edinburgh, Scotland: Edinburgh University Press, p.266. Mitchell P, Rowley L, Sherman J, et al. (2022) Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem. 26 September. Washington, D.C.: The Atlantic Council's Cyber Statecraft Initiative, under the Digital Forensic Research Lab (DFRLab). Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/ (accessed 24 October 2022).

[1033] Council on Foreign Relations (CFR) (2015) *Connect the Dots on State-Sponsored Cyber Incidents - Compromise of TV5 Monde*. Cyber Operations, April. New York, NY, USA: Council on Foreign Relations (CFR). Available at: https://www.cfr.org/cyber-operations/compromise-tv5-monde (accessed 13 September 2022).

The framework was created by surveying experts from the media, cyber security and the IoT, and states' capabilities, to ensure that the suggested countermeasures were both effective, potentially durable, and usefully personalisable for those working in journalism. As discussed in this chapter and Chapter 3, four online questionnaires were used, collecting twenty responses.

When asked whether this framework of countermeasures would usefully add to the journalist security materials available, media experts overwhelmingly said yes. They also attested that they had observed some of the countermeasures already in practice within media operations, although most referred in their responses to this question to basic non-IoT specific cyber-hygiene, therefore highlighting the need and novelty of this framework.

The majority of countermeasures were shown by media experts to be applicable to and useful for all phases of the journalistic workflow, demonstrating that the framework is relevant to the user population. The framework can therefore be considered to have achieved its goals in that it offers one answer to the research question, "How can members of the press in democratic countries improve their identification of, protection from, and resilience against threats from the Internet of Things?", and fills a gap in the literature, both academic and grey.

Chapter 9: Discussion and Conclusion

9.1 Introduction

The chapter first reiterates the question and literature gap that motivate this research, and outlining the resolution provided by this thesis. Then, it will explain the interplay between the chapters that gives their findings resonance on multiple levels. It will discuss how to use the components of the toolkit to raise awareness of security threats and to create structured risk assessment and management systems for individuals and organisations within the media, underpinned by the NIST CSF functions. The utility of this toolkit for combating issues such as those on the national and international scales highlighted in the Country Profiles will also be discussed.

The chapter will then break down the key contributions made to audiences of this thesis: academia, policymakers, and the media and technology sectors. Limitations of the research will then be evaluated, followed by potential future work and a discussion of the implications of this research.

9.2 Summary of chapters and synthesis of research findings

9.2.1 Thesis aims and findings

In recognition of a clear absence of literature accessible to the press on how to recognise and counter IoT threats to their work and wellbeing, this DPhil has asked: How can members of the press in democratic countries improve their identification of, protection from, and resilience against threats from the Internet of Things?

In aiming to answer this question, this thesis has presented a multi-piece toolkit that enables members of the press to identify threats from IoT devices to themselves and their work, and then identify the countermeasures best suited to their context, customisable on numerous levels. This toolkit is intended for habitual use by members of the media, to determine the specific IoT threats that are most relevant to them, which countermeasures can help, and how to implement them in a sustainable way that does not compromise the press' ability to do their jobs. Although it cannot be claimed that this toolkit is future-proof because the IoT changes rapidly, both conceptual models and the framework are structured to facilitate the inclusion of new information as it emerges. Further, the toolkit's anticipated utility over time was assessed through surveying states' capabilities experts (see: Chapter 8, section 8.5). As previously discussed, these experts responded that, in the foreseeable future, all of the threats would either remain likely or increase in relevance, and that all but two countermeasures would also either stay useful or indeed gain utility. This suggests that the toolkit will be resilient to predicted changes in the IoT landscape. This toolkit is therefore a useful contribution to journalists' security resources as it provides a starting point for the media to assess and manage IoT risk, and can grow as their knowledge and practices evolve.[1034]

Another aim of this thesis was to show that while civilians targeted by nation-state adversaries are faced with significant asymmetries of power, there are nevertheless countermeasures that can be considered for mitigating some of those threats. As discussed in Chapter 8 and expanded later in this chapter, protections and mitigations to reduce the effects of these hostile actions by advanced actors are especially possible if media stakeholders coordinate industry-wide efforts. The inclusion of four different country profiles in this thesis showcased that while there are different cultural influences on societal perceptions of the utility and dangers of technology, there is nonetheless sufficient similarity in the concerns raised

[1034] McGregor SE (2021) *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.

by research participants (see: Chapters 4, 6 and 7) to create a framework (see: Chapter 8) that can be widely used, given how it can be filtered for different needs within the media community.

The overall objective of this thesis was to bridge the literature and perception gap found in the literature synthesis (see: Chapter 2) and the exploratory study (see: Chapter 4), by investigating how the press in democracies can improve their identification of, protection from, and resilience against Internet of Things-specific threats to the work and well-being of journalists and sources. Later chapters established threat models that included secondary threats and their consequences for the press (see: Chapter 5), focusing on the practical and policy challenges that compound or supersede IoT threats to journalists in profiled countries (see: Chapters 6 and 7), and compiling recommended countermeasures in a framework tailored to use by the press (see: Chapter 8).

9.2.2 How the chapters came together

The parts of this thesis built upon each other and came together to form not just the toolkit itself but also the country profiles (see: Chapters 6 and 7) and literature synthesis (see: Chapter 2) that both demonstrated the need for the toolkit and contributed to its content and form. Section 2.4 of Chapter 2 outlined the different ways in which democratic governments approach regulation of the IoT, while Chapters 6 and 7 examined how the contemporary effects and practicalities of these legal and political strategies create challenges for news organisations and journalists. These country profiles highlighted elements that are crucial to adoption of countermeasures such as those in Chapter 8's framework, such as the significance of peer-to-peer information sharing networks for threat education (countermeasure N), and the need to account for a variety of media roles and workflow phases when designing security behaviours and processes. Thus, the country profiles were intended to demonstrate the limiting factors regarding protection mechanisms for journalists, as well as other threats that must be balanced in order to effectively advise the media on how to prioritise and manage IoT-related risk. Interviews conducted for Chapters 4, 6 and 7 also provided anecdotal evidence that some limited knowledge of IoT threats exists and is shared among members of the media, but not widely or accurately.

The decision to use this thesis to present a toolkit in response to the identified literature gap was influenced by Pierce *et al.* They referred to security toolkits as "(1) collections of tools and actions, (2) actionable and usable for individuals and groups, which are (3) offered as solutions or other ways of addressing immediate user needs related to cybersecurity".[1035] They recognised that toolkits targeted toward specific communities are able to reflect shared touchstones and can "include emotional and social aspects [of security]"[1036] when recommending relevant actions and tools – many of which are collected from third-party sources, such as the experts who contributed to the thesis from outside the media sector.

Chapter 5 (conceptual models) built upon previous chapters by clarifying and amplifying significant elements of, in particular, the exploratory study detailed in Chapter 4, as well as setting the context for subsequent research. Therefore, the organisational models of Chapter 5 were intended to provide a formalised foundation for identifying IoT (both "asset" and unavoidable) devices with which journalists interact, and to evidence the threats that these devices embody. These twin objectives were key to understanding existing literature on categorisation systems and associated methodologies, as detailed in Chapter 2.

[1035] Pierce J, Fox S, Merrill N, et al. (2018) Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. Proceedings of the ACM on Human-Computer Interaction 2(CSCW): 139:1-139:24. DOI: 10.1145/3274408.
[1036] Pierce J, Fox S, Merrill N, et al. (2018) Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. Proceedings of the ACM on Human-Computer Interaction 2(CSCW): 139:1-139:24. DOI: 10.1145/3274408.

The literature synthesis chapter (see: Chapter 2) determined the need to recognise that, as a core function of IoT devices is communication with each other, metadata may effectively be synonymous with message contents within a given network.[1037] Amalgamating metadata across devices or services with which an individual has interacted (even if unknowingly) may enable comprehensive personal profiling, which could be a threat to both their privacy and security.[1038] Building on this point, Chapters 5 (conceptual models), 6 (legislative and policy challenges for the press) and 7 (geopolitical and organisational challenges for the press) raised the issue of legal surveillance and profiling threats relating to states' access to IoT data that may be collected and retained by private companies.

The framework in Chapter 8 closed the gap between journalist need and cyber expertise exposed in the pilot chapter (see: Chapter 4) and in Chapters 6 and 7, which documented and compared the press freedom situation and the IoT landscape, both in terms of the market and threats, across four influential democracies.

To illustrate the usability of this toolkit and the utility of the different components of this thesis, please see the following vignette: Apple AirTags have been at the centre of controversy, given their appropriation as tools for stalking.[1039] For a journalist trying to establish their risk profile, they may consult the IoT device organisational model in Chapter 5 and note that AirTags are a portable threat that exist across all spheres. They may then turn to the threat categorisation model in Chapter 5 to assess how much risk is posed by either their ownership of these devices, or the possibility that a malicious actor is using an AirTag to track their movements. When consulting Chapter 8's framework, the journalist may note that the only two immediate-impact countermeasures that would be effective for "prevention" of "continuous surveillance" threats by a single-purpose tracker that are suggested for individual implementation are A (Limit connectivity) and L (Block the signal). Following these recommendations, a journalist could decide not to purchase an AirTag, and to purchase a Faraday bag in which to routinely place their portable possessions (e.g. workbag), to allow them time to search for an adversary's AirTag while preventing it from relaying tracking information. The journalist may also decide to collaborate with others in the media to push for Q (Legal scrutiny in favour of press freedom), specifically on the issue of limiting the capabilities of tracking devices. They may turn to the country analyses in Chapters 6 and 7 to learn about the factors affecting the development and market of these devices in their country.

9.3 Contributions

This section will discuss the findings of the thesis and elaborate on the contributions of this toolkit to the academic fields of computer science, cyber security, and surveillance studies, as well as to policy and industry. In so doing, it demonstrates how existing cyber security guidelines, such as the NIST CSF discussed in Chapter 1, can be tailored to non-technical audiences who would benefit from such information. It also discusses how the toolkit may be incorporated into journalistic security strategies, to mitigate these emerging threats to journalists and sources.

[1037] Branch P (2015) How will data retention laws cope with the Internet of Things? Available at: http://theconversation.com/how-will-data-retention-laws-cope-with-the-internet-of-things-36885 (accessed 26 February 2020).
[1038] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[1039] Moore A (2022) 'I didn't want it anywhere near me': how the Apple AirTag became a gift to stalkers. *The Guardian*, 5 September. Available at: https://www.theguardian.com/technology/2022/sep/05/i-didnt-want-it-anywhere-near-me-how-the-apple-airtag-became-a-gift-to-stalkers (accessed 15 September 2022).

9.3.1 Contributions to academic scholarship

Before this research was undertaken, there was a clear knowledge gap in academic literature regarding identification and examination of links between the IoT and media security, either regarding threats or protections. As explored below, Chapter 2 discussed four questions to establish the components necessary to answer the overarching research question of this thesis. The results of this thesis clearly address these questions by using interdisciplinary perspectives to inform and link cyber security and journalism studies concerns, to create contributions that enhance all relevant fields. There are therefore four main ways in which this thesis contributes to academic scholarship on cyber security and journalism. (1) As will be expanded on below, this thesis addressed the first question by exploring IoT risk through a location-based lens and how this interacts with journalists' activities. (2) It answered the second question by presenting proof-of-concept threats and countermeasures in a new way that is tailored to a non-technical audience. (3) For the third question, the thesis provided detailed comparative profiles of the media environment in four countries, thereby ensuring that the recommended countermeasures account for and do not impede journalistic realities. (4) It answered the fourth question by centring the media as the targets and defenders of emerging threats. To this end, this thesis contributes to privacy, cyber security, and surveillance studies by focusing on a specific, hyper-watched community, and reviewing the effects and potential protections that are relevant to this community's interactions with the IoT.

To the first of Chapter 2's questions, which asked how to define and structure the IoT, a contribution that this thesis makes to journalism studies is that both Chapter 5's IoT device organisational model and Chapter 8's framework examined how the work and workflow of journalists create unique environmental risks. This aligns with an insight from Eliot Stempf, BuzzFeed's head of high risk (cited by McGregor), who noted that traditional risk assessments are still built "around the notion of the reporter going abroad to do an assignment and then returning to [a] safe home country."[1040] This does not reflect patterns of IoT proliferation, as IoT risk, especially from data collection, is everywhere, all the time, and by all actors, and inspired this thesis's toolkit for managing that risk, as it cannot be eradicated. This is relevant to literature on privacy and security because this thesis both acknowledges that consumer devices may be found in public spaces, and includes countermeasures that defend against ambient threats to bystanders, even when devices are designed to be unobtrusive and to continually collect data.[1041]

The second question that helped to structure the literature gap pertained to the relationship between the IoT and privacy and security. Chapter 2 found that academic scholarship acknowledged many IoT threats in different categories, but rarely consolidated them in discussion. Chapter 5's journalism-specific IoT threat categorisation is a particular contribution to the literature on privacy and security, especially the Human-Computer Interaction community within cyber security. This is because of its collation of information around IoT threats to stakeholders in the media, which has not yet been done either academically or journalistically beyond proofs-of-concept for individual threats.[1042] This collection and analysis of different journalism-relevant IoT threats may be used to develop IoT threat models for other populations.

[1040] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[1041] Flammer I (2016) Genteel Wearables: Bystander-Centered Design. IEEE Security Privacy 14(5): 73–79. DOI: 10.1109/MSP.2016.91.
[1042] Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2017. pp. 21-22. Itkin E (2020) *Don't be silly - it's only a lightbulb*. 7 August. Tel Aviv, Israel: Check Point Institute for Information Security (CPIIS) in Tel Aviv University. Available at: https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/ (accessed 3 December 2022).

A core contribution of this thesis to both cyber security and journalism research is a way of presenting both threats and countermeasures, so that audiences do not feel overwhelmed or alienated by the information.[1043] McGregor noted that information security literacies and skills are underdeveloped for those in journalistic circles, who lack the foundational knowledge necessary for reflexive and efficient threat modelling.[1044] Further, Chapter 2 identified that existing systems for classifying and stratifying IoT devices are largely aimed at readers with technical or computer science backgrounds and they assume a baseline understanding of protocols and processes. In response, this thesis has attempted to address some of the concerns and build on the recommendations in such scholarship for the toolkit recommendations. For example, the conceptual models presented in Chapter 5 and built on in Chapter 8 are customisable and relevant across environments, so that members of the press, regardless of their role, can understand their specific IoT threats profile and share this with their peers.[1045]

As recommended by P. W. Singer, the use of FicInt, i.e. hypothetical consequences in the threat categorisation system (see: Chapter 5), also enables users to imagine themselves as their adversaries, equipping them to understand the ways in which their defences may need bolstering.[1046] Further, this thesis learned from the point made by Kazansky and Oliver that there are issues with only recommending specific tools as solutions, which act as one-off interventions that can concentrate vulnerabilities for exploitation.[1047] This inspiration was further confirmed by an insight from an interviewee for this thesis who found that journalists they trained engaged most with basic but tailored scenarios that encouraged them to think about the way in which cyber security and even abstract emerging threats affect the daily practical realities of their work, regardless of their varying levels of technical understanding (see: Chapter 7).[1048]

Chapter 2's third question asked, "How do states regulate the IoT?". Chapter 4 (exploratory study) excavated gaps between journalists' and journalism researchers' perceptions of cyber security and the expertise of cyber security researchers, and the thesis builds on this in two key ways: First, it evaluates the roles of institutions, corporations, and states in facilitating these threats. As discussed in Chapter 2, this requires an interdisciplinary perspective that includes surveillance theory. Particularly, Bentham and Foucault's panopticism relating to the role of the state in regulating and accessing IoT data and devices,[1049] and Zuboff and Burgess and Hurcombe's insights around corporate use and oversight (or lack thereof).[1050]

The thesis combined these insights with cyber security findings, and geopolitical and legislative concerns. This is best demonstrated in Chapters 6 and 7, as interviewees expressed anxiety about the difficulty of

[1043] *The True Story of Using Fiction to Enhance Risk Intelligence* (2021) The Association of International Risk Intelligence Professionals (AIRIP). Available at: https://www.youtube.com/watch?v=qP_i94eP2Ho (accessed 18 January 2023).
[1044] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[1045] McGregor SE (2021) *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.
[1046] *The True Story of Using Fiction to Enhance Risk Intelligence* (2021) The Association of International Risk Intelligence Professionals (AIRIP). Available at: https://www.youtube.com/watch?v=qP_i94eP2Ho (accessed 18 January 2023); McGregor SE (2021) *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.
[1047] Kazansky B (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society 8(1). SAGE Publications Ltd: 2053951720985557. DOI: 10.1177/2053951720985557; Oliver J (2018) Journalism schools still behind on cybersecurity training, new survey finds. Available at: https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php (accessed 15 November 2020).
[1048] Interviewee for Chapters 6 and 7: P40
[1049] Bentham J (2012) The Works of Jeremy Bentham, Vol. 4 (ed. J Bowring). RareBooksClub.com; Foucault M (1977) DISCIPLINE AND PUNISH: The Birth of the Prison. New York: Knopf Doubleday Publishing Group.
[1050] Zuboff S (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books Ltd.; Burgess J and Hurcombe E (2019) Digital Journalism as Symptom, Response, and Agent of Change in the Platformed Media Environment. Digital Journalism 7(3). Routledge: 359–367. DOI: 10.1080/21670811.2018.1556313.

managing their privacy and security in a surveillance capitalist age. They were especially concerned about entangled supply and maintenance chains, as there are myriad of state and corporate actors whose goal is to extract value from data subjects via a single IoT device. This means that the odds of a data breach at some point in the chain are increased and could be devastating for a journalist. Particularly regarding corporations, including the IoT manufacturers discussed in Chapter 2, it is clear that their control over data and devices is detrimental to the ability of the free press to hold them accountable for any lapses in judgement or execution. To contribute to combating the corporate hegemony that facilitates emerging threats from the IoT to journalists, the framework in Chapter 8 presented countermeasures C (transparency reporting) and I (collaborative technology design).

Finally, the fourth question assessed the materials available that mention the IoT as a potential issue for journalists, and any literature on countermeasures to such threats. The primary contribution of this thesis to academic research was its examination of emerging technology threats that had not previously been considered in either cyber security or journalism research literature. This involved examining how journalists and the media industry existentially are particularly at risk from the IoT. Wider studies of security and privacy relating to the IoT do not specifically focus on the media. This thesis does so because of the high likelihood of journalists being targeted, including via IoT devices, due to the value of information held by those within and proximal to the media. Journalists are not uniquely targeted; this thesis has acknowledged that other communities are similarly vulnerable and high risk, such as organisations and individuals working in the human rights sector. However, this thesis considers journalists to warrant particular study because highly-resourced actors, particularly nation-states, are well-documented adversaries of journalists' and news organisations' cyber security.[1051] Further, the ramifications for attacks on the media include impeding democratic processes.

A related contribution of this thesis, specifically to journalism studies, is demonstrating the ways in which journalists can be encouraged to improve their protective behaviours, while providing support to prevent this from compromising their work. In particular, the scenarios presented in Chapter 5 centre on the fact that journalistic work relies on the collection and interpretation of original information, which involves creating and recognising networks. Thus those within the press that do not consider themselves to work on high-risk subjects can understand how they might be a pivot point for an adversary targeting a colleague or peer.[1052] This built on existing research in the journalism studies and security space, for example Crete-Nishihata *et al*. which demonstrated the volume and severity of attacks on journalists and their relative lack of training and security measures in response.[1053] This is why the threats categorisation (see: Chapter 5) included hypothetical consequence scenarios to make it a useful tool for security awareness training.

To directly address the challenges of security training raised in journalism studies literature, Chapter 5's threat categorisation utilised scenarios that are relevant to this specific population and explained in lay-

[1051] Perlroth, N.: Washington Post Joins List of News Media Hacked by the Chinese, https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html, (2013); Huntley, S., Marquis-Boire, M.: Tomorrow's news is today's intel: Journalists as targets and compromise vectors. Black Hat Asia 2014., Singapore (2014); Wagstaff, J.: Journalists, media under attack from hackers: Google researchers, https://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328, (2014); Reporters Without Borders: RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders, https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators, last accessed 2020/09/11.

[1052] McGregor SE (2021) Chapter 3: Assessing Risks and Threats, in: *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.

[1053] Crete-Nishihata M, Oliver J, Parsons C, Walker D, Tsui L, Deibert R. The Information Security Cultures of Journalism. Digit Journal. 2020 Jun 25;0(0): pp. 1-24.

terms, enabling structured risk assessments that do not overwhelm individuals (per Henrichsen) or are quickly forgotten (per Oliver).[1054] The goal of the framework was to build security and risk management habits, as well as community to hold each other accountable through, for example, countermeasure N (intelligence sharing). Di Salvo and Henrichsen's research on the multiplicity of roles within the media also influenced the framework, as it was designed to be helpful across the industry, to encourage both uptake and consistent use.[1055] Further, countermeasure O's emphasis on institutional support for press security (through top-down education), combined with the framework's clear identifiers of corporate responsibility and corporate beneficiaries were intended to encourage acknowledgement of the distinct needs of the newsroom and the news organisation as a business.[1056]

Acknowledging this, Chapter 8's framework can be used at strategic and organisational levels as well as by individuals, while Chapter 5 can be used to translate this strategy into tactics on an operational level within the organisation or to build an understanding from the bottom-up in order to engage with more holistic protections and mitigations.[1057]

These results, detailed throughout the thesis, lead to potential future areas of research, detailed in section 9.6.

9.3.2 Contributions to policy

There are three predominant contributions to policy from this thesis: (1) First, it addressed ways in which privacy and security must be enshrined in the IoT and its use. (2) Second, it evaluated the challenges of different methods of regulation of the IoT, and how associated legal and regulatory threats affect the press. (3) Third, it presented ways in which policy and legislation may create more hospitable environments for press freedom and security against IoT threats to the media. The fact this thesis has potential policy contributions is in line with Smith's insight that the IoT's linking of the "cyberworld to physical reality" is unprecedented, and spawns such multifaceted outcomes that it threatens to subvert the work of policymakers, unless explicitly addressed.[1058]

The primary contribution of this thesis to technology policy derives from Chapters 6 and 7, which raised issues relating to a lack of privacy and security by design in IoT hardware, software, and networking capabilities. Chapter 8's framework included countermeasures that may contribute towards addressing threats that result from this problem. For example, countermeasures G (patching) and H (create stronger passwords) could be enacted by individuals or by corporations, but this would likely result in some gaps

[1054] Henrichsen JR (2021) Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice* 0(0). Routledge: 1–20. DOI: 10.1080/17512786.2021.1927802; Oliver J (2018) Journalism schools still behind on cybersecurity training, new survey finds. Available at: https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php (accessed 15 November 2020).

[1055] Di Salvo P (2021) "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice* 0(0). Routledge: 1–18. DOI: 10.1080/17512786.2021.2014346; Henrichsen JR (2021) Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice* 0(0). Routledge: 1–20. DOI: 10.1080/17512786.2021.1927802.

[1056] Crete-Nishihata M, Oliver J, Parsons C, Walker D, Tsui L, Deibert R. The Information Security Cultures of Journalism. Digit Journal. 2020 Jun 25;0(0): pp. 1-24.

[1057] Tsui L and Lee F (2019) How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. Journalism 00(0). SAGE Journals: 1–23. DOI: 10.1177/1464884919849418; Alves, L. (2019). Application of Management and Control Techniques in Brazilian Construction Industry. Current Trends in Civil & Structural Engineering. 2. 1-6. 10.33552/CTCSE.2019.02.000545.

[1058] Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2017. pp. 6, 20-21, 40.

where these were not carried out in a timely fashion. If incorporated into national policies and laws, these gaps would be lessened, as the onus would be on technology companies to ensure that devices have distinct default passwords and patches are released promptly, with clear warning when these updates will no longer be released. Further, by putting the onus on manufacturers to secure connected devices, the framework of recommendations can remain agnostic to specific IoT devices, which facilitates its continued utility given the variety of devices on the market is so heterogeneous.

Another contribution to policy is that Chapters 6 and 7 found that there is limited efficacy of self-regulatory efforts, given international IoT supply chains which are a source of concern for potential targets of IoT threats, due to the centrality of China in manufacturing and distribution of device components. They also found that legal protections for the press are being eroded in a variety of ways that can only be counteracted through coordinated pressure on behalf of the media. These legal threats can include government and law enforcement access to IoT data, enabled by insufficiently specific wording in legislation and a culture of surveillance that has been growing since 9/11. Interviewees additionally highlighted a lack of experience including the IoT in risk assessment and management procedures, even at news organisations. These considerations provided evidence of areas in policy and law that require further scrutiny in order to bolster journalistic security, and protect press freedom and democracy from domestic and geopolitical threats.

Thirdly, this thesis contributed concepts that could be developed into complete policy ideas primarily through the framework presented in Chapter 8. However, there are ways in which the toolkit cannot solve problems raised in the country profiles. For example, anything relating to a federal/state divide, such as the press freedom issues associated with diminished federal oversight of consolidation of media ownership found in the US and Australia, would require an overhaul of the countries' political system. That type of restructuring is beyond the scope of this toolkit. Nonetheless, the framework included four countermeasures that need to be addressed and prioritised at the policy level as they cannot be reliably implemented or enforced at any level below that. For example, if implementation of countermeasure C (transparency reporting) were successful, governments would consistently engage in transparency reporting, which could drastically affect public trust in different corporations and in their state agencies themselves.

Of course, countermeasure Q (legal scrutiny in favour of press freedom) also explicitly argued for greater legal, political and media interrogation of legal clauses that enable exploitation of IoT functionalities and data in ways that may pose risks to press freedom. As mentioned in Chapter 8, this work would not require solely grassroots efforts and may build upon the pressure applied by existing groups with this mission, such as the Media Freedom Coalition and The Walkley Foundation.[1059] Ultimately, the hope is that this thesis will inspire sufficient foresight and prioritisation by policy-makers, such that they can assess the potential impact of IoT threats to the press, conduct policy analysis, and establish both deterrents and mitigations to limit risks and the extent to which their manifestation would cause harm.

[1059] Media Freedom Coalition (2022) Coalition Objectives. Available at: https://mediafreedomcoalition.org/about/objectives/coalition-objectives (accessed 13 September 2022); Graham L (2019) The Walkley Foundation's Submission to the Inquiry Into the Impact of The Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press. Available at: https://docslib.org/doc/11350449/the-walkley-foundations-submission-to-the-inquiry-into-the-impact-of-the (accessed 26 September 2022).

9.3.3 Contributions to industry

Although the previous sections outline contributions to academia and policy that affect both the media and technology sectors, this thesis has further impact specifically on the media industry. It does so in five ways: (1) First, the thesis recognised and offered suggestions for countering operational gaps within media security processes, such as obtaining timely threat intelligence. (2) Second, many of the contributions to the media industry are influenced by the NIST CSF, such as the second contribution: defining and clarifying the applicability of IoT risk to the media industry. (3) Third, the thesis provided clear resources to help systematise IoT risk management within the media industry. (4) Fourth, it humanised the countermeasures, encouraging the long-term support of media stakeholders. (5) Fifth, it contextualised IoT threats to the press by showing competing priorities, such that members of the media can allocate resources effectively. Then, this subsection briefly discusses the generalisability of research into media security.

There are several ways in which the toolkit proposed in this thesis would contribute to mitigating cyber security challenges faced by the media industry. First, Chapters 6 and 7 explicitly recognised practical gaps in media industry security processes, that were then addressed through Chapter 8 countermeasure recommendations. For example, in Chapter 7's investigation into press freedom factors, UK media participants mentioned the utility of ad hoc threat intelligence sharing networks, i.e. at after-work drinks in pubs in cities with high concentrations of news organisation buildings. Meanwhile, Australian interviewees lamented the lack of such networks due to geographical differences that meant there were fewer occasions of spontaneous socialising for employees at different news outlets. Therefore, countermeasure N (intelligence sharing) encouraged propagating and institutionalising the idea of information sharing across the media. This means that more members of the media would have access to industry-specific threat intelligence such that they can pre-emptively defend themselves against attacks that their peers are experiencing in real-time.

Second, both the framework and Chapter 5's organisational models were intended to systematise information about institutional IoT risk management, and to make it relevant to and understandable by all members of the media (per the role umbrellas in Chapter 8). They did so by demonstrating how existing cyber security guidelines, such as the NIST CSF, could be made useful for non-technical audiences. Personalisability of Chapter 8's framework of countermeasures enables members of the press to choose which IoT protections to implement, depending on their specific concerns and abilities. For example, based on what kind of threats they might be most concerned with (column D) or how quickly they need a countermeasure to be implemented (column I). The framework is interactive, intuitive (as Excel has a recognised format) and provides practical recommendations. For example, countermeasures B (IoT-free contingency plans), M (corporate maintenance of device security), O (top-down education), and P (IoT-specific risk assessments) were designed to promote investment in IoT risk prevention and mitigation by corporate actors within the media industry. Further, if countermeasures C (transparency reporting), M (corporate maintenance of device security), and Q (legal scrutiny in favour of press freedom) were successfully implemented, the subsequent shifts in policy would help to improve the industry's information security and to give institutions within the media more informed autonomy when making purchasing and collaboration decisions.

Another way in which this thesis contributes to the media industry is that it presents tools inspired by the first of the NIST CSF functions, 'Identify,' so that media stakeholders, particularly corporations, may more easily recognise and catalogue their assets and vulnerabilities. Chapter 5's organisational system of IoT devices did not identify risks itself, but it should help to systematise the risk identification and assessment

processes for relevant members of the media. Without such a model to support their comprehensive and continuous identification of centres of gravity and points of potential exploitation, journalists could struggle to understand the pervasiveness of the IoT and the threats that they pose.

A crucial way in which this thesis contributed to the long-term security of the media industry is its framing of findings and recommendations to stimulate buy-in from members of the industry, even those who have expressed in this research that there is difficulty committing to behavioural adjustments. For example, the "Beneficiaries" column of Chapter 8's framework demonstrated that securing identified assets and vulnerabilities has a direct impact on members of the media industry, to heighten the sense of responsibility felt by those engaging with the framework. As part of this contribution, this thesis highlighted that NIST's 'Protect' function is similarly important to the media industry as it is applicable to the segmentation of networks and other procedures that are vital for restricting the access and influence of the IoT regarding organisational security policies and plans.[1060] Therefore, the "Countermeasures", "Function of countermeasure" and "Media roles that are most likely to be responsible for implementation of this countermeasure" columns of the framework were intended to address this function together, to ensure that the relevant personnel in each organisation and in the industry generally are aware of the imperative for specific and stringent access control measures. Another two NIST Framework Core functions that were particularly relevant to this contribution are 'Respond' and 'Recover,' as it was important for this thesis to acknowledge that successful breaches are inevitable, rather than claiming that all threats can be effectively quelled. Therefore, this thesis argued that resilience through both agility and consistency is the most crucial part of securing the on-going provision of the products of a free press. Chapter 8 advocated for both short- and long-term measures, as demonstrated by the framework's "Feasibility" column.

This thesis additionally contributed to the media industry by increasing journalists' awareness of the existence of IoT threats as a contemporary and future issue, and by giving them the necessary context to establish priorities for resource allocation. For example, Chapters 6 and 7 provided a real-world basis for the toolkit presented in Chapters 5 and 8, so that it was founded on evidence of gaps in the resources available to the media industry across multiple countries. As such, members of the media can review these country profiles to see which competing priorities exist for the press in each country, and how domestic laws and international insecurity may exacerbate IoT threats to the press. That over one hundred participants were involved in this research speaks to the consideration given to personal, industrial, national, and international contexts when designing the toolkit,[1061] causing the versatility of the framework (including features such as workflow phases, media roles responsible for implementation, and beneficiaries of each countermeasure). One respondent hoped that this framework would encourage the media industry to lobby for laws relating to privacy that account for the needs and risks of a free press. Experts acknowledged that all of these recommendations necessitate buy-in from executive media roles. To make this clear, the framework includes the "Business/Corporate/Commercial/Organisational Stakeholders" role umbrella option for implementation responsibility and the "news organisations as businesses" option in the beneficiary column. These are both intended to demonstrate the utility of incorporating the IoT into risk management procedures for business continuity.

The research in this thesis was intended to be applicable to the media industry, but has potential generalisability for any highly-targeted communities whose adversaries are disproportionately well-

[1060] Trend Micro (2018) NIST Cybersecurity Framework Series Part 2: Protect. Available at: https://blog.trendmicro.com/nist-cybersecurity-framework-series-part-2-protect/ (accessed 23 January 2020).
[1061] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.

resourced, as it has raised interesting questions about how people perceive and react to risk. Additionally, given the selection of four democratic states across a range of sizes and geographic locations of the country profiles (see: Chapters 6 and 7), the findings from those chapters could be used to understand threats faced by the press from the IoT in similar places, such as Canada. Chapter 8's framework can also be used as a foundation for cyber security experts looking to create similar risk assessment and risk management tools for other vulnerable or highly targeted populations.

9.4 Discussion: Emerging trends and outlook

Given the far-reaching ramifications of improved journalistic security, the question remains as to whether it is possible to mitigate IoT threats or if they add to existing risk such that the press will be overwhelmed and unable to address them. It is important to remember that the media industry should not be rallying against these threats alone; they are not the only community under threat whose attackers may exploit the IoT. In fact, many of the people who journalists may need to protect in their role as communicators of information are vulnerable sources who would benefit from learning about and responding to these risks. Further, corporate, national, and international policies relating to regulation of the IoT and its data must take into account the unique position of journalists in an information ecosystem, and their heightened risk.[1062]

Interviewees for Chapters 6 and 7 opined that it is difficult for the press to trust that state actors will address these threats effectively, either through legislation or policymaking, given states' involvement in undermining journalists' cyber security. Although Taiwanese interviewees did not identify the Taiwanese government as a threat actor, there was fear that their lack of active safeguarding of press freedom facilitates attacks by other state actors, particularly China. This was also the case across all three other studied countries, as cyber-attacks and surveillance by Chinese adversaries were noted as a grave concern. There is no way to fully address the Chinese threat within the scope of this thesis, but this is such a great threat that any recommendation for mitigation, however small, seemed necessary. As such, countermeasure J (firewalls) was included in the framework, to limit the indexing of IoT devices that could be done via notorious tools such as Shodan and other IoT camera discovery and hijacking services for hire, to the extent possible.[1063]

In contrast to the Taiwanese government, the Australian, UK and US states were considered to be active threat actors by interviewees for Chapters 6 and 7. As noted in those chapters, the intelligence agencies of these three states are part of the Five Eyes network, which was recognised by interviewees as promoting a culture of hypervigilance that involves overbearing surveillance and legal threats that stifle press freedom and security. Of course, both defining a free country, and determining the extent to which states that claim to be bastions and protectors of freedom live up to their claims, are political theory questions beyond the scope of this thesis.

Further, all interviewees for Chapter 4's exploratory study identified the most likely perpetrators of cyber-attacks on journalists as actors with advanced cyber capabilities and immense political and financial

[1062] Blanchard T (2017) Journalists in Distress: Assessing the Digital Viability of a Global Emergency Assistance Network. The Digital Security of Journalists in Distress: Report 3. Toronto, Canada: Canadian Journalists For Free Expression: 30 Available at: https://d3n8a8pro7vhmx.cloudfront.net/cjfe/pages/2913/attachments/original/1484964569/Report_3_-_The_Digital_Security_of_Journalists_in_Distress.pdf?1484964569 (accessed 11 January 2020).

[1063] Benjakob O (2022) This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure - National Security & Cyber - Haaretz.com. Haaretz, 26 December. Available at: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000 (accessed 12 January 2023).

influence internationally. Named adversaries included states' intelligence and law enforcement agencies, private intelligence operations companies that spun out of militaries around the world, banks, and other well-resourced private actors. A 2022 report on Advanced Persistent Threat (APT) groups working on behalf of states such as China, North Korea, Iran and Turkey found that some of the most relentless threat actors in the world are each targeting members of the media as leverage to access their associates as part of their modus operandi.[1064] This was consistent with the idea of journalists as vectors to attacking other people, regardless of their own beat.[1065] The report noted that focusing on the press "lowers the risk of failure or discovery to an APT actor than going after other, more hardened targets of interest."[1066] This provided further evidence that countermeasures N (intelligence sharing) and O (top-down education), which promote the value of intelligence sharing, would enable the press to identify common malicious actors and their patterns of activity. This would increase the likelihood of "failure or discovery" and so reduce the ease with which such threat actors can successfully exploit any media targets. Further, this was part of the motivation for the creation of Chapter 8's framework, as a tool for members of the press to look up threats that they may face. This function may be useful to provide information on threat models that could then, through intelligence-sharing, be linked to different threat actors.

It is likewise relevant to ask whether the potential effect of the virtually unfettered spread of the consumer IoT on journalism is a harbinger of how they will affect the other pillars of democracy and all of society. This research has surfaced concerns in risk perception literature relating to encouraging people to react proportionately to problems that are both ubiquitous (as the IoT is diverse both in types of devices and range of potential threats) and part of daily life. Possible responses from readers of this thesis and users of the toolkit include burgeoning fear and obsession with IoT threats and, more likely, ignoring problems with this risk profile. None of the countermeasures proposed in Chapter 8's framework are flawless, nor will they be optimally effective in perpetuity.

9.5 Limitations

All research has inevitable limitations, for example due to decisions about scope, logistical challenges such as access and funding, and the acquisition of more data and raw participant information than can possibly be included in one doctoral project.

For instance, the IoT device organisation model in Chapter 5 is by no means comprehensive, nor does it go into significant detail when delineating between different devices, wireless networking standards, or communications protocols. However, Smith's book on IoT risk discussed the implications of Moore's Law for future IoT devices, noting that they will be vastly more powerful and advanced than today's IoT technologies, and proposing that all research does not limit the duration of its utility by setting granular distinctions between categories.[1067] Further, the acceptance of Chapter 5's IoT device environmental model to *the International Association for Media and Communication Research* 2022 conference and the

[1064] Giering C, Miller J, Raggi M, et al. (2022) *Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media*. 11 July. USA: Proofpoint US. Available at: https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists (accessed 27 September 2022).
[1065] McGregor SE (2021) Chapter 3: Assessing Risks and Threats, in: *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.
[1066] Giering C, Miller J, Raggi M, et al. (2022) *Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media*. 11 July. USA: Proofpoint US. Available at: https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists (accessed 27 September 2022).
[1067] Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2017. 240 p. 40.

warmth of its reception when published as an explainer through *The Journalist's Resource*[1068] shows a clear need for high-level resources for journalists.

Further, the measures in the framework were intended to be viewed separately to maximise fairness and utility of each value. For example, by making function and beneficiary two separate columns, the goal was for the feasibility values to be determined independently of any benefit of each countermeasure. However, it is possible that participants in the study let their opinion on the value colour the judgement about the cost, despite the imposed distinctions.

Additionally, the toolkit and the thesis overall acknowledge that within the media, there is heterogeneity in terms of roles, and there are disparities that affect access to and uptake of recommended cyber-risk mitigations. Recent mass lay-offs from large media companies have resulted in an abundance of freelance journalists without access to institutional security tools and trainings.[1069] More generally, the ubiquity of internet-connected devices, combined with the effects of the COVID-19 pandemic, has facilitated a rise in work environment flexibility, i.e. "telecommuting," particularly in terms of people who spend at least a portion of their time working from home offices.[1070] The prevalence of the IoT has also had a clear effect on the evolution of journalistic practices and institutions, demonstrated by the pervasiveness of citizen journalism online, from blogs to collectives that diverge from the formal structure formerly employed by most news organisations. This is concurrent with a trend that shows that both new and established news organisations are placing an emphasis on engaging with digital media, particularly "more immersive formats that allow a brand personality to be expressed more fully while maintaining the choice and control demanded by a younger generation."[1071]

These changes have highlighted the imperative for a better understanding of all journalists' perceptions of cyber threats, particularly under-studied ones such as those through the IoT, not just members of the press who have institutional support. The toolkit is important for improving news organisations' security, and is tailored to individual members of the media. However, freelance work may involve taking on all the roles listed in Chapter 8's countermeasures framework, which could lead to security burnout. This was one motivation for the inclusion of countermeasure disadvantages and workflow phases as columns in Chapter 8's framework. These filters should enable users to choose to implement or not to implement countermeasures based on their capacity to take on security and risk management work at a given point, and to tailor these considerations to their workflow phase. This decision was inspired in part by McGregor's note that the valuation method for a given member of the media should reflect their specific

[1068] Shere A (2021) How the Internet of Things poses a threat to journalists. In: The Journalist's Resource. Available at: https://journalistsresource.org/home/how-the-internet-of-things-poses-a-threat-to-journalists/ (accessed 5 May 2022).
[1069] Goggin B (2019) 3,200 people have lost their jobs so far this year in a media landslide. Available at: https://www.businessinsider.com/2019-media-layoffs-job-cuts-at-buzzfeed-huffpost-vice-details-2019-2 (accessed 9 September 2019); Aratani L (2022) Concern as US media hit with wave of layoffs amid rise of disinformation. *The Guardian*, 10 December. Available at: https://www.theguardian.com/media/2022/dec/10/media-layoffs-cnn-buzzfeed-gannett-recount-protocol (accessed 7 February 2023).
[1070] United States Office of Personnel Management (2016) *Status of Telework in the Federal Government: Report to Congress: Fiscal Years 2014 – 2015*. November. Washington, D.C.: United States Office of Personnel Management. Available at: https://www.telework.gov/reports-studies/reports-to-congress/2016-report-to-congress.pdf (accessed 27 February 2020): 43; Autry T (2019) *Secure IoT Compliance Behaviors Among Teleworkers*. D.I.T. Capella University, United States -- Minnesota. Available at: https://search.proquest.com/docview/2313671125/abstract/462C5E8E633348B0PQ/1 (accessed 27 February 2020).
[1071] Kleis Nielsen R, Newman N, Fletcher R, Kalogeropoulos A. (2019) *Reuters Institute Digital News Report 2019*. Oxford: Reuters Institute for the Study of Journalism (RISJ): 30.

context, rather than relying on default approaches, such as financial cost, which may be less influential than other factors.[1072]

It must also be said that all protective recommendations are imperfect, especially against well-resourced attackers. The chance of a catastrophic failure increases as the individual implementing the countermeasure experiences human stressors, such as tiredness and time constraints. There is often no guarantee that protections are working until an attack has been launched, similarly to the function of a safety mechanism on a firearm. Still, there is value in the creation and proliferation of responsible and evidence-based risk assessment and management resources.[1073] This toolkit presented in Chapters 5 and 8 is not intended to be faultless but rather to stimulate meaningful thought processes and as a practical guide for improving the way that the press conceptualises and handles IoT risk.

The framework presented in this thesis aimed to offer protections and mitigations for 19 threats, many of which can overlap and compound. Therefore, there are inevitable limitations to the countermeasures proposed, especially given the low technical knowledge and lack of time that most journalists face in considering these topics. One such limitation was noted by one expert respondent to the states' capabilities survey, who mentioned that the use of IoT protections at specific times could lead to an absence of data that could highlight those timings as being of particular interest to adversaries, thus underscoring the ceaselessness of the data collection undertaken by such technologies. Per Nissenbaum, a way of responding to this problem could be "obfuscation," increasing the amount of meaningless "noise" (irrelevant, random data) in the "noise-to-signal ratio" created to obscure any information about meaningful events (such as source meetings).[1074] This kind of protective behaviour could be considered part of countermeasure R (no clear IoT-specific countermeasure yet). However, this was not directly recommended within the framework due to concerns that users would insufficiently attempt obfuscation, for example, forgetting to obfuscate constantly and thereby only engaging in "noise-making" at times relevant to the significant activities, which does not resolve the risk. Another way in which this obfuscation could reveal more than intended would be if the "noise" were not random but instead weighted toward particular topics - such as the toolkit user's surroundings, or the subjects of their article drafts. Although obfuscation was not explicitly included in the framework, it could be part of the security training offered by media stakeholders to members of the press who have demonstrated mastery of the toolkit and work on consistently high-risk topics.

Another limitation is that mapping the capabilities of states, in particular, in terms of surveillance capabilities relevant to modelling IoT threats is challenging. States' technological capabilities and intelligence actions are by nature clandestine, and are likely to have become even more expansive since divulged in Snowden's evidence in 2013.[1075] This, juxtaposed with the disproportionately under-resourced security of the media globally, means that one cannot be certain about which of these threats have already manifested.[1076] To mitigate this risk, only threats that can be amply substantiated by academic research and news articles to be possible and even probable were included in Chapter 5's threat categorisation.

[1072] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[1073] McGregor SE (2021) Information Security Essentials. 1st ed. New York, NY, USA: Columbia University Press.
[1074] Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, Massachusetts: The MIT Press; Brunton F and Nissenbaum H (2019) The Fantasy of Opting Out. In: *The MIT Press Reader*. Available at: https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/ (accessed 9 November 2019).
[1075] Wells AR (2020) Between Five Eyes: 50 Years of Intelligence Sharing. United Kingdom: Casemate, pp. 110-111.
[1076] Lashmar P (2020) Spies, Spin and the Fourth Estate: British Intelligence and the Media. Edinburgh, Scotland: Edinburgh University Press, pp. 261-262.

Further, it could be argued that the release of this framework enables ideas on threats and countermeasures to become public, including to potentially malicious actors. When conducting and publishing this research, Phillips' guidance on responsible research and reporting on extremism was followed, with particular consideration given to minimising the potential harm and maximising the benefit to defenders.[1077] With these goals in mind, it is important to recognise that unfortunately, if a nation-state or similarly well-resourced criminal enterprise is targeting a specific journalist, the asymmetry in capabilities is too great to effectively or sustainably defend against. Additionally, the states' capabilities expert gave all threats median "future" realism scores of 4 or 5 out of 5 ("5: Totally realistic/this is already being planned/developed", "4: Somewhat realistic/this is likely to be already in the process of development"), suggesting that few, if any, of these threats are novel to attackers, and indicating the need for countermeasures known and used by defenders. However, regarding benefit, increasing the media's awareness of and protection against IoT threats would force threat actors to commit more time and resources for attacks, which may be prohibitive investments for some adversaries. It may also mean that untargeted attacks are less likely to affect members of the media and news organisations, as employing these countermeasures would afford some protection.

Additionally, states' capabilities experts were surveyed about the threats presented in Chapter 5 during the validations study, to assess the current and future realism of threats. The median results (due to the shift from the old threats "taxonomy" to the new system of categorisation, see: Appendix D and Chapter 8, section 8.3.3) show that all threats were given "current" scores of 4 or 5 out of 5 ("5: Totally realistic/this is already possible", "4: Somewhat realistic/this is probably possible"), with the exception of "legitimate interest clauses", which received a score of 3 ("3: Not sure/don't know"). The findings from the exploratory study, as well as other research conducted during this thesis show that legitimate interest clauses are already in use as a method of information access by governments, and are a concern for journalists.[1078] Further, no threats were seen as becoming less realistic over time. This therefore supports the inclusion of these threats not just from academic literature, news reports, but also current experts in the field. Even though this thesis cannot comprehensively cover every possible IoT threat to journalists, nor know all resources at the disposal of their adversaries, there is utility to its imperfect (but evolving) tools that enable members of the media to begin consciously practising making judgements regarding estimated risk.[1079]

Finally, given the importance of the other three functions and how integral they are to the research (see above), the lack of focus on the NIST "Detect" function could be seen as a limitation. However, this decision was undertaken in response to the journalism-specific IoT-threat models explored in Chapter 5, which are characterised by their ability to appear accidental, as well as the challenges of attribution in the media environment where attackers may be highly skilled and resourced. Combined with the participant interviews that inform the country profiles presented in Chapters 6 & 7, this thesis is motivated to solve the presented user issue of protections and mitigations, not more precise detection of attackers. Some literature, such as NIST's report on 'Security and Privacy Controls for Federal Information Systems and

[1077] Phillips W (2018) The Oxygen of Amplification. Report, 22 May. USA: Data & Society Research Institute. Available at: https://apo.org.au/node/172901 (accessed 1 December 2022).
[1078] Shere ARK (2020) Now you [don't] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy* 5(3). Routledge: 429–448. DOI: 10.1080/23738871.2020.1832129; Shere ARK, Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.
[1079] McGregor SE (2021) *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.

Organizations,' provides highly detailed guidance that advises organisations on how to develop "policy- and technology-neutral" privacy and security controls.[1080] However, such guidance is often highly detailed and technical – for example, the aforementioned report is 462 pages – which can reduce the likelihood that it is read completely, understood, and put into effect by all the relevant parties. Further, this thesis' references to the NIST CSF should not be viewed uncritically. NIST is a US government agency whose work has been subverted in the past by a national intelligence agency in precisely the manner that this thesis's research participants from the media have so feared, although it remains an accepted standard that is made useful through interpretation for non-technical user groups.[1081]

9.6 Future work

There are many ways in which this thesis may motivate future research and the professional enhancement of the toolkit. Regarding the former, the literature syntheses in Chapters 2 and 5 illuminated areas for further interdisciplinary study relating to IoT threats, factors affecting press freedom, and categorisation of consumer IoT devices.

Future academic work may extend this toolkit to include resources for members of the press who have experienced IoT-facilitated threats. This includes those who require support as they process the emotional, social, professional and financial ramifications of such attacks, as shown by Rostami *et al*., who note the need for methods of harm alleviation with respect to the IoT.[1082] Another area for further work is investigating whether the overall goal of safeguarding journalistic security and press freedom is achievable, or whether adversary-defender asymmetries are too great to overcome. This would also involve investigating in greater detail how IoT threats would manifest if enacted by non-state actors and by states other than those profiled for this thesis.

Another underexplored risk that would benefit from future research, and consideration by policymakers, is that some data that governments access may need to be erased, but the difficulty of this can further complicate data protection. For example, after the Birney and McCaffrey raid was declared unlawful by the UK High Court, the journalists' lawyers contended that the electronic materials seized and copied by law enforcement must be comprehensively deleted.[1083] However, the police claimed that this "would cost tens of thousands of pounds for them to adequately scrub this from their systems – because it was stored on a police database and backed up"[1084], and agreed to delete the amount that they could, in a staggered fashion.[1085] This case suggests that journalists need to consider the potential for confidential digital files to be replicated such that they become ineradicable, thereby adding a new logistical layer to legal threats, because this then means that data must be well-protected indefinitely, lest it be attacked while held by state agencies. Conversely, Chiou wrote about the legal right to be forgotten in Taiwan, which is intended

[1080] NIST Joint Task Force Transformation Initiative (2015) *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication (SP) 800-53 Rev. 4, 22 January. Gaithersburg, MD: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-53r4.

[1081] Kostyuk N and Landau S (2022) Dueling over Dual_EC_DRGB: The Consequences of Corrupting a Cryptographic Standardization Process. *Harvard National Security Journal* 13(2): 1–61.

[1082] Rostami A, Vigren M, Raza S, et al. (2022) Being Hacked: Understanding Victims' Experiences of {IoT} Hacking. In: *Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA, USA, 8 August 2022, pp. 613–631. USENIX Association. Available at: https://www.usenix.org/conference/soups2022/presentation/rostami (accessed 19 September 2022).

[1083] Interviewee: P44

[1084] Interviewee: P44

[1085] Goodwin B (2020) NI police unable to delete data seized unlawfully from journalists for 10 years. Available at: https://www.computerweekly.com/news/252489306/NI-Police-unable-to-delete-data-seized-unlawfully-from-journalists-for-10-years (accessed 28 October 2022).

to enshrine privacy for members of the public[1086], but may not be possible with an increase in data collection mechanisms (such as due to the expansion of the IoT). Chiou noted that the right to be forgotten is only indirectly enshrined in Taiwanese law and that, while it must be balanced with the press's right to publish, individuals' right to a clean slate is also essential for democracy. As such, both future academic and policy research should focus on the conflicting risks and challenges of data that cannot be erased, particularly relating to media freedom.

With respect to the toolkit, there are trainings, tools to be designed, and threat models that individual journalists and media organisations could adopt in future to further protect against threats from the IoT. For example, to enhance the user experience of this framework and to develop it from a prototype into a publicly available product, the validation study experts suggested that the framework be turned into a simple document. This would possibly take the form of a checklist that emphasises the "hands-on" actions that individuals can enact, that could be used to design both security training and organisational security policies. According to the feedback, the former would require standardisation across the industry, and the latter would require implementation timelines and integration into editorial workflows. Another example could be the development of the threat categories and their hypothetical examples in Chapter 5 into vignettes for use in journalist security training materials.

Despite not explicitly discussing the IoT, Pierce *et al.*'s paper was interesting for its identification of the distinction between toolkits developed by small nonprofits, compared with larger and governmental organisations: they "found few examples of government and corporate sponsored toolkits that address specific differential vulnerabilities, such as those of journalists."[1087] During this research project, collaboration was undertaken with the media trade organisation, the Association for International Broadcasting (AIB). With the AIB, it may be possible to partner with large media corporations and governments to encourage recognition and use of the toolkit.

The commercialisation of the toolkit could lead to it being converted into a series of online interactive tools, which could make it more useful and accessible. This could mean that users interested in the organisational models could click on an environment category and see device types that might be found there, or click on a kind of IoT threat and see scenarios that are journalism-specific. Further, adding hover text for complex points would avoid cluttering the framework while still allowing the addition of threat descriptions, giving options for expansion of diagrams so that information is not overwhelming for viewers.

9.7 Conclusion

This thesis determined how members of the press in democratic countries can improve their identification of, protection from, and resilience against threats from the Internet of Things. This work is intended to raise awareness of the ways in which democracies are threatened by the casual proliferation of IoT devices, and the extent to which they may be bowing to geopolitical and internal pressures to decrease freedom of the press. The creation of a novel threats categorisation to model and manage risk in a branch of critical national infrastructure has potentially far-reaching consequences, as increasing democratic safeguards, such as protection of the press, helps to limit the adversary-defender asymmetry shown

[1086] Chiou W-T (2020) Limits and Prospects of the Right to Be Forgotten in Taiwan. In: Werro F (ed.) The Right To Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia. Ius Comparatum - Global Studies in Comparative Law. Cham: Springer International Publishing, pp. 311–318. DOI: 10.1007/978-3-030-33512-0_16.
[1087] Pierce J, Fox S, Merrill N, et al. (2018) Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. Proceedings of the ACM on Human-Computer Interaction 2(CSCW): 139:1-139:24. DOI: 10.1145/3274408.

through the in-depth investigation of challenges facing the press in four countries: the US, UK, Australia, and Taiwan.[1088] Ultimately, the toolkit presented in this thesis was created to improve the problem recognition capabilities and the ease of mobilisation for prevention of future IoT threats by media stakeholders, ranging from individual journalists to policy-makers.

A major objective of this research project has been to make the concept of IoT threats to the media and the subsequent destructive consequences for press freedom and democracy more easily comprehensible. With the goal of narrative communication, this research lends itself to a re-thinking of the Black Swan theory of risk: The idea of a Black Swan in risk literature is a metaphor for rare events that have a severe impact and for which people are unprepared due to perceived low likelihood.[1089] The phrase originates from the fact that black swans (the bird) had previously been misperceived by Europeans as impossible, and the discovery of one black swan destabilised an entire system of thought. As such, Black Swan events are seen as entirely unpredictable and high-impact. However, in some parts of the world, such as Western Australia, black swans are common sights, and so do not have this outsized effect on world-view for those who regularly see them. This thesis seeks to demonstrate that IoT risk for the media is currently widely characterised as though it is a mythological European Black Swan, when in fact it is more common than realised. Similarly, emerging technology, for example IoT devices, are much more commonly threats to the journalists and the free press than might be popularly perceived. This thesis has worked to demonstrate that the popular perception of rarity is no longer warranted in this arena, especially as IoT devices become more prevalent, more embedded, and therefore less noticeable.

Stricter regulation, per the 'Contributions to Policy' section of this chapter, would eliminate some of the potential for distress and inertia experienced by individuals who must deal with IoT threats. As argued by Rendall, when such high-impact risks materialising is "just a matter of time", adequate preparation by policy-makers is key to preventing widespread procrastination in the hope that a quick and easy technological solution will appear.[1090] As with "tragedies of the uncommons,"[1091] the risk of IoT threats is easily underestimated by those who have not experienced them. But targeting members of the press has the potential to affect unknowing swathes of the public, which attackers may anticipate will have knock-on effects for stability in a given democracy. It is important that decision makers in the media, cyber security research and technology development, and policy and law, recognise and accurately conceptualise and frame IoT risk so that it can be addressed before it becomes an inevitable threat to journalism across the globe.

[1088] Kazansky B (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society 8(1). SAGE Publications Ltd: 2053951720985557. DOI: 10.1177/2053951720985557.
[1089] Orlik A and Veldkamp L (2014) Understanding Uncertainty Shocks and the Role of Black Swans. Working Paper Series 20445, Working Paper. National Bureau of Economic Research. DOI: 10.3386/w20445.
[1090] Rendall M (2022) Nuclear war as a predictable surprise. *Global Policy* 0(0): 1–10. DOI: 10.1111/1758-5899.13142.
[1091] Wiener JB (2016) The Tragedy of the Uncommons: On the Politics of Apocalypse. *Global Policy* 7(S1). John Wiley & Sons, Ltd: 67–80. DOI: 10.1111/1758-5899.12319.

Appendices

Appendices from Chapter 4: Exploratory Study

Appendix A: Interview Guide

Hello, thank you for meeting with me today. My name is Anjuli and I am conducting PhD research in cyber security, specifically focusing on improving the cyber security of the media sector. I chose this theme because I have experience of journalism and the media industry more generally and I feel that it is an important but often overlooked part of Critical National Infrastructure that requires more attention.

The aim of this interview is to gain insight into your cyber security perceptions and practices as a member of the media industry. Can I just confirm that you're happy to discuss this topic, particularly relating to cyber-threats against journalists' devices, and your understanding and experience of the area?

- This interview should only take roughly 60 minutes. You are welcome to cut it short at any point, but is this time-scale convenient for you?
- Are you happy for this interview to be recorded digitally and for me to make occasional notes? You can ask for me to stop recording at any point.
- Are you happy for me to directly quote your responses in any subsequent research output? [ASK AGAIN AT THE END OF THE INTERVIEW]
- Have you had time to read through the information sheet and consent form that I sent you?
- Do you have any questions about this preliminary material?
- Are you happy to proceed with the interview on this basis? [RECORD ORAL CONSENT GIVEN]

1. In order to help you understand the equipment and systems we are researching, which of these devices do you use?
    - Laptop/desktop computer
    - Smart phone/ tablet
    - Smart TV
    - Voice operated assistant, i.e. Alexa, Google Home etc.
    - Wearable smart technology, e.g. fitness trackers, smart watches
    - Cloud Storage
    - Location tracking devices, i.e. sat nav, "find my phone," "find my keys"
    - Smart phone-enabled locks, i.e. remote-access door locks
    - Smart toys, e.g. gaming systems, children's toys, recreational use drones
    - Internet-connected cars
    - Internet-connected security systems
    - Internet-connected HVAC and lighting systems
2. Let us now look at your general journalism experience. How long have you been a journalist? (must be at least 1 year)
3. What motivated you to become a journalist?
4. Do you specialise in any particular journalism area and within your career what general areas of journalism have you covered?
5. What motivated you to specialise in this/these areas?
6. Have you worked in any other jobs other than journalism within your career?

Let us now turn to cyber security and the risks to journalists from the IoT and more generally the "online" world we all now inhabit.

7. Is cyber security something that you consider while carrying out your day-to-day work?
8. Do you think that cybersecurity is relevant to your work as a journalist? If so, how?
9. Is cyber security a subject element of your journalism?
10. Have you been the target of any digital attacks? If yes, please give details
11. What distinctions, if any, do you perceive between the following four categories:
    a. "internet-enabled devices,"
    b. "internet-connected devices,"
    c. "Internet of Things devices" or
    d. "smart devices."

In this interview, the phrase "Internet of Things" will be used to refer to "'smart' [i.e. analytically capable], internet-connected devices that can share data with each other, creating a 'network' of devices."[1092]

12. Do you have any concerns about these sorts of devices?
13. Are there any of these devices you would not use and for what reasons?
14. Do you have any privacy concerns about any of these devices?
15. Would you say your use/views of these devices are typical of journalists you know?
16. What knowledge do you have of cyber-attacks on journalists' devices? // What knowledge do you have of cyber-attacks on journalists?

Let us look at what you think about the people who are attacking journalists.

17. Who would you consider being the perpetrators of these threats?
18. What do you think are the objectives of cyber-threat actors who are targeting journalists?
19. How at risk do you feel, as a journalist, with respect to exploitation of new technologies like Internet of Things devices?
20. How do you think that threats against journalists and their sources have evolved with the introduction and expansion of Internet of Things devices?
21. To what extent do you perceive threats to you from or via Internet of Things devices?

Let us now look at threats that are not cyber based: (Age of interviewee will be a factor in this question)

22. As a journalist, did you experience threats before Internet of Things devices became very popular?
    a. What sort of other threats did you experience?
23. What other threats were you aware of?
24. Are you concerned with the IoT's increased potential for attacks to jump from the cyber realm into the physical world?
25. Are you aware of any combined threats that involve cyber and non-cyber-attacks?

Let us now move on to your personal cyber security strategies.

26. Would you say you have personal cyber security strategies?
27. What are your strategies or tactics for protection of your Internet of Things devices against cyber-attacks?/ What are your strategies for defence against IoT-related threats?
28. Are these specific to your profession or generic, and in what way are they specific if they are?
29. Has your approach to source protection changed in light of your understanding of new and evolving cyber-threats, specifically related to Internet of Things devices?
30. Do you warn your sources about Internet of Things device-related risk to their anonymity and security?

There have been many examples of journalists being subject to surveillance, censorship, and intimidation specifically by governments and law enforcement agencies. Sometimes what would be

[1092] "Tech Abuse: How Internet-connected Devices Can Affect Victims of Gender-based Domestic and Sexual Violence and Abuse," UCL, accessed July 2018, , https://www.ucl.ac.uk/steapp/sites/steapp/files/gender-iot-tech-abuse.pdf, appendix 3

discerned as friendly states. These state players are making greater use of internet-enabled device exploitation. So, let's now look at governments and law enforcement agencies' Internet of Things exploitative capabilities as they relate to you and your work. We are not looking for general or rumoured issues but ones you have personally encountered, and we understand the potential sensitivity of this so it will be kept highly confidential.

31. Given any sensitive topics that you may have covered, do you feel there is a threat to you from any country's governments or law enforcement agencies?
32. What do you believe the threat is, can you describe it?
33. If you are willing to say, which countries and which agencies?
34. If you are not willing, can you say why you are not willing to identify them?

Looking to the future for journalists.

35. From your knowledge of the industry, do you think that journalists are becoming more aware of cyber-threats and effectively protecting themselves?
36. Whose responsibility is it to improve journalists' understanding of threats through IoT devices? (i.e. the journalists themselves, device suppliers, media organisations, etc.)
37. Do you need better technical systems as well as knowledge?
38. Is there an aspect of journalists' cyber security that you feel is disproportionately overlooked?

…….and finally

39. Do you have anything you'd like to add or comment on?

Thank you very much for taking the time to talk to me. I can't stress enough how useful these interviews are in trying to assess the current state of journalists' cyber security.

Is there anyone else that you could recommend as a relevant contributor to this research?

Appendix B: Association for International Broadcasting survey matrix

(With thanks to the AIB for their support and assistance with this research)

Online questionnaire hosted at:
https://docs.google.com/forms/d/e/1FAIpQLScPg9dXLe2LjQk1frmx4OfGDwf5hkxB1SmmpiT3ZKx0LVhgxQ/viewform

Please consent to your answers being used (and potentially directly quoted) in future research conducted by Anjuli Shere and/or the Association for International Broadcasting.

- Age (Optional)
- Gender (Optional)
- Nationality (Optional)

1. In this project we are interested in the following devices/systems listed. To enable us to better understand your perspective, could you let us know which of these you use?
    a. Laptop/desktop computer
    b. Smart phone
    c. Smart TV
    d. Voice operated assistant, e.g. Alexa, Google Home etc.
    e. Wearable smart technology, e.g. FitBits, smart watches, etc.
    f. Internet-connected security systems
    g. Internet-connected HVAC and lighting systems
    h. Cloud Storage
    i. Location tracking devices, i.e. sat nav, “find my phone,” “find my keys”
    j. Internet-connected cars
    k. Smart phone-enabled locks
2. Do you believe there is a difference between Internet of Things devices, internet-enabled devices, internet-connected devices, and smart devices?
    a. If yes: How do you perceive these differences?
    b. If no: How would you define this group of technologies?
3. How long have you been a journalist?
4. Do you specialise in any particular journalism area? If so, in which area?
5. Do you think that cyber security is relevant to your work?
6. Is cyber security a subject element of your journalism?
7. Have you been the target of any digital attacks?
    a. If so, how many?
8. Do you have security or privacy concerns about internet-enabled smart devices (such as voice assistants, smart watches, smart fitness trackers, smart home appliances, etc.)? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones.
    a. If yes, how are these concerns related to your work as a journalist?
    b. Would you say you are typical of journalists you know in terms of their view of these new kinds of devices?
9. How at risk do you feel, as a journalist, with respect to third-parties exploiting data from new internet-enabled smart devices? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones. RATE 1 (low risk) to 10 (high risk)
    a. Why do you feel this level of risk?

10. Would you say you have professional cyber security strategies against exploitation of new devices? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones.
11. What are your strategies or tactics for the protection of your new internet-enabled devices against cyber-attacks? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones.
12. How do you preserve the integrity and confidentiality of your sources in light of the threats posed by potential internet-enabled device exploitation of new devices? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones.
13. Do you warn your sources about risks associated with their internet-enabled devices to their anonymity and security? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones.
14. Given any sensitive topics that you may have covered, do you feel there is a threat to you from any country's governments or law enforcement agencies?
    a. If you are willing to say, which countries and which agencies?
    b. If you are not willing, can you say why you are not willing to identify them?
15. From your knowledge of the industry, do you think that journalists are becoming more aware of cyber-threats to themselves and their work through new internet-enabled devices? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones.
16. From your knowledge of the industry, do you think that journalists are adequately protecting themselves from cyber threats to them through new internet-enabled devices? This question does not pertain to more mature devices such as laptops, tablets, desktops, and phones.
17. Do you think more needs to be done in your profession to improve journalists' understanding of cyber security of these new devices (not just laptops, tablets, desktops, and phones)?
    a. If yes, whose responsibility is this? (i.e. the journalists themselves, device suppliers, media organisations, etc.)

Appendix C: Academic experts in cyber security survey matrix

Online questionnaire hosted at: https://oxford.onlinesurveys.ac.uk/iotthreats

Page 1: General information about the study

PROJECT TITLE: Securing a Free Press inside a Networked Panopticon: The case of the Internet of Things
SURVEY OBJECTIVE: The main objective of this survey is to find out what, if anything, can be done to counter threats to the public through the Internet of Things. This research project as a whole focuses on perceived threats to journalists through Internet of Things devices.

Page 2: Informed consent

We appreciate your interest in participating in this questionnaire/ online survey.
You have been invited to participate as you are over the age of 18 and have experience conducting academic research in the area of cyber security. Please read through these terms before agreeing to participate by ticking the 'yes' box below. You may ask any questions before taking part by contacting the researcher (details below).

I, Anjuli Shere (doctoral researcher in Cyber Security at the University of Oxford) am investigating threats associated with the Internet of Things. The following online questionnaire contains 6 questions and only requires your thoughts on the dangers associated with the Internet of Things. It should take roughly 10 minutes, if you are willing to spend time answering some of the open questions.

The resultant data will be analysed by Anjuli Shere and will be accessible by her supervisors and supporters of the project within the University of Oxford.

Do you have to take part?

Please note that your participation is voluntary. You may withdraw at any point during the questionnaire for any reason, before submitting your answers, by closing the browser.

How will your data be used?

Although every reasonable effort has been taken, confidentiality during actual internet communication procedures cannot be guaranteed.
Your data may be used in academic publications. Your IP address will not be stored.
Research data will be stored for a minimum of three years after publication or public release, according to university policy.

Who will have access to your data?

This survey is being conducted via 'Bristol Online Surveys,' which is fully compliant with all UK data protection laws. 'Bristol Online Surveys' is the data controller with respect to your personal data and, as such, will determine how your personal data is used. Please see their privacy notice here [https://www.onlinesurveys.ac.uk/terms-and-conditions/]. 'Bristol Online Surveys' will share only anonymised data with the University of Oxford, for the purposes of research. Your data is automatically anonymised because no names or IP addresses will be recorded.

Your information may be shared with supervisors and members of the project. We would like your permission to use your anonymised data in future studies. Any personal information that could identify you will be removed or changed before files are shared with other researchers or results are made public. Responsible members of the University of Oxford and funders may be given access to data for

monitoring and/or audit of the study to ensure we are complying with guidelines, or as otherwise required by law.

This questionnaire is for a DPhil (doctoral) project. The principal researcher is Anjuli Shere, who is currently attached to the department of Computer Science at the University of Oxford. This project is being completed under the supervision of Dr. Ivan Flechais (University of Oxford) and Dr. Jason Nurse (University of Kent).

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee. Reference number: CS_C1A_10_017

What if there is a problem?
If you have a concern about any aspect of this project, please speak to the researcher, Anjuli Shere (anjuli.shere@cybersecurity.ox.ac.uk), or their supervisor, Dr. Ivan Flechais (ivan.flechais@cs.ox.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant Chair of the Research Ethics Committee at the University of Oxford: Chair of the Computer Science Departmental Research Ethics Committee; Email: ethics@cs.ox.ac.uk; Address: Wolfson Building, Parks Road, Oxford OX1 3QD. The Chair will seek to resolve the matter in a reasonably expeditious manner.

Please note that you may only participate in this survey if you are 18 years of age or over.
☐ I certify that I am 18 years of age or over.

If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started.
☐ Yes, I agree to take part

We would like your consent to quote some of your responses in any research output, e.g. published papers. If you consent to this, please check the box below.
☐ Yes, I consent to my responses being quoted in any research output

Page 3: Survey

1. Please rate the level of your knowledge about cyber security: [Likert Scale with 5 levels based on knowledge]
2. What do you think are the digital threats associated with the use of smart devices and the Internet of Things? [Free text box]
3. What do you think are the physical threats associated with the use of smart devices and the Internet of Things? [Free text box]
4. To what extent do you think members of the general public are able to opt-out of their use of smart devices and the Internet of Things now? [Can opt-out/Can't opt-out]
5. To what extent do you think members of the general public will be able to opt-out of their use of smart devices and the Internet of Things in the future (e.g. over the next 5 years)? [Will be able to opt-out/Won't be able to opt-out]

6. What do you think are some of the ways in which members of the public are able to mitigate digital and physical threats associated with the use of smart devices and the Internet of Things? [Free text box]

Page 4: Thank you

Thank you for your involvement in this survey! If you have any questions about the research or how your responses will be used, please contact Anjuli Shere at anjuli.shere@cybersecurity.ox.ac.uk

Appendices from Chapter 5: Conceptual Models

Appendix D: Old "Taxonomy" of IoT threat models

The following taxonomy was the first draft of Chapter 5's categorisation of IoT threats that have the potential to particularly harm journalists' work and wellbeing, first relating to information, and then how those threats to information may burgeon into legal and material threats. The threats to information are: (1) Stealing information, (2) tracking journalists and sources, (3) altering information, (4) assuming control over intended device functionality to discredit or physically harm journalists, and (5) limiting device functionality. All categories of threat offer examples to illustrate the ways in which they would specifically harm press freedom.

These five categories of threat involve varying degrees of risk, with the severity of different threats depending on the individual circumstances and work of each journalist, their colleagues, and their sources. However, given existing news coverage of similar threats, the most likely categories to occur are 1[1093], 2[1094], and 5.[1095]

1. Stealing information from journalists

The news media relies on the dissemination of factual information and maintenance of source confidentiality. Theft of information could threaten one or both of these hallmarks, thereby undermining journalism.

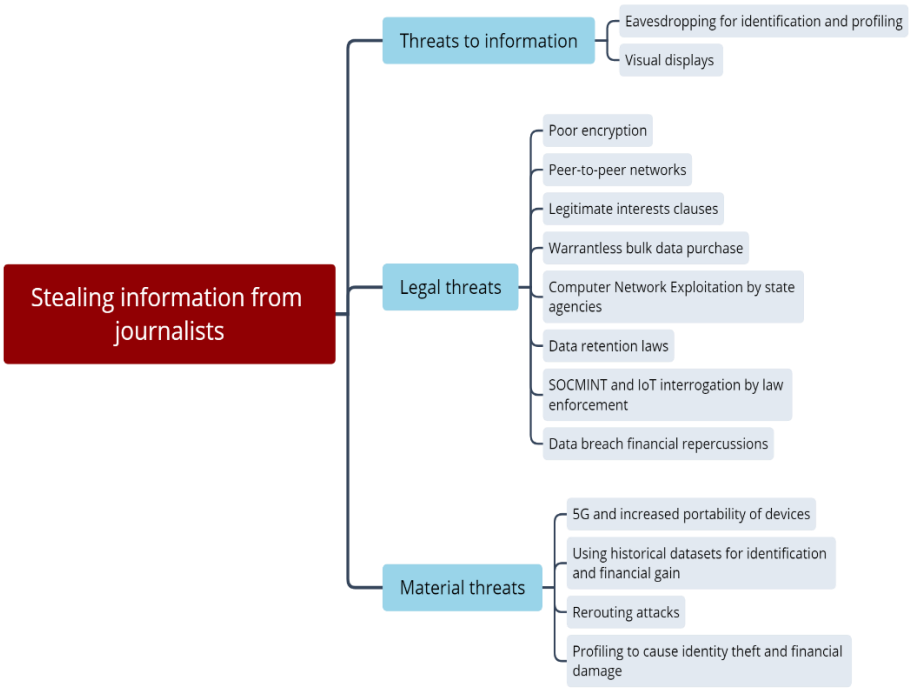


Figure 18: Stealing information from journalists

[1093] MEAA. 2019. Journalist Information Warrants. *Medium*. Retrieved December 31, 2020 from https://pressfreedom.org.au/journalist-information-warrants-d47b402ae071.
[1094] Ryan Nakashima. 2018. AP Exclusive: Google tracks your movements, like it or not. *AP NEWS*. Retrieved September 9, 2019 from https://apnews.com/828aefab64d4411bac257a07c1af0ecb.
[1095] Vittoria Elliott. 2021. Four ways governments disrupt internet access. *Rest of World*. Retrieved May 4, 2021 from https://restofworld.org/2021/four-ways-governments-disrupt-internet-access/.

1.1 Threats to information

IoT devices and apps often have poor inbuilt security and privacy measures.[1096] There is therefore a high risk that information will be shared without consent with third parties, from lurking adversaries to performance monitoring organisations. Information theft through IoT devices can be carried out through a variety of different technical mechanisms, for example:

Eavesdropping for identification and profiling: Access level attacks on IoT systems target system availability and can be passive or active, including monitoring and eavesdropping.[1097] This ongoing access to information presents the dual issues of both identification of individuals and profiling.[1098] There is also the possibility of devices with microphones picking up the sounds of nearby typing patterns, to allow reconstruction of messages sent, which could compromise confidential communications even when sent through secure channels.[1099]

Visual displays: Some ambient consumer IoT devices visually display information that owners would prefer not to be shared with bystanders, which could be problematic for journalists whose homes are visited by law enforcement officers, even if they do not have warrants to seize devices.[1100]

1.2 Legal threats

Lax security and privacy by design requirements: Poor inbuilt IoT security results from lax legal restrictions regarding security and privacy by design. Data is left vulnerable because, e.g. security settings are configured to an inadequately low default, and it is unclear how users can alter them.[1101]

Poor encryption: There is currently no legal or financial incentive for manufacturers to encrypt data or otherwise increase the security of purchased devices. This leaves endpoint management unsupported as devices have out of date firmware or software that can be exploited through well-known channels.[1102]

Peer-to-peer networks: For reasons such as maintenance, IoT device manufacturers can legally ensure that devices continually upload data to, e.g., peer-to-peer networks that are coordinated by the

---

[1096] Ignacio Sanchez, Riccardo Satta, Igor Nai Fovino, Gianmarco Baldini, Gary Steri, David Shaw, and Andrea Ciardulli. 2014. Privacy leakages in Smart Home Wireless Technologies. DOI:https://doi.org/10.1109/CCST.2014.6986977; Mikko Hypponen and Linus Nyman. 2017. The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. *Technology Innovation Management Review* 7, 4 (2017), 7.

[1097] Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834; Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1098] Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658; Jide S. Edu, Jose M. Such, and Guillermo Suarez-Tangil. 2019. Smart Home Personal Assistants: A Security and Privacy Review. *arXiv:1903.05593 [cs]* (March 2019). Retrieved August 21, 2020 from http://arxiv.org/abs/1903.05593; Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

[1099] Layal Liverpool. 2020. Voice assistant recordings could reveal what someone nearby is typing. *New Scientist*. Retrieved January 1, 2021 from https://www.newscientist.com/article/2261844-voice-assistant-recordings-could-reveal-what-someone-nearby-is-typing/.

[1100] Karen Levy and Bruce Schneier. 2020. Privacy threats in intimate relationships. *J Cyber Secur* 6, 1 (January 2020). DOI:https://doi.org/10.1093/cybsec/tyaa006.

[1101] Mary C. Kay Michel and Michael C. King. 2019. Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In *2019 IEEE International Symposium on Technology and Society (ISTAS)*, IEEE, Medford, MA, USA, 1–7. DOI:https://doi.org/10.1109/ISTAS48451.2019.8938009.

[1102] Stacie Hoffmann. 2018. *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. IoT Security Foundation, Oxford, United Kingdom. Retrieved August 12, 2020 from https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf.

manufacturer, regardless of the length of the chain of components and actors within these networks.[1103] Data collected by consumer devices is therefore made accessible to an indeterminate number of parties, regardless of the knowledge or active consent of device owners.[1104]

Legitimate interest clauses: Data protection laws intended to protect individuals' personal data from unwarranted collection or access and exploitation by third parties usually include provisions for their negation for legitimate interest.[1105] This allows governments and associated corporations to justify their access to and use of data and metadata, including from the IoT.[1106] This includes data that may be associated with journalists or sources, without violating pre-existing legal protections for journalists and whistleblowers.[1107]

Warrantless bulk data purchase: Government agencies and private companies can legally sidestep warrant requirements by purchasing bulk user data from service providers, including those that are involved in the maintenance of IoT devices.[1108]

Computer Network Exploitation by state agencies: Representatives of intelligence agencies of democratic states have openly stated their intention to use poorly secured IoT devices to pivot into a network and gather data on users,[1109] including credentials that would give them access to more secure systems.[1110]

Data retention laws: Data retention laws may be vague on whether they consider clearly identifiable data from IoT devices to constitute metadata. Australian metadata retention laws still require metadata storage for a minimum of two years. There is already evidence that these laws have chilled the Australian press, as well as counteracting some of the protections of pre-existing source shield laws.[1111]

SOCMINT and IoT interrogation by law enforcement: Law enforcement's use of social media analysis, cross-referenced with interrogation of portable IoT devices belonging to individuals who are suspected

[1103] Brian Krebs. 2016. This is Why People Fear the 'Internet of Things.' *Krebs on Security*. Retrieved December 31, 2020 from https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/comment-page-1/#comments.

[1104] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. 2019. "I don't own the data": end user perceptions of smart home device data practices and risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (SOUPS'19), USENIX Association, USA, 435–450.

[1105] Information Commissioner's Office. 2019. Data Protection Act 2018: For Organisations. Retrieved May 28, 2019 from https://ico.org.uk/for-organisations/data-protection-act-2018/.

[1106] Anjuli Shere. 2020. Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis. *The New Collection* 14, (2020), 3–21.

[1107] Anjuli R. K. Shere. 2020. Now you [don't] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy* 5, 3 (September 2020), 429–448. DOI:https://doi.org/10.1080/23738871.2020.1832129.

[1108] Simon Anell, Lea Grober, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. In *The 5th European Workshop on Usable Security*, IEEE, Genova, Italy, 10. Retrieved from https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf; Joseph Cox. 2020. Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal. *Vice*. Retrieved September 11, 2020 from https://www.vice.com/en_ca/article/k7qyv3/customs-border-protection-venntel-location-data-dhs; Joseph Cox. 2020. The Loophole the DMV Uses to Sell Your Data to Private Investigators. *VICE*. Retrieved September 11, 2020 from https://www.vice.com/en_us/article/ep47na/dmv-dppa-drivers-privacy-protection-act-buy-data-private-investigators.

[1109] Jenna McLaughlin. 2016. NSA Looking to Exploit Internet of Things, Including Biomedical Devices, Official Says. *The Intercept*. Retrieved October 26, 2020 from https://theintercept.com/2016/06/10/nsa-looking-to-exploit-internet-of-things-including-biomedical-devices-official-says/.

[1110] Spencer Ackerman and Sam Thielman. 2016. US intelligence chief: we might use the internet of things to spy on you. *The Guardian*. Retrieved October 26, 2020 from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

[1111] Benedetta Brevini. 2017. Metadata Laws, Journalism and Resistance in Australia. *Media and Communication* 5, 1 (March 2017), 76–83. DOI:https://doi.org/10.17645/mac.v5i1.810.

of attending protests, chills the press by creating a fear of identification and reprisals both among sources and journalists gathering information on the ground.[1112]

Data breach financial repercussions: Given the lack of funding available to many news organisations, the vague guidance inherent in data protection legislation such as the GDPR, and a media-industry-wide culture of under-prioritisation of security, it would be easy to identify IoT devices as being part of a news organisation's networks and to exploit their inherently poor security to cause data breaches. This would likely trigger devastating financial pressures, including regulatory fines, investigation costs and compensation payments that would force the news organisation to lay off some of its staff.[1113]

1.3 Material threats

5G and increased portability of devices: 5G may enable IoT devices that were previously kept in one location and connected to Wi-Fi to gain portability in private and public spaces.[1114] This could enable, for instance, an adversary planting even a basic consumer IoT device, such as a cheap wireless voice assistant, under a table in a newsroom, connecting it to 5G because the news organisation's Wi-Fi is password-protected, and configuring it to transmit all conversations within range. While this is something that could happen via 4G or via hacking the Wi-Fi network, the increased speed of 5G makes this more attractive to adversaries.

Using historical datasets for identification and financial gain: Even if a user can purge the logs held on an old device after years of ownership, they may never know how many times that data was transmitted, accessed, consolidated, or sold prior to the purge. This creates a rich dataset from which adversaries may isolate key dates and events, in order to cross-reference these with information gathered on suspected sources, thereby definitively identifying a confidential source. Similar online datasets are lucrative and there are already academic proposals for ways in which service providers can sell IoT datasets to advertisers and other third parties.[1115]

Rerouting attacks: Due to the poor inbuilt security of IoT devices, there have already been recorded instances of accidental malfunction, such as when voice assistants have recorded more audio data than intended and have sent this to members of the user's contacts list.[1116]

Profiling to cause identity theft and financial damage: The rich datasets that are created by the varied and interlinked consumer IoT devices that comprise smart home systems without sufficient network segregation enable user profiling, which can cause identity theft and financial damage.[1117]

[1112] Access Now. 2020. New world disorder: digital attacks on freedom of assembly. *Access Now*. Retrieved September 11, 2020 from https://www.accessnow.org/new-world-disorder-digital-attacks-on-freedom-of-assembly/.

[1113] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J Cyber Secur* 4, 1 (January 2018). DOI:https://doi.org/10.1093/cybsec/tyy006.

[1114] Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658.

[1115] Hidayet Aksu, Leonardo Babun, Mauro Conti, Gabriele Tolomei, and A. Selcuk Uluagac. 2018. Advertising in the IoT Era: Vision and Challenges. *arXiv:1802.04102 [cs]* (January 2018). Retrieved September 11, 2020 from http://arxiv.org/abs/1802.04102.

[1116] Jide S. Edu, Jose M. Such, and Guillermo Suarez-Tangil. 2019. Smart Home Personal Assistants: A Security and Privacy Review. *arXiv:1903.05593 [cs]* (March 2019). Retrieved August 21, 2020 from http://arxiv.org/abs/1903.05593; Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660; Hamza Shaban. 2018. An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says - The Washington Post. *The Washington Post*. Retrieved September 13, 2020 from https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/.

[1117] Simon Anell, Lea Grober, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. In *The 5th European Workshop on Usable Security*, IEEE, Genova, Italy, 10. Retrieved from https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

2. Tracking journalists and sources

Tracking journalists and sources poses a threat to confidentiality that could ultimately chill the press. Knowledge of their pattern of life may also facilitate physical attacks.

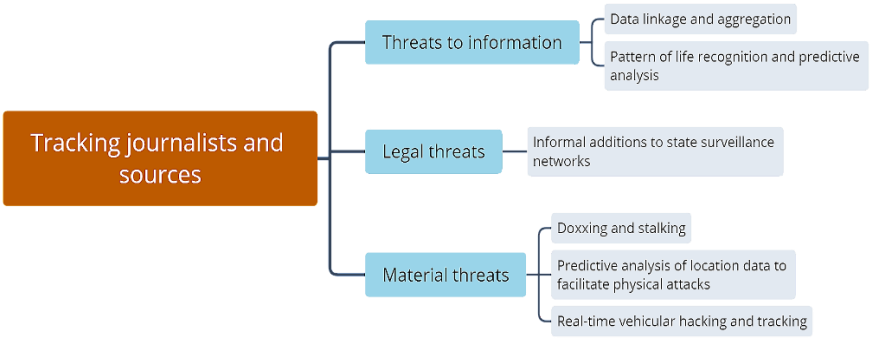


Figure 19: Tracking journalists and sources

2.1 Threats to information

In addition to mapping applications and wearable devices using GPS or other tracking mechanisms, other functionalities such as weather apps also track users' locations and some devices include presence sensors that record bystanders' presence and motions.[1118]

Data linkage and aggregation: The heterogeneity of IoT devices and their capabilities means that data aggregation can reveal far more than was previously possible, which could jeopardise source confidentiality if data and metadata from both ambient and wearable IoT devices is cross-referenced.[1119]

Pattern of life recognition and predictive analysis: Pattern of life information may be inferred by unwanted third parties based on data gathered by automated household management and utility devices. The timing of interaction with these devices would allow detailed daily routines to be surmised and exploited.[1120] Predictive analysis can also be used to infer more sensitive data by devices or attackers with analytical capabilities, such as one's health status being recognised based on requests made to voice assistants,[1121] or wearable devices.[1122] The IoT-sourced data allows extrapolation to substantiate both true and false scenarios.

[1118] J. Sturgess, J.R.C. Nurse, and J. Zhao. 2018. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In *2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018*, Institution of Engineering and Technology, London, UK, 37 (8 pp.)-37 (8 pp.). DOI:https://doi.org/10.1049/cp.2018.0037.

[1119] J. Sturgess, J.R.C. Nurse, and J. Zhao. 2018. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In *2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018*, Institution of Engineering and Technology, London, UK, 37 (8 pp.)-37 (8 pp.). DOI:https://doi.org/10.1049/cp.2018.0037.

[1120] Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658.

[1121] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than smart speakers: security and privacy perceptions of smart home personal assistants. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (SOUPS'19), USENIX Association, USA, 451–466.

[1122] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. "There is nothing that I need to keep secret": sharing practices and concerns of wearable fitness data. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (SOUPS'19), USENIX Association, USA, 421–434; Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658; Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

2.2 Legal threats

Informal additions to state surveillance networks: Consumer IoT networks can become informal features of smart cities and therefore easily accessible by law enforcement and intelligence agencies. This centralisation of data would therefore easily facilitate the tracking of journalists by governments without transparent oversight.

2.3 Material threats

Doxxing and stalking: Access to the huge amounts of personal information gathered by IoT devices, either historic data (such as location information from a fitness tracker[1123] or live data such as hacking the camera of a smart television, which may record both video and audio)[1124] can facilitate the doxxing and stalking of journalists. These could result in financial and reputational damages that harm journalist's credibility.[1125]

Predictive analysis of location data to facilitate physical attacks: Tracking of a journalist by accessing the location data gathered by and streamed from their car, fitness tracker or smart watch[1126] could allow an adversary to infer previous routes[1127] and locations or to predict future ones, information that could be capitalised on to facilitate a physical attack[1128] or to implicate the journalist in a crime.

Real-time vehicular hacking and tracking: Vehicular hacking would allow adversaries to access real-time geographic data,[1129] which could be used to track journalists and sources.

3. Altering information

The continued existence of a free press depends on journalists' dissemination of accurate information. If this is threatened, it could discredit the work of entire news organisations and lower public trust in the news media.

[1123] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. "There is nothing that i need to keep secret": sharing practices and concerns of wearable fitness data. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (SOUPS'19), USENIX Association, USA, 421–434.

[1124] J. Sturgess, J.R.C. Nurse, and J. Zhao. 2018. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In *2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018*, Institution of Engineering and Technology, London, UK, 37 (8 pp.)-37 (8 pp.). DOI:https://doi.org/10.1049/cp.2018.0037.

[1125] Simon Anell, Lea Grober, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. In *The 5th European Workshop on Usable Security*, IEEE, Genova, Italy, 10. Retrieved from https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[1126] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. "There is nothing that i need to keep secret": sharing practices and concerns of wearable fitness data. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (SOUPS'19), USENIX Association, USA, 421–434.

[1127] @DFRLab. 2018. Data and Defense: The Case of Strava. *Medium*. Retrieved August 9, 2019 from https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2.

[1128] Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658; National Security Agency. 2020. *Limiting Location Data Exposure*. National Security Agency, USA. Retrieved September 11, 2020 from https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF.

[1129] National Security Agency. 2020. *Limiting Location Data Exposure*. National Security Agency, USA. Retrieved September 11, 2020 from https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF.

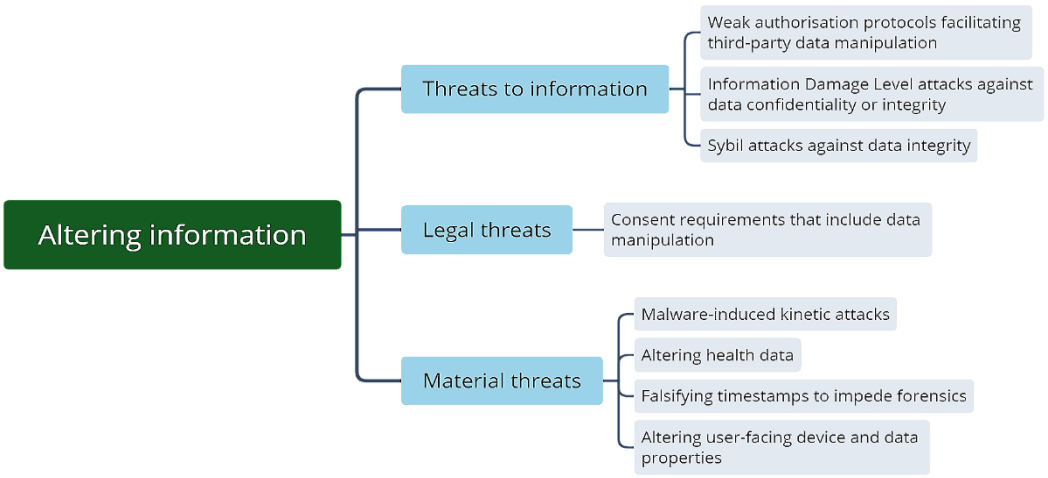


Figure 20: Altering information

3.1 Threats to information

Weak authorisation protocols facilitating third party data manipulation: Apps and the IoT devices on which they are hosted often have weak authorisation protocols that allow overreach, including downloading malware, that could facilitate data theft and manipulation via third party software or device layers, either in storage or in transit.[1130] The resultant ambiguity as to whether a journalist is responsible for specific information, either through sharing or creation, could have ramifications for their credibility and public trust.

Active access level attacks: E.g. attacks specific to voice assistants, such as "voice squatting in which an attack skill carries a phonetically similar invocation name to that of its target skill" and "word squatting where the attack invocation name includes the target's name and some strategically selected additional words".[1131] These are active access level attacks which, for example, manipulate the data received by either end of a communications channel, and would be particularly problematic for journalist-source communication, or even for different members of a newsroom team discussing a sensitive story.[1132]

Information Damage Level attacks against data confidentiality or integrity: Information can also be changed via Information Damage Level attacks which relate to the sensors in IoT devices. They can take different forms, usually involving monitoring, intercepting, modifying, fabricating, or replicating data collected by these sensors and sent through a network. These attacks particularly affect data confidentiality and integrity, as messages can be altered or recorded and replayed to the wrong people

[1130] Simon Anell, Lea Grober, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. In *The 5th European Workshop on Usable Security*, IEEE, Genova, Italy, 10. Retrieved from https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[1131] Nan Zhang, Xianghang Mi, Xuan Feng, XiaoFeng Wang, Yuan Tian, and Feng Qian. 2019. Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. In *2019 IEEE Symposium on Security and Privacy (SP)*, IEEE, Stockholm, Sweden, 1381–1396. DOI:https://doi.org/10.1109/SP.2019.00016.

[1132] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660; Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

or at the wrong times.[1133] These attacks could prevent journalists from feeling confident that they can effectively protect source information and that their work is founded in verifiable data.

Sybil attacks against data integrity: An adversary may infiltrate a network through one compromised node, that then masquerades as multiple nodes, allowing it to access and influence information transfer throughout an IoT network, as well as resource distribution.[1134] If this attack is used to spread disinformation, this could affect both journalists' reputations and their beliefs about their own information security.

3.2 Legal threats

Consent requirements that include data manipulation: Some apps and IoT devices require users to consent to all manner of data acquisition, transfer, and processing, as well as allowing access to other device functionalities (such as cameras, microphones, and messaging systems) in order to function. Similarly, with the evolution of deep fake technologies, the wealth of data created by IoT devices could be used to effectively and potentially legally use an individual's likeness. Both of these considerations would allow the problematic potential for access and manipulation of journalists' data, possibly in ways that could dupe or reveal sources.[1135]

3.3 Material threats

Malware-induced kinetic attacks: Malware may change device settings and to alter the behaviour or functionality of a device without the device owner's recognition. This can facilitate clandestine surveillance and kinetic attacks in technologies from small consumer IoT devices to core national infrastructure, as happened with the Stuxnet hack. In this way, it is possible to conduct large-scale kinetic attacks against an urban area where lots of news organisations are concentrated, by attacking IoT devices that control public goods.[1136]

Altering health data: Insecurity of wearable fitness or medical devices, including those that collect health information can contribute to inaccurate diagnoses and prescriptions, or even altered test results. These flaws could be fatal and could be used to put psychological, financial, or physical pressure on journalists.[1137]

Falsifying timestamps to impede forensics: Digital forensics, which is already notoriously unreliable regarding consumer IoT devices, may be made more challenging as, for example, monitoring when specific actions have been taken could be hindered if time stamps can be easily falsified by changing the

[1133] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1134] Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

[1135] Mary C. Kay Michel and Michael C. King. 2019. Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In *2019 IEEE International Symposium on Technology and Society (ISTAS)*, IEEE, Medford, MA, USA, 1–7. DOI:https://doi.org/10.1109/ISTAS48451.2019.8938009.

[1136] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1137] Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658; Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

time on the device's clock.[1138] This could make journalists' task of verification of sources much more difficult, which may then allow their conclusions to be debunked and their reputations to suffer.

Altering user-facing device and data properties: Attacks used to alter user-facing information displayed by the IoT device are also possible, including clock skewing or deletion or editing of messages and alerts.[1139] These kinds of attacks could be particularly problematic for journalists if used to put psychological pressure on them. Journalists often receive threatening messages,[1140] which could also be delivered through their devices, such as a voice assistant. If these two events coincide, there is likely to be a chilling effect as they question the security of their professional systems and their own perceptions due to gaslighting.[1141]

4. Assuming control over intended device functionality to discredit or physically harm journalists

Sometimes consumer IoT devices have sufficiently intrusive intended functionalities that an adversary can use existing capabilities in ways that the user may not have intended.

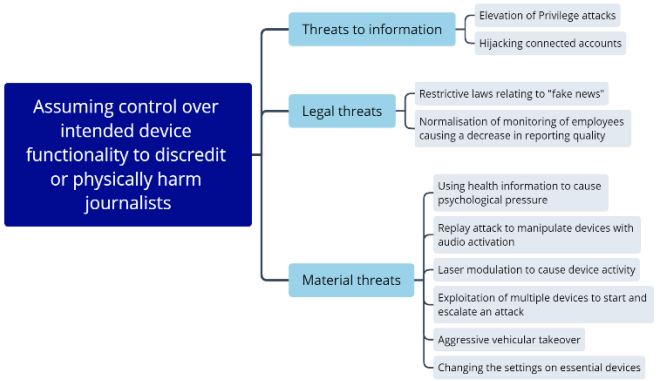


Figure 21: Assuming control over intended device functionality to discredit or physically harm journalists

4.1 Threats to information

The fourth threat category involves adversaries co-opting the intended functionality of devices within an environment to pose threats to journalists and their work. Cyber-physical attacks on journalists can cause a chilling effect, as they effectively self-censor to avoid greater harm. Attacks that affect journalists' credibility have knock-on effects for both their livelihood and their physical wellbeing.

Elevation of Privilege attacks: Even if the identified device is not connected to a social media account, a journalist might use their smart watch as a proxy for their smartphone to remotely control their other IoT devices, so compromising the smart watch could potentially affect the configurations of all other

[1138] Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

[1139] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1140] Amy Binns. 2017. Fair game? Journalists' experiences of online abuse. *Journal of Applied Journalism & Media Studies* 6, 2 (June 2017), 183–206. DOI:https://doi.org/10.1386/ajms.6.2.183_1.

[1141] Lucy Middleton. 2020. Woman "hacked into ex-boyfriend's Alexa and told his new girlfriend to leave." *Metro*. Retrieved October 19, 2020 from https://metro.co.uk/2020/10/12/woman-hacked-into-ex-boyfriends-alexa-and-told-his-new-girlfriend-to-leave-13407458/; Glyn Moody. 2020. The enemy within: welcome to the Internet of gaslighting. *Privacy News Online by Private Internet Access VPN*. Retrieved September 11, 2020 from https://www.privateinternetaccess.com/blog/the-enemy-within-welcome-to-the-internet-of-gaslighting/.

devices, as well.[1142] Similarly, smart hubs that coordinate devices can be attacked in a variety of ways, and can be used for Elevation of Privilege attacks, therefore giving adversaries high-level access to and control of connected IoT devices.[1143]

Hijacking connected accounts: Some smart White Goods have the ability to post from users' social media accounts or send emails,[1144] and hacking into a journalist's fridge and accessing their social media accounts in order to imitate them could be used for a variety of nefarious purposes. Already, there have been instances of journalists being imitated and having article bylines intentionally misattributed to them,[1145] as well as of hackers posting false articles on legitimate news sites.[1146] If an adversary is able to publish disinformation under a journalist's name from their own account that would likely undermine the journalist's credibility. If this process repeats, the journalist's audience could shift or disappear to such an extent that the journalist no longer has a following of note or a sufficiently good reputation to have standing within the industry.

4.2 Legal threats

Restrictive laws relating to 'fake news': The advent of global digital media platforms has created an environment with huge public influence and little regulation. Even democratic governments are using the disinformation crisis to pass more subversively restrictive laws on journalism with the pretext of inhibiting the spread of disinformation.[1147] If a consumer IoT device that has access to a journalist's social media accounts is hacked and used to spread disinformation,[1148] this could be used as evidence to invoke laws that would then result in the prosecution of the journalist. It is possible for a state-affiliated adversary to use this kind of attack to implicate a journalist and use this as the rationale to hinder their ability to operate. While these kinds of attacks are feasible and have been evidenced, their use with the IoT to legally impede journalistic work may be unlikely. This is because of widespread state abuse of traditional laws with an established history of use to silence journalists, including criminal defamation laws, blasphemy laws, insult laws, and those with expansive definitions of terms such as terrorism and national security, thereby allowing arbitrary imprisonment.[1149]

[1142] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1143] Stacie Hoffmann. 2018. *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. IoT Security Foundation, Oxford, United Kingdom. Retrieved August 12, 2020 from https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf.

[1144] Agence France-Presse (AFP). 2014. Hackers use 'smart' refrigerator to send 750,000 virus-laced emails. *Raw Story*. Retrieved October 23, 2020 from https://www.rawstory.com/2014/01/hackers-use-smart-refrigerator-to-send-750000-virus-laced-emails/.

[1145] Eric Hamilton. 2020. Eric Hamilton on Twitter: "Here's a thing that happened today. I was recently -- and falsely -- linked to an article I didn't write, because the author who DID write it happens to share the same name/byline as I do. I'm not going to link to it because it's complete garbage." *Twitter*. Retrieved September 13, 2020 from https://twitter.com/OnetheycallEric/status/1270857748092239872; Leigh Honeywell. 2020. Leigh Honeywell @ 🏠 on Twitter: "Btw this Eric Hamilton is _not_ the author of the shitty stalker article, just has the misfortune of the same name and profession." *Twitter*. Retrieved September 13, 2020 from https://twitter.com/hypatiadotca/status/1270978645327110145.

[1146] Andy Greenberg. 2020. Hackers Broke Into Real News Sites to Plant Fake Stories. *Wired*. Retrieved October 19, 2020 from https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/.

[1147] Reporters Without Borders. 2020. 2020 World Press Freedom Index: "Entering a decisive decade for journalism, exacerbated by coronavirus" | RSF. *2020 World Press Freedom Index*. Retrieved September 11, 2020 from https://rsf.org/en/2020-world-press-freedom-index-entering-decisive-decade-journalism-exacerbated-coronavirus.

[1148] Shannon Schwedel and Heather Palus. 2019. A Ranking of the Weirdest Appliances That You Can Technically Tweet From. *Slate Magazine*. Retrieved September 11, 2020 from https://slate.com/technology/2019/08/twitter-electronics-ranked-list-which-is-best.html.

[1149] Gill Phillips. 2020. How the free press worldwide is under threat. *The Guardian*. Retrieved September 11, 2020 from https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat.

Normalisation of monitoring of employees causing a decrease in reporting quality: Additionally, given the normalisation of IoT technology used to monitor the real-time productivity of employees,[1150] it is feasible that this would be implemented in newsrooms, exacerbating the imperative for journalists to be constantly writing, with fewer periods of reflection or discussion. This would have effects for journalists' reputations as established journalists are forced to sensationalise stories to keep earning money.[1151]

4.3 Material threats

Using health information to cause psychological pressure: Journalists' portable or wearable devices to track personal health information, may not have the inbuilt security to prevent leaks. Malicious actors may use this information to cause psychological or physical distress and thereby influence a journalist's output, e.g. through blackmail.[1152] A feasible but unlikely example is a diabetic journalist having a wearable blood sugar tracker that can be hacked, enabling adversaries to identify vulnerable moments.[1153]

Replay attack to manipulate devices with audio activation: The ability to identify IoT devices present in an individual's home through open-source investigations is the first step to many different attacks. E.g., for a journalist who has done public interviews, manipulation of the audio from those interviews to record a command that can then be played when an adversary calls the journalist's home phone, to activate a voice assistant.

Laser modulation to cause device activity: Some IoT devices, e.g. voice assistants, can be hacked through windows by modulating a laser pointer, using it to issue commands to the IoT device.[1154] The devices could then cause physical harm to device owners and those in the vicinity, or cause financial loss because voice assistants are often granted access to online shopping accounts and thus also banking accounts. This is feasible but unlikely, given the possibility of remote access to such devices with the same outcomes.

Exploitation of multiple devices to start and escalate an attack: Similarly, the combination of multiple devices into IoT ecosystems presents unique challenges that can culminate in much greater harm than that posed by any single device.[1155] This was demonstrated by the National Cyber Security Centre, who used a vulnerability in an IoT doll to unlock a smart door lock.[1156] In practice, such cyber-kinetic attacks

---

[1150] Bruce D. Weinberg, George R. Milne, Yana G. Andonova, and Fatima M. Hajjat. 2015. Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons* 58, 6 (November 2015), 615–624. DOI:https://doi.org/10.1016/j.bushor.2015.06.005.

[1151] Reporters Without Borders (RSF). 2017. #SPOILERSFORFREEDOM: Exiled journalists warn democracies about decline in media freedom. *RSF*. Retrieved January 1, 2021 from https://rsf.org/en/news/spoilersforfreedom-exiled-journalists-warn-democracies-about-decline-media-freedom; UNESCO. 2018. Trends in media pluralism - UNESCO Digital Library. In *World trends in freedom of expression and media development: global report 2017/2018*. UNESCO, Paris, 66–100. Retrieved January 1, 2021 from https://unesdoc.unesco.org/ark:/48223/pf0000261370.

[1152] Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658; Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1153] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J Cyber Secur* 4, 1 (January 2018). DOI:https://doi.org/10.1093/cybsec/tyy006; Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. 2019. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6, 2 (April 2019), 2159–2187. DOI:https://doi.org/10.1109/JIOT.2018.2878658.

[1154] E&T editorial staff. 2017. IoT devices could communicate using ambient radio waves. *Engineering & Technology*. Retrieved September 9, 2019 from https://eandt.theiet.org/content/articles/2017/05/iot-devices-could-communicate-using-ambient-radio-waves/.

[1155] Ben Nassi, Ron Bitton, Ryusuke Masuoka, Asaf Shabtai, and Yuval Elovici. 2021. SoK: Security and Privacy in the Age of Commercial Drones. IEEE Computer Society, 73–90. DOI:https://doi.org/10.1109/SP40001.2021.00005.

[1156] Ian Levy. 2017. Hacked doll "could open front door." *BBC News*. Retrieved September 13, 2020 from https://www.bbc.co.uk/news/av/technology-38966285.

could be used to harm journalists whose public-facing social media might reveal that they own IoT devices.

Aggressive vehicular takeover: Remote hacks of internet-connected vehicles could result in adversaries gaining control of vital functions such as steering and braking,[1157] which could be used to physically harm journalists and sources.[1158]

Changing the settings of essential devices: An attacker could manipulate the settings of devices upon which a journalist relies, to cause tangible disruption and thereby delay their work. E.g., the temperature control function of a journalist's smart fridge so that it overcorrects, thereby spoiling the contents and poisoning the journalist.[1159] While feasible, this threat may be unlikely, due to the indefinite timeframe of its consequences.

5. Limiting device functionality

Given the range of functionalities that consumer IoT devices can possess, users may come to rely on them, triggering detrimental physical and psychological effects if device functionality is unexpectedly limited.

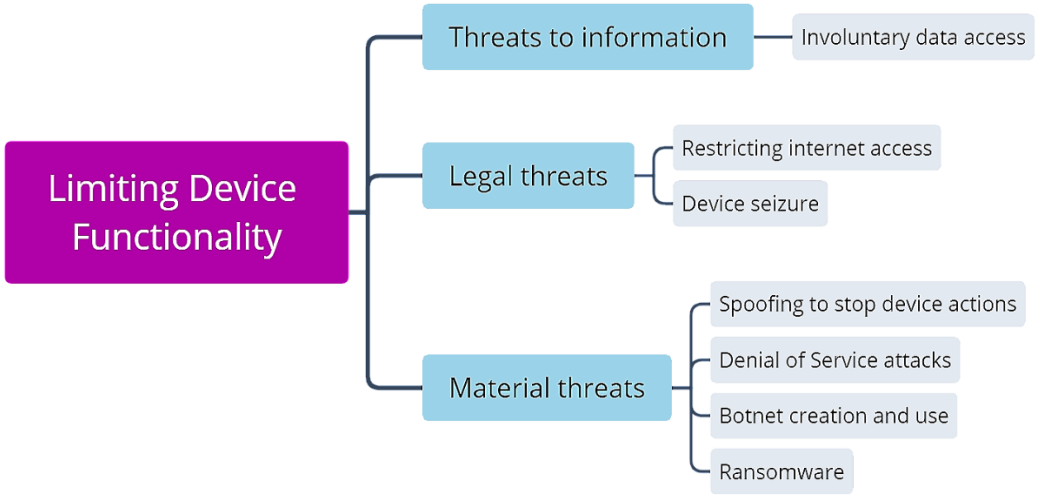


Figure 22: Limiting device functionality

5.1 Threats to information

The innately poor security of consumer IoT devices makes data leakage and hacking to disrupt device functionality realistic for all users, but particularly for individuals with divisive public profiles, such as journalists.

[1157] National Security Agency. 2020. *Limiting Location Data Exposure*. National Security Agency, USA. Retrieved September 11, 2020 from https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF.

[1158] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J Cyber Secur* 4, 1 (January 2018). DOI:https://doi.org/10.1093/cybsec/tyy006; Staff of Senator Ed Markey. 2015. *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*. Office of the United States Senator for Massachusetts, Massachusetts, USA. Retrieved October 26, 2020 from https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[1159] Swapnil Bhartiya. 2017. Your smart fridge may kill you: The dark side of IoT. *InfoWorld*. Retrieved November 18, 2020 from https://www.infoworld.com/article/3176673/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html.

Involuntary data access: Involuntary data access, sometimes classed as data loss, can result in consequences such as entirely halting the ability of a device to function, or inhibiting functions to a lesser degree that nonetheless can facilitate legal and material threats to journalists.[1160]

5.2 Legal threats

Restricting internet access: State-wide activities that have a disproportionate impact on journalists (and on others who are reliant on IoT-based infrastructure) include denial of internet access such as through electronic curfews.[1161] Restricting access to the internet impedes some of the functionality of consumer IoT devices,[1162] which could have a particularly negative impact on journalists who are using such devices to report, such as camera-equipped drones. Internet-access denial tactics are also used to reinforce aggressive treatment of journalists covering protests by preventing them from using portable IoT devices to report on the ground.

Device seizure: Police raids of newsrooms and journalists' offices and homes involve a variety of coordinated efforts to undermine the press, including seizing or compromising assets such as IoT devices by physically or digitally accessing and distorting their features such that they are no longer fit for purpose.[1163]

5.3 Material threats

All of the threats in this category could have physical and psychological effects on journalists and news organisations, because of their likely high reliance on and use of devices in their work, as well as the importance of source and information secrecy.

Information Damage Level attacks to shut down a device: Information Damage Level attacks can affect the physical functionalities of an IoT device if so much data is sent that an adversary exhausts a system's resources and therefore stymies its availability, possibly shutting down an IoT device.[1164]

Software compromise to drain device power: Software compromise may involve exhausting the resources of a specific IoT device or network by overloading communications or overusing a specific functionality. This could then cause the device to shut down due to low power, which would be particularly problematic if it is a device that centrally coordinates other IoT devices thus impacting the wider network.[1165]

Spoofing to stop device actions: Spoofing data packets would cause devices to stop, start, or modify actions.[1166]

[1160] Simon Anell, Lea Grober, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. In *The 5th European Workshop on Usable Security*, IEEE, Genova, Italy, 10. Retrieved from https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf; Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

[1161] Elisabeth Mahase. 2019. Kashmir communications blackout is putting patients at risk, doctors warn. *BMJ* 366, (August 2019), l5204. DOI:https://doi.org/10.1136/bmj.l5204.

[1162] Klint Finley. 2014. Why Tech's Best Minds Are Very Worried About the Internet of Things. *Wired*. Retrieved October 26, 2020 from https://www.wired.com/2014/05/iot-report/.

[1163] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J Cyber Secur* 4, 1 (January 2018). DOI:https://doi.org/10.1093/cybsec/tyy006.

[1164] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1165] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1166] Stacie Hoffmann. 2018. *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. IoT Security Foundation, Oxford, United Kingdom. Retrieved August 12, 2020 from https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf.

Denial of Service attacks: Denial of Service attacks can be both caused by and effected against IoT devices. The former can be carried out against third party devices and systems, e.g. if a device is co-opted into a botnet and used to execute exploits against other systems.[1167] The latter can occur if the device's availability is maliciously overloaded through unnecessary data traffic,[1168] which can be particularly damaging if the device has an essential function, such as monitoring blood sugar or pulse.[1169] DoS could be achieved by exploiting vulnerabilities in the hub to disrupt the entire smart home ecosystem.[1170] In practice, being targeted by DoS attacks reduces a network's capacity and can disable it. If a journalist is reliant on the availability of a specific network or device that can be accessed through an insecure IoT device, DoS attacks could leave them vulnerable to extortion.[1171]

Botnet creation and use: IoT devices, while potentially low-powered on their own, generally have such lax security that they can be easily co-opted into botnets, i.e. networks of (even unrelated and disparate) IoT devices that have been infected with malware. Host takeover resulting in botnets can execute data breaches, Distributed Denial of Service (DDoS) attacks on well-secured networks or internet infrastructure, and further malware delivery that can drastically affect services on which society relies, including news provision.[1172] Any of these activities can be devastating for individual journalists and for news organisations, both of which might be at risk of losing access to vital devices or systems for indeterminate periods of time, as well as the potential that data held on those systems has been compromised.[1173] Further, these botnets could be used to launch large-scale online attacks on members of the press using troll armies.[1174]

[1167] Syed Rizvi, Andrew Kurtz, Joseph Pfeffer, and Mohammad Rizvi. 2018. Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 163–168. DOI:https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034.

[1168] Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

[1169] Simon Anell, Lea Grober, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. In *The 5th European Workshop on Usable Security*, IEEE, Genova, Italy, 10. Retrieved from https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

[1170] Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834; Stacie Hoffmann. 2018. *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. IoT Security Foundation, Oxford, United Kingdom. Retrieved August 12, 2020 from https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf; Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 321–326. DOI:https://doi.org/10.1109/ICED.2016.7804660.

[1171] Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834; Stacie Hoffmann. 2018. *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. IoT Security Foundation, Oxford, United Kingdom. Retrieved August 12, 2020 from https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf.

[1172] Catalin Cimpanu. 2016. A Massive Botnet of CCTV Cameras Involved in Ferocious DDoS Attacks. *softpedia*. Retrieved October 23, 2020 from https://news.softpedia.com/news/a-massive-botnet-of-cctv-cameras-involved-in-ferocious-ddos-attacks-505722.shtml; Brian Krebs. 2016. KrebsOnSecurity Hit With Record DDoS — Krebs on Security. Retrieved October 23, 2020 from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/; Sean Smith. 2017. *The Internet of Risky Things: Trusting the Devices That Surround Us* (1st ed.). O'Reilly Media, Inc., Sebastopol, CA, USA.

[1173] Susan McGregor. 2016. Why DDoS attacks matter for journalists. *Columbia Journalism Review*. Retrieved November 15, 2020 from https://www.cjr.org/tow_center/journalists_ddos_hack_passwords.php.

[1174] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J Cyber Secur* 4, 1 (January 2018). DOI:https://doi.org/10.1093/cybsec/tyy006; Maria Gulzar and Ghulam Abbas. 2019. Internet of Things Security: A Survey and

Ransomware: Criminal actors could exploit news organisations' notable lack of effective security protocols and the potential for IoT devices that are connected to a central Wi-Fi network. They may distribute ransomware that locks journalists and other media staff out of their work, thereby hindering the progress of a story and creating more financial and legal stressors for executives.[1175]

Taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, IEEE, Lahore, Pakistan, 1–6. DOI:https://doi.org/10.1109/CEET1.2019.8711834.

[1175] Simon Anell, Lea Grober, and Katharina Krombholz. 2020. End User and Expert Perceptions of Threats and Potential Countermeasures. In *The 5th European Workshop on Usable Security*, IEEE, Genova, Italy, 10. Retrieved from https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

Appendices from Chapters 6 and 7: Country Profiles

Appendix E: Participant Information Sheet and Oral Consent Form

Participant Information Sheet

Ethics Approval Reference: CS_C1A_20_003

1. What is the purpose of this research?

There have recently been a number of high-profile cyber-attacks on news organisations and individual journalists, from the use of Pegasus spyware to online intimidation efforts and Denial of Service attempts at censorship. As a result, many media companies and non-governmental organisations have shared information on how journalists can increase their cyber security. At the same time, internet-enabled devices have become ubiquitous in people's daily lives, with little public regard for the threat to privacy that they pose if compromised. A dearth of understanding about the risks associated with Internet of Things (IoT) devices pervades all branches of society, which is exemplified by the November 2017 'Strava' incident when US military forces did not recognise that their fitness tracking apps were publicly transmitting secret patrolling patterns.[1176]

As such, it is imperative that news organisations – particularly those that operate across continents – prepare their staff and sources using anticipatory legal threat models that take into account the vast amounts of data collected, transferred, stored, and analysed as a result of the IoT, as well as the inherent cyber-physical threats that will only continue to evolve with the expansion of the market. One aspect of news agencies' security strategies must be keeping abreast of and mitigating threats from emerging technologies, but the findings of the exploratory study (see: Ethics Approval Reference: CS_C1A_19_017-1) that journalists may be largely unaware of the threats stemming from the rising prevalence of the IoT suggest that the threat models presently employed by the news industry are likely to be outdated.

The ultimate purpose of this research is to create a framework for transcontinental media organisations that are headquartered in democratic countries to consider applying when designing their internal policies and strategies to protect their staff and sources against relevant legal threats and Internet of Things-specific threat models. In order to do this, the researcher intends to collect information on the current national context of four case studies, all transcontinental news organisations.

2. Why have I been invited to take part?

You have been invited to participate because of your expertise in an aspect of this research, whether that be the IoT, transcontinental news organisations, or one or more of the case study countries: The United Kingdom, the United States, Taiwan, and Australia.

Depending on your specialism, the researcher is primarily interested in discussing your knowledge of the following areas:

- Media sector/journalism:
    - E.g. Threat intelligence sharing between news organisations and/or journalists;
    - Geopolitical pressures and national security tensions regarding the media;
    - Any other threats to the maintenance of a free press in these countries;
- State capabilities:
    - E.g. Relevant data protection/retention or cyber security legislation;

[1176] https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

    - Laws regarding ambient/targeted surveillance;
    - The technical capabilities of law enforcement, security and intelligence agencies;
- The IoT:
    - E.g. The domestic market for emerging technologies (particularly the IoT);
    - IoT security and privacy;
    - IoT regulation – both proposed and enacted (and sceptics about governments having a hand in this)

However, these interviews are semi-structured rather than prescriptive and the researcher is eager to hear your thoughts on other facets of the problems explored by my research, guided by the discussion.

As the aim of this set of interviews is to gain an insight into the threat landscape of each of my case study countries, I have chosen not to dictate 'inclusion' or 'exclusion' criteria for recruitment of participants, other than a minimum age of 18 years old, for the purpose of informed consent. This is mainly due to the variety of topics to be covered and the fact that, for example, the length of someone's time in a specific professional role is not necessarily an indicator of their specialist knowledge of peripheral subjects. Instead, you have either been chosen as part of a 'purposive sample' of experts, found through research into your specialism, *or* through 'snowball sampling' – i.e. one such expert has suggested that I contact you to deepen my knowledge of your area.

3. Do I have to take part?

No. You can ask questions about the research before deciding whether or not to participate. You will be able to withdraw your information up until 07/04/2023 (i.e. the expected date of completion of the researcher's doctorate) or within three months of the interview taking place, whichever date comes first. If you choose to do so, you are not obligated to give a reason, but may withdraw yourself from the study by advising the researcher of this decision so that all your research data can be erased.

4. What will happen to me if I take part in the research?

If you are happy to take part in the research, you will be asked to take part in a single interview session, lasting roughly one hour. The researcher may contact you to ask if you are willing and able to answer follow-up questions at a later stage, unless you wish not to be contacted after the interview.

The interview may take place in-person or via a voice- or video-calling platform of your choice. Prior to the interview commencing, the researcher will talk you through the study procedures and give you the chance to ask any questions, although you may feel free to ask questions at any point during the process.

If you are still happy to participate in the research, you will be asked to give oral consent, which will be noted down by the researcher. This will include being asked to confirm that you are happy for the interview to be audio recorded. If you decide that the interview should not be audio recorded, the researcher will take notes manually instead.

You are free to request audio recording or note-taking to be suspended at any time during the interview and can request that any of your data be deleted, during or after the interview.

5. Are there any potential risks in taking part?

Unless participants explicitly request anonymity, the researcher does not plan to anonymise participant data. Participants are welcome to request that their responses and data be anonymised, but the researcher anticipates that attributing quotes or knowledge to individual participants will lend the final analytical product of this research more authority through transparency.

While participants will have the chance to review their transcripts if they so choose, and to request that other information be removed, there is still a risk that any answers given by participants could be used to identify individual participants, even if they request that their data be anonymised. In order to reduce any potential risks, if any identifying information is revealed during the course of an interview with a participant who has requested anonymity, this detail will be purposefully obfuscated (e.g. through the use of pseudonyms) or removed in the transcript, following which the interview recording will be deleted.

Additionally, the interviews will touch upon subjects that may be distressing to participants, such as threats to journalists. Participants are encouraged to inform the researcher if they would like to pause or end the interview, or change topic.

6. Are there any benefits in taking part?

There will be no direct benefit to you from taking part in this research. However, once the research is completed, participants may receive copies of the researcher's final thesis and/or any other related research publications to which their interviews contributed, if they so wish.

Additionally, the researcher hopes that the analysis to be undertaken and framework to be created will benefit news organisations and the free press more widely by giving them guidance on how to improve their cyber security protections, particularly regarding IoT threats to journalists and sources as these technologies become more widespread and powerful.

7. What happens to the data provided?[1177]

The information you provide as part of the study is the **research data**. Any research data from which you can be identified (e.g. your name or audio recording), is known as **personal data**. This includes more sensitive categories of personal data (sensitive data) such as your politics, racial or ethnic origin. It does not include data where the identity has been removed (anonymous data).

The researcher will minimise use of personal and sensitive data in the study as much as possible and any audio recordings of your interview will be transcribed and destroyed within three months of the interview. Transcribed interviews will include your name and other identifying details, unless you have requested otherwise. They can also be sent to you, if you would prefer, to confirm that you are happy with any details from the transcribed interview being included in the final thesis and any other research papers.

If so requested, in order to anonymise transcripts, the researcher will do this by removing any name/email address stored with the transcript and redacting any information that might be used to identify individual participants.

The researcher would like your permission to use direct quotes, but this is not obligatory. If you have requested anonymity but would be happy to be quoted, any quotes used will not include personal information and will not identify the individual.

[1177] Please refer to CUREC's Best Practice Guidance on Data Collection and Management (BPG 09).

The **research data** will be stored confidentially, with all audio recordings and notes taken during the interviews transcribed and deleted within three months of their creation. Until then, recordings will be stored and reviewed locally on the device used to record them.

Transcribed interviews (including records of oral consent) and their associated notes will be encrypted, stored on a password-protected personal laptop and backed-up through Virtual Private Network (VPN) to the University of Oxford's servers (HFS back-up).

Your personal data may be transferred to, and stored at, a destination outside the European Economic Area. We will make sure that identifiable data is removed whenever possible and that any data transfer is done securely and with a similar level of data protection as required under UK Law.

The researcher and supervisors will have access to research data. Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.

All voice recordings will be erased within three months of their creation. Digital transcripts and associated materials will be stored for a minimum of 3 years after completion of doctoral research or public release of the work of the research. We may retain and store your personal data for an additional period of time as necessary for the purposes of the study, and for further research. You will be able to withdraw your information up until 07/04/2023 (i.e. the expected date of completion of the researcher's doctorate) or within three months of the interview taking place, whichever date comes first. Any paper-based notes will be transcribed, with the originals shredded after scanning.

8. Will the research be published?

The research may be published in articles in print and online, likely in an academic venue.
The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.

The research will form part of the researcher's thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives, to facilitate its use in future research. The thesis will be openly accessible.

9. Who is organising and funding the research?

This research is funded by a scholarship (EP/P00881X/1) granted by the **British Engineering and Physical Sciences Research Council (EPSRC)**, through the **Centre for Doctoral Training in Cyber Security, University of Oxford**.

10. Who has reviewed this study?

This study has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Reference number: CS_C1A_20_003).

11. Who do I contact if I have a concern about the study or I wish to complain?

If you have a concern about any aspect of this study, please speak to the relevant researcher, Anjuli R. K. Shere (anjuli.shere@cybersecurity.ox.ac.uk) or their supervisors, Dr. Andrew Martin (+44 (0)1865 2-83605) and Dr. Jason Nurse (+44 (0)1227 82 7615), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter in a reasonably expeditious manner:
Chair, Computer Science Department Research Ethics Committee; ethics@cs.ox.ac.uk; Wolfson Building, Parks Road OX1 3QD

12. Data Protection

The University of Oxford is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study.

The University will process your personal data for the purpose of the research outlined above. Research is a task that we perform in the public interest.

Further information about your rights with respect to your personal data is available from http://www.admin.ox.ac.uk/councilsec/compliance/gdpr/individualrights/.

13. Further Information and Contact Details

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:
Anjuli R. K. Shere
Doctoral Researcher
Centre for Doctoral Training in Cyber Security, Department of Computer Science, University of Oxford
Oxford e-mail: anjuli.shere@cybersecurity.ox.ac.uk

Oral Consent Sample Script

(To be carried out at the start of the interview, following an email interaction in which the interviewee received the above information sheet and a copy of this Oral Consent Script, so that they are fully aware of to what they are consenting. The researcher will write a Record of Consent, which will be transcribed along with the interview voice recording).

Hello again, I'm Anjuli Shere from the University of Oxford and I wanted to talk to you about the project I gave you information about before. To recap, the broad aim of my project is to investigate the threat landscape faced by transcontinental news organisations based in four countries – UK, US, Taiwan, and Australia – particularly regarding the Internet of Things (IoT), including those pertaining to the massive data collection facilitated by the IoT. Ultimately, I plan for my research to culminate in the design of a framework for transcontinental news organisations that are headquartered in democratic countries to consider applying when designing their internal policies and strategies to protect their staff and sources against relevant legal threats and Internet of Things-specific threat models. It is my hope that these globally influential organisations will set a trend of implementing cyber security strategies against emergent technological and legal threats that will filter down to all journalists and sources.

In order to do this, I am interviewing you to collect information on the current national context of one or more of my four case studies. As mentioned in the information sheet with which I previously provided you, depending on your specialism, I am primarily interested in discussing your knowledge of the media sector/journalism; relevant data protection/retention or cyber security legislation; ambient surveillance;

the domestic market for emerging technologies (particularly the IoT); IoT security and privacy; threat intelligence sharing between news organisations and/or journalists; the capabilities of law enforcement, security and intelligence agencies; geopolitical pressures and national security tensions regarding the media; and any other threats to the maintenance of a free press in these countries. However, these interviews are semi-structured rather than prescriptive and I am keen to hear your thoughts on other facets of the problems explored by my research, guided by our discussion.

Are you still interested in taking part in the project? *[Await confirmation].* Now I'd like to confirm some of the details of the project to make sure you understand what's involved for you:

- If you agree to take part, I'll need to interview you for roughly one hour, preferably via a voice- or video-calling platform, or in-person. I may also contact you for clarification or brief follow-up questions, if that's alright with you?
- I am aware that this is a complex topic and that you may have many thoughts that you wish to share with me. In order to avoid you becoming fatigued, please let me know if and when you would like any comfort breaks. If you would prefer, I can signpost points for potential comfort breaks when I alert you to any changes of topic, or we can ensure that we pause at regular points. Which would you prefer?
- In terms of risks associated with taking part in this research: Unless participants explicitly request anonymity, the researcher does not plan to anonymise participant data. Participants are welcome to request that their responses and data be anonymised, but the researcher anticipates that attributing quotes or knowledge to individual participants will lend the final analytical product of this research more authority through transparency. While participants will have the chance to review their transcripts if they so choose, and to request that other information be removed, there is still a risk that any answers given by participants could be used to identify individual participants, even if they request that their data be anonymised. In order to reduce any potential risks, if any identifying information is revealed during the course of an interview with a participant who has requested anonymity, this detail will be purposefully obfuscated (e.g. through the use of pseudonyms) or removed in the transcript, following which the interview recording will be deleted. Until the data is analysed, interviewees will also have the chance to review their transcripts if they so choose, and to request that other information be removed.
- You may find aspects of this interview distressing as we may touch upon physical attacks and cyber-attacks on journalists. I will understand if you decide to withdraw from the research if this occurs. However, I believe that it is important to map what is currently being done to protection journalists and their sources against legal and cyber-physical threats through the IoT and how to improve news organisations' cyber security strategies, with the goal that all media organisations and journalists can become better prepared against IoT compromise or attempted data acquisition by the most well-resourced potential adversaries.
- You don't have to agree to take part; you can ask me any questions you want before or throughout; you can also withdraw at any stage without giving a reason.
- The researcher (me) and my two supervising academics will have access to research data. You will be able to withdraw your information up until 07/04/2023 (i.e. the expected date of completion of the researcher's doctorate) or within three months of the interview taking place, whichever date comes first. If you choose to do so, all your research data will be erased and you will not be included in the analysis for any publications, including my thesis.
- You are aware that an Oxford University Research Ethics committee has approved this research project and how to contact me (in the first instance) or the committee in case of any concerns or

complaints. I have given you the project's ethics reference number (CS_C1A_20_003) and relevant contact details. To reiterate: their contact details are ethics@cs.ox.ac.uk

- If you choose to participate, all voice recordings will be erased within three months of their creation. Digital transcripts and associated materials will be encrypted and stored on a password-protected device for a minimum of 3 years after completion of doctoral research or public release of the work of the research. We may retain and store your personal data for an additional period of time as necessary for the purposes of the study, and for further research.
- If explicitly requested, your responses will also be pseudonymised. This means that you will not be named in any subsequent publications but will instead be given a participant number (pseudonym). Would you prefer to contribute to my research as an anonymous interviewee?
- Do I have your permission to quote you directly in research publications?
- I would like to be able to use your data in future studies, and to share this data with other researchers. Are you happy with this?
- I would like to audio record our interview. Are you happy with this?
- You're aware that my written work may be published online and possibly also in print?
- When the study is written up, would you like to receive a copy of the report/lay summary?

Are you still willing to take part? Do you give your permission for me to interview you and audio record our discussion?

[*Await confirmation]* So if you're happy with all of that, and have no more questions, let's start.

Researcher Record of Oral Consent *(to be attached to the interview transcript, both of which may be reviewed by participants if requested)*

- Interviewee Name (or, if they have requested anonymity, Interviewee Number):
- Date:
- Location (City / Region):
- Project Explained (Yes/No):
- Interview recorded or Notes Taken:
- Participant agreed to direct quotes? (Yes / No):
- Participant agreed to quotes which would not identify them? (Yes/No):
- Participant is not to be quoted at all (Yes/No):

Appendix F: List of questions asked for Country Profile interviews

Legal threats to journalists in x country

- You mentioned that the threat model you were dealing with during [international collaborative journalistic investigation] was primarily corporate non-state actors. How does that change your considerations and security mechanisms relative to state actors?
- Is there a history of law enforcement and intelligence agencies in x using their powers to surveil, manipulate or intimidate the press?
- What can you tell me about the domestic intelligence and law enforcement agencies' technical capabilities?
- Could you give me more information on legal threats that affect journalists?
    - Are there any protections against these threats currently?
    - Are there any protections that you think would be important but haven't been coordinated yet?
    - How do you think that these threats would be affected by the IoT?
- How would you foresee or even recommend that existing laws and internet/information controls be updated in light of emerging technologies like the IoT?
- Are there (positive or negative) impacts of national IoT legislation/government policy on journalism/the free press?
    - Do you think that they are accidental or planned?
    - Do you think they are systemic?

Legal: Surveillance and analysis of journalists'/sources' data in x country

- What are the domestic laws on targeted surveillance?
- What are the domestic laws on ambient surveillance? How do you think these will interact with the increasing pervasiveness of IoT devices? What about with devices that are sort of informally contributing to structural surveillance, such as Amazon Ring footage being accessible by police forces. Do you have any thoughts or knowledge of situations like Amazon's Ring, about partnership with police forces around the world and how that effectively allows the data to be stored and accessed at various points by various parties?
- What are the domestic intelligence and law enforcement agencies' legal capabilities regarding access to IoT data and use of it?
- What can you tell me about the current encryption legislation (both in general and regarding the IoT)?
- What do you think is the likelihood that the government is going to pass legislation or pass bills that allow security and intelligence services and law enforcement agencies to tap without warrant or more readily even and without journalistic exemptions, the devices present in a home?
- What do you do to counter legal threats, e.g. legislation intended to quash encryption or to allow surveillance?
- Have you come across anything that deals with law enforcement agencies or intelligence agencies using sneaky ways of accessing things that they might otherwise not have been allowed to do?
- Have you ever engaged with a case where you felt very confident that second sourcing was occurring, whether the state had said or a law enforcement agency had said, "we discovered this information in this way" and you thought they definitely used this other channel that they don't want us to have confirmation they have access to?

Legal: Restrictions on reporting in x country

- I'd like to ask you about the legislation and policy landscape in x, particularly regarding information/internet controls. Which ones have the most impact on the free press?
- What are the dominant laws that are non-content-specific (e.g. "even legislation which is non-content-specific does have an indirect effect on content? So, the rules for example on sectoral mergers and specific competition law regulations which affect the media industry have an effect on content") – How do they affect the media industry?
- How quickly/via what mechanisms can the government increase its involvement in domestic media and international media within the country (e.g. changing broadcasting rules, asking for prior notification of sensitive content, revoking visas, etc.)?
- What kind of legally binding involvement does the government have in controlling/regulating media content (aka broadcasting rules, prior notification of sensitive content, journalistic visas etc.)?

Consumer IoT landscape in x country

- What is the scope of the Internet of Things market in x, which devices do you think are bought or sold or manufactured? And why do you think that is?
- Can you give me any high-profile examples of IoT-related cyber security or privacy incidents that have occurred?
- Has there been talk about moving IoT manufacturing or data centres to x country?
- What are your thoughts on the security implications of the international supply chain that contributes to the IoT market in x country?

Legal threats related/specific to the IoT in x country

- Is there a baseline level of understanding about what IoT devices are or how Computer Network Exploitation cases work and what they affect, among judges?
- Do you believe that the IoT's increasing prevalence is likely to contribute to this history of law enforcement and intelligence agencies in x using their powers to surveil, manipulate or intimidate the press?
- How do you think domestic intelligence and law enforcement agencies' technical capabilities are affected/enhanced by proliferation of the IoT?
- How does x's legislation address informal, voluntary additions to smart city infrastructure, e.g. Amazon Ring cameras that feed into a database that is accessible by police forces?
- What can you tell me about the current data protection legislation regarding the IoT?
- What can you tell me about the current data retention legislation regarding the IoT?
- What can you tell me about the current encryption legislation (both in general and regarding the IoT)?
- What are your thoughts on data aggregation from various streams and how it might be affected (e.g. scaled up) by the increasing prevalence and diversity of the consumer IoT?
- How do you think this will affect the legal capabilities of the government/LEAs/intelligence and security agencies in x? How do you think this will affect the technical capabilities of the government/LEAs/intelligence and security agencies in the UK?

Regulation of the consumer IoT in x country

- What can you tell me about the current policies and legislation that deal with regulation and security of the IoT in x? (For example, what is the government's stance on 'Security by Design' and how is this enacted?)

- What would you say are the biggest challenges to regulation and standardisation of the IoT? How would you anticipate or recommend they be mitigated or threat modelled?
- What are your thoughts on the government being involved in the creation and implementation of IoT regulations? (Regulation is the corporate interpretation of national legislation) What are the alternatives?
- Does the huge amount of data collected by IoT manufacturers give them a disproportionate amount of power, even relative to state governments?
- In terms of there being such a sort of diversity of stakeholders in the field of Internet of Things devices, do you think that a system for developing security or building and security to the devices would have to start with legislation?

Media organisations' cyber strategies in x country

- What are the major domestic media organisations and how are they different?
- What can you tell me about the cyber protection policies of any media organisations, given the increase in technological engagement (both voluntary and ambient) by journalists and news organisations?
    - How are they developed?
    - How are they adapted/updated?
    - What role does government regulation play in the adoption/revision/implementation of these policies?
    - Do journalists feel these policies are sufficient? If not, why not?
- What can you tell me how organisations are advised to/are currently improving their cyber resilience against IoT threats?

IoT threats to journalists in x country

- Do you think it's realistic that IoT devices might be manipulated to enact physical threats against journalists, e.g. lightbulbs and epilepsy?
    - What about psychological threats?
- Given the expanding heterogeneity of the IoT, do you consider ways in which those different devices and their international supply chains might cause problems for journalists?
- Can you think of any ways in which journalists might be able to counter/mitigate IoT threats, without simply avoiding them? Do these work for ambient IoT threats?
- What can you tell me about how emerging technologies like consumer IoT devices (e.g. fitness trackers, Wi-Fi-enabled TVs, CCTV-equipped doorbells, as well as any that are used by journalists for their work, such as drones fitted with cameras) are viewed by news organisations and journalists?
- What can you tell me about the potential use of IoT devices that are linked to social media accounts to spread disinformation that could undermine public trust in the press?
- Can you give me any examples you've seen of IoT devices being used to surveil/intimidate/attack individuals, especially journalists or activists?
- Do you think there's an awareness amongst the journalistic community of the threats that can be enacted through IoT devices?

Overview of journalists' security in x country

- In your experience, how, if at all, do the media organisations/journalists in x share threat intelligence? Is there anything that you could recommend to improve those threat intelligence sharing mechanisms?

- In your experience, how, if at all, do the media organisations/journalists in x threat model/conduct risk assessments for their work?
- Is there anything that news organisations can do to protect journalists in light of this extensive legal surveillance?
- Would it help to make it a legal requirement to alert journalists when their information is investigated?
- Given how long you've worked in this area, would you say you've seen security attitudes shift?
- For operational security, for the institution and also for newsroom and journalistic security, do you have any recommendations for how those strategies are updated in light of news about malware that is being proliferated or adversarial capabilities that are coming to light through threat intelligence?

Pandemic-related changes in press freedom in x country

- Did the 2020 COVID-19 pandemic facilitate a change in the press freedom conditions?
- Can you tell me if/how these powers interact with the IoT?
- For how long do you believe that the emergency powers granted to the state will last? (Do the pandemic measures have sunset clauses or are they indefinite?)
- How, if at all, do you foresee these powers having an impact on press freedom in x country after the pandemic? (e.g. state surveillance, geofencing devices, etc.)
- We've discussed geofencing, which is a technique that I am aware has been considered in several states regarding pandemic measures, track and trace. I was wondering whether you think that that requires a warrant as far as you know, or whether there are any similar technical measures that have been put in place in x?

UK-specific questions

- What can you tell me about issues that this particular UK government has with the press, e.g. the threat to end the BBC Charter?
- Do you have any thoughts on the GDPR's legitimate interest clause and how it might be used as a loophole to create a power imbalance in terms of the information that's collected and who can be collecting the information, which I guess is particularly relevant to the topic of journalism?
- What are your thoughts on the fact that security and intelligence services have the legal authority to view and change any data that they find when hacking devices?
- How can someone challenge bulk data collection, using the GDPR's Right to be Forgotten?
- Why do you think there aren't currently efforts to get journalistic exemptions coming from the political parties? Why do you think there is this sort of bipartisan approach to national security that allows and encourages attacks on the press, whether they take a legal form or otherwise?
    - Could you foresee any efforts to get journalistic exemptions that might gain traction in the next few years, particularly if the public are able to see that the Official Secrets Act is used more?
    - So that seems very similar to a trend in Australia, but the major difference, I imagine legally would be that Australia doesn't have a Bill of Rights. Do you think that's going to have any impact in terms of relief?
- What can you tell me about IoT data portability and the GDPR?

Taiwan-specific questions

- What are your thoughts on regional politics in Asia-Pacific and how these affect the political and legal environment in Taiwan?

- And do you give particular consideration to your cyber security while posted in Taiwan? Is there anything that you do in terms of your cyber protection policies and tactics that you think is indicative of the general behaviours, security behaviours and practises of journalists in Taiwan? Or you wouldn't do if you were anywhere else?
- Can you tell me a bit more about the PTT bulletin board website?
- What can you tell me about how your work regarding the global semiconductor industry relates to the Taiwanese technology industry and security more generally?
- Regarding that kind of restriction, that kind of understanding of the threat level from China in terms of importing Internet connected devices and the data collection capabilities of those devices, do you think that the public is particularly understanding of the decisions that the government makes in those areas?

US-specific questions

- Is it difficult to speak about or work on issues such as legal threats to journalists in the US, when the states are so different?
- Do you know if the NIST Code of Practice for IoT is going to tie into current commercial legislation regarding regulation of the consumer Internet of Things in America?
- What would you change at the federal level to effectively counter/mitigate IoT threats of all kinds?
- What can you tell me about the counter-surveillance work of the Electronic Privacy Information Center (EPIC), both corporate and government-based? How has it engaged with novel consumer IoT devices?

Australia-specific questions

- When the Australian newspapers all blacked out their front pages in solidarity against government interference in the press, did that raise awareness and inspire any movement?
- Do you know anything about restrictions on imports or about e-safety legislation relating to the IoT? I know Turnbull was proposing a sticker scheme.
- I'm curious about the disparity between Australian law enforcement being able to use these devices and their data, while Australia is also putting a lot of energy into research into the IoT and domestic violence?

Comparison questions asked to interviewees with expertise in multiple case studies

- In your experience, what are the main differences between media infrastructure in [countries]? Do you think that the reason for the differences in their rankings in the press freedom list is because they're targeted by different actors or they're having to deal with different internal threats? Do you think it's a lack of funding or is there something else that means that there's this discrepancy that's exhibited?
- Do you think that the information/internet controls in place are dramatically affected by/affect the prevalence of the IoT? Would you say this differs broadly between the [countries]?
- Have you seen the recent footage and reports of police in the US targeting journalists who are trying to cover the George Floyd protests? In your opinion, how does US law enforcement's attitude towards the press differ from that in x?
- I know that one of your research interests is 'journalists' responses to change,' would you say this differs broadly between [countries]?
- What can you tell me about Customs and Border Patrols legal ability to seize IoT devices in the [countries]?

- Are these threat modelling/threat intelligence sharing mechanisms different to those of other media organisations in [countries]? How?
- What would you consider to be the greatest threats to press freedom in [countries]? How do they differ?

Appendices from Chapter 8: Framework

Appendix G: Validator Invitations

Dear **[NAME]**,

I hope you are safe and well.

My name is Anjuli Shere and I am a cyber security DPhil student at the University of Oxford, a predoctoral fellow at the Shorenstein Center at the Harvard Kennedy School, and a research analyst for the Association for International Broadcasting (AIB). My doctoral research project investigates whether and how the rise in prevalence of the Internet of Things (IoT) threatens the maintenance of a free press in democratic countries.

I was referred to you by **NAME/AFFILIATION**, who recommended that I invite you to participate in this project **[OR "I have read in such and such an article..."]**. Given your **involvement/expertise in [INSERT BIT ABOUT THEIR RELEVANT BACKGROUND]**, I am writing to ask whether you would be willing to complete a survey to assess the validity of my framework of recommended countermeasures for IoT threats to journalists.

The objective of my research is to document and anticipate the impact of the Internet of Things (IoT) on journalism in the UK, US, Australia, and Taiwan, to create a useful framework for mitigation of IoT threats to the free press. **I would be interested in your thoughts and perspectives on the utility of this framework with respect to your experience and expertise in [the Internet of Things OR cyber security OR journalism OR state capabilities regarding legal OR technical exploitation of the IoT].**

This framework covers individual and collective technical, social, and legal actions that can be undertaken to mitigate the effects of threats that have the potential to disproportionately affect the press, ranging from interception of IoT communications through to ambiguous metadata retention laws. The framework takes the form of an Excel spreadsheet, and you will be asked if you agree/disagree with content in a range of columns, and how you would improve this: e.g. **[each countermeasure's feasibility and suitability to mitigate assigned IoT threats / matching countermeasures to their beneficiaries in the media and to the relevant phase in the editorial workflow]**. **[As a state capabilities expert, you will also be asked for your thoughts on whether this framework is a useful tool for journalists who might be targeted using legal means available to democratic governments and state agencies.]**

To give you a general overview of my research, I am keen to understand in the ways in which the boom in novel consumer IoT devices **(e.g. fitness trackers, Wi-Fi-enabled TVs, CCTV-equipped doorbells)** particularly affects the free press in democracies such as the UK, US, Australia, and Taiwan. I have thus-far researched this through interviews with experts on each national media industry, the IoT (including cyber-physical threats), and state capabilities relating to the IoT (e.g. national security legislation allowing access to the vast amounts of data collected, transferred, stored, and analysed as a result of the IoT). For reference, my exploratory study can be found here: https://eusec20.cs.uchicago.edu/eusec20-Shere.pdf

This research study has been approved by The University of Oxford's Central Ethics Committee and the official information sheet is **attached** with more information about the benefits and risks of taking part, as well as specifics about how your information will be protected in accordance with UK law including GDPR and the supervisors for the project.

The survey should take about XXX mins and can be found [HERE]. Please feel free to forward this to anyone you think may be relevant and interested in participating as well. Thank you for your consideration and I look forward to hearing from you.

Best wishes,

Anjuli Shere

Anjuli (@AnjuliRKShere) is an analyst, writer, and researcher, currently pursuing a DPhil in Cyber Security at the University of Oxford. Building on years of professional experience in both journalism and open-source investigations, Anjuli's doctoral project focuses on how transnational media companies establish threat models and respond to perceived cyber security threats in terms of training, protection, and prevention. She is particularly interested in exploring these issues in democracies who are currently facing strains from outside influences and new overreaching data protection and retention legislation, such as Taiwan, Australia, the UK, and the US, building on her existing academic and professional experiences in these countries. In her research, Anjuli combines theoretical understandings of computer science, cyber security, and journalism training with policy-oriented practical solutions, developed through both qualitative and quantitative methods. The objective is to create a framework for the press in democratic countries to consider when designing their internal policies and strategies to protect journalists and sources against contemporary and anticipatory threat models.

Appendix H: Validation study media expert survey

Online questionnaire hosted at: https://oxford.onlinesurveys.ac.uk/media-expert-survey

Page 1: General information about the study
Survey Objective: Co-creation of a framework of protections against consumer Internet of Things threats to the media

I, Anjuli Shere (doctoral researcher in Cyber Security at the University of Oxford) am investigating Internet of Things threats to journalists and their sources.

The "Internet of Things" has nebulous definitions, but here refers to networked devices that can collect and share data with each other. For the purposes of this research, examples cannot include phones, laptops, or tablets; however, the IoT does include: voice operated assistants (Alexa, Google Home), wearable smart technology (fitness trackers, smart watches), smart toys (gaming systems and smart TVs, children's toys, recreational use drones), internet-connected cars, internet-connected security systems, remote-access lighting systems, etc.

I have created a framework of possible protective measures that can be implemented by the media to counter these threats. This survey is intended to validate this framework.

Validation is an important stage in the academic process, which involves evaluation of a specific output - in this case a multi-column framework - to assess the content of the framework. Following validations, my research will build on this framework to create an interactive tool that can be used by members of the media as part of risk assessment and management practices.

Page 2: Informed consent
We appreciate your interest in participating in this online survey.

You have been invited to participate as you are over the age of 18 and have experience and expertise in journalistic issues. Please read through these terms before agreeing to participate by **ticking the 'yes' box below**. You may ask any questions before taking part by contacting the researcher (details below). This survey will cover basic biographical information to establish your expertise and experience in journalism, as well as questions about the countermeasures we have collected to protect against Internet of Things threats. **It should take approximately 45 minutes to complete**, if you are willing to spend time answering some of the open questions, with a deadline of 1st March 2022.

Questions will be broken into sections for ease of response. The resultant data will be analysed by Anjuli Shere and will be accessible by her supervisors, Prof. Andrew Martin and Dr. Jason Nurse.

Do I have to take part?
Please note that your participation is voluntary. You may withdraw at any point during the questionnaire for any reason, before submitting your answers, by closing the browser.

How will your data be used?
Participants are welcome to request that their responses and data be pseudonymised, but I anticipate that attributing responses to individual participants will lend the final analytical product of this research more authority through transparency. Privacy options for participants are that they are named with

direct quotes, named with indirect quotes, pseudonymised with direct quotes, or pseudonymised with indirect quotes.

At the start of the survey, there are also biographical questions that specifically ask about your job title and company. If you do not feel comfortable revealing this information, please describe the answers in whatever amount of detail you feel comfortable disclosing. Although every reasonable effort has been taken, confidentiality during actual internet communication procedures cannot be guaranteed.

Your data will be stored in a password-protected file and may be used in academic publications. Your IP address will not be stored. If you prefer not to answer any open-ended questions, please just write "Prefer not to say" in the box provided.

Research data will be stored for a minimum of three years after publication or public release, according to university policy.

Who will have access to your data?
This survey is being conducted via 'Online Surveys,' which is fully compliant with all UK data protection laws. 'Online Surveys' is the data controller with respect to your personal data and, as such, will determine how your personal data is used. Please see their privacy notice here [https://www.onlinesurveys.ac.uk/terms-and-conditions/].

Your information may be shared with supervisors and members of the project. We would like your permission to use your responses in future studies. Any personal information that you provide that we feel to be sensitive will be removed or changed before files are shared with other researchers or results are made public. Responsible members of the University of Oxford and funders may be given access to data for monitoring and/or audit of the study to ensure we are complying with guidelines, or as otherwise required by law. This questionnaire is for a DPhil (doctoral) project. The principal researcher is Anjuli Shere, who is currently attached to the **Department of Computer Science** at the University of Oxford. This project is being completed under the supervision of **Prof. Andrew Martin and Dr. Jason R. C. Nurse**.

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee. **Reference number: CS_C1A_021_027**.

What if there is a problem?
If you have a concern about any aspect of this project, please speak to the researcher, Anjuli Shere (anjuli.shere@cybersecurity.ox.ac.uk), or their supervisors, Prof. Andrew Martin (andrew.martin@cs.ox.ac.uk) or Dr. Jason R. C. Nurse (j.r.c.nurse@kent.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant Chair of the Research Ethics Committee at the University of Oxford:
Chair of the Computer Science Departmental Research Ethics Committee; Email: ethics@cs.ox.ac.uk; Address: Wolfson Building, Parks Road, Oxford OX1 3QD. The Chair will seek to resolve the matter in a reasonably expeditious manner.

Please note that, due to the nature of our ethical approval, you may only participate in this survey if you are 18 years of age or over.

☐ **I certify that I am 18 years of age or over.**

If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started.

☐ **Yes, I agree to take part**

We would like your consent to use some of your responses in any research output, e.g. published papers. If you consent to this, please check the box below.

☐ **Yes, I consent to my responses being used in any research output**

Page 3: Survey Section 1: Professional Experience & Expertise

1. OPTIONAL: What is your name? *[text answer]*
2. How would you like the information you provide to be attributed in this research project? *[multiple-choice]*
    a. *Named with direct quotes*
    b. *Named with indirect quotes*
    c. *Pseudonymised with direct quotes*
    d. *Pseudonymised with indirect quotes*
3. How would you describe the general category of your role in the media? *[multiple-choice]*
    a. *Risk Management Personnel;*
    b. *Editorial/Narrative Producers (inc. Programme Editors);*
    c. *Business/Corporate/Commercial/Organisational Stakeholders;*
    d. *Technical Operators;*
    e. *other + text*
4. For how many years have you worked in/on, studied, and/or researched journalism? *[numerical answer]*

Page 4: Section 2: Validating the framework - Explanation

The framework suggests 20 countermeasures that were found through 70+ interviews with experts, as well as reviewing academic literature and news articles. These countermeasures cover behaviours, actions and long-term goals that are likely to protect against and mitigate threats to the media from the Internet of Things.

On the following pages, you will be asked to match each countermeasure to:

(1) The overarching phase(s) of the journalistic workflow to which the countermeasure is most relevant (per the top-level workflow designated by the Association for International Broadcasting, AIB)
(2) The category of media roles that is most likely to be responsible for implementation of the countermeasure
(3) The beneficiary of the countermeasure
(4) The feasibility of the countermeasure

For many of the countermeasures, you may feel that there are multiple possible answers. However, in order to streamline recommendations to users, *please choose only the single best answer.*

In the final section of this survey, you will be asked some open-ended questions regarding your thoughts on the content of the survey. Thank you in advance for your time.

Pages 5-25: Section 2: Validating the framework - Questions
[NOTE DESCRIBING EACH COUNTERMEASURE]

1. To which phase(s) of the journalistic workflow do you think that this countermeasure is most relevant? *[multiple choice]*
    a. *Stage 1: Pitch/Propose, Research, Plan, Develop Script*
    b. *Stage 2: Deploy, Gather, Acquire, Create*
    c. *Stage 3: Script Revisions, Assemble, Edit, Review*
    d. *Stage 4: Publish, Distribute, Curate*
    e. *Stage 5: Archive, Report, Legal Review, Complaints, Re-Use*
    f. *All of the above/This countermeasure is an action that exists in parallel with the editorial workflow*
    g. *Other + text*
2. What is the category of media roles that you think is most likely to be responsible for implementation of this countermeasure? *[multiple-choice]*
    a. *Risk Management Personnel;*
    b. *Editorial/Narrative Producers (inc. Programme Editors);*
    c. *Business/Corporate/Commercial/Organisational Stakeholders;*
    d. *Technological Editorial Contributors*
    e. *Other + text*
3. Which of the following options do you think this countermeasure will most help? *[multiple-choice]*
    a. *individual members of the press*
    b. *news organisations as businesses*
    c. *the future of the news media existentially*
    d. *Other + text*
4. OPTIONAL: What, if anything, would you change about the phrasing of this countermeasure? Why? *[text answer]*

No clear countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.

- What, if anything, would you change about the phrasing of this countermeasure? Why? *[text answer]*

Page 26: Section 3: Feasibility of implementation scales
Feasibility can help members of the media make the decision about which countermeasures to implement first, or at all.

In this section, you will see that every countermeasure has a 1-5 numbered scale next to it. Each point on the scale relates to a description relating to feasibility:

1. "quick win" (i.e. controls that can be swiftly implemented),
2. "mid-term effort" (i.e. takes weeks to months),
3. "long-term effort" (i.e. this work is unlikely to ever be finished),
4. "collective win" (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat),

5. “unicorn” (i.e. unlikely to be worth time and effort in most circumstances).

Having read these descriptions, please assign each countermeasure the level of feasibility of implementation that you think is most accurate.

Example:

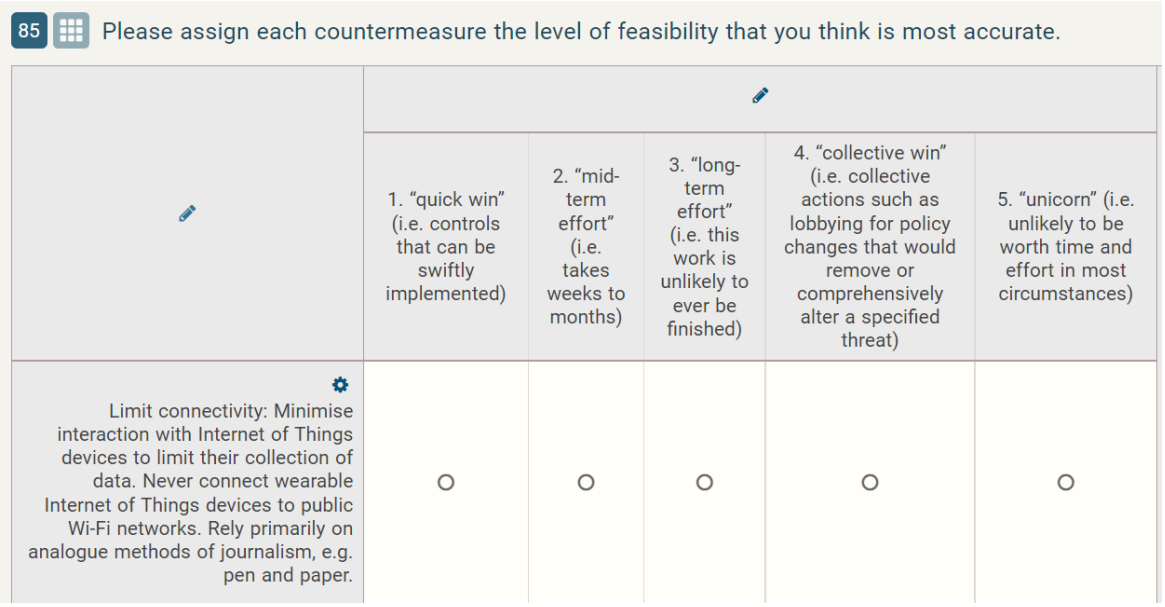


Figure 23: Screenshot to show survey question about feasibility

1. **Limit connectivity:** Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.
    a. *1-5 scale*
2. **IoT-free contingency plans:** Push for media stakeholders (e.g. news organisations) to create emergency/contingency plans that do not involve Internet of Things devices. These plans should acknowledge the risks associated with reliance on such devices to, for example, keep track of correspondents in dangerous environments.
    a. *1-5 scale*
3. **Transparency reporting:** Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices about device purchasing and can warn their sources about these devices.
    a. *1-5 scale*
4. **Travelling without local storage:** Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control.
    a. *1-5 scale*
5. **Network segmentation:** Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices.

    a. *1-5 scale*
6. **Aesthetic disguises:** Consider employing some methods of hiding one's face in ambient settings, through make-up, masks, clothing choices, etc.
    a. *1-5 scale*
7. **Audio obfuscation:** White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.
    a. *1-5 scale*
8. **Patching:** Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.
    a. *1-5 scale*
9. **Stronger passwords:** Internet of Things devices should not have default passwords (this is both an individual responsibility to change passwords upon purchase of a device, and also a necessary legislative shift to make sure that devices all have distinct default passwords).
    a. *1-5 scale*
10. **Wi-Fi security:** Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.
    a. *1-5 scale*
11. **Collaborative technology design:** News organisations and media-related civil society organisations could fund and collaborate with cyber security researchers and designers on the creation of cutting-edge intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become mandatory within press institutions.
    a. *1-5 scale*
12. **Firewalls:** If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.
    a. *1-5 scale*
13. **Physically cover cameras:** Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.
    a. *1-5 scale*
14. **Block the signal:** Faraday bags can be used to transport devices or temporarily block Internet of Things device capabilities.
    a. *1-5 scale*
15. **Research device security:** As with smartphones, if an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. If an individual member of the press must frequently use or be in spaces where Internet of Things devices exist, they should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.
    a. *1-5 scale*
16. **Intelligence sharing:** Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). Their goal is to share information on topics from best practices to threat intelligence,

which would establish a minimum standard of education and awareness of emerging Internet of Things threats.
    a. *1-5 scale*
17. **Top-down education:** Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.
    a. *1-5 scale*
18. **IoT-specific risk assessments:** Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.
    a. 1-5 scale
19. **Legal scrutiny:** There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.
    a. 1-5 scale
20. **No clear countermeasure yet:** Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.
    a. 1-5 scale

Page 27: Section 4: Open-ended contributions

1. Do you have any additional suggestions about countermeasures that could be useful to journalists against consumer IoT threats? *[text answer]*
2. Based on your experience and expertise, would this framework of countermeasures usefully add to the journalist security materials available? *[Y/N]*
    a. If yes, why?
    b. If no, why not?
3. Can you attest that any of the named countermeasures are already in practice within media operations for which you are responsible? *[Y/N]*
    a. If yes, when did you first see them implemented? *[text answer]*
3. In your experience, how could this framework of countermeasures be best used to improve journalist security practices? *[text answer]*
4. Do you have any additional suggestions about how best to make journalists aware of Internet of Things threats and countermeasures, such as those included in this survey? *[text answer]*
5. Do you have any other feedback about the material covered in this survey? *[text answer]*

Page 28: Thank you - and focus group invitation

Thank you for your involvement in this survey!

If you have any questions about the research or how your responses will be used or if you are interested in taking part in ONE focus group to evaluate a new tool based on this research, please contact the researcher Anjuli Shere at anjuli.shere@cybersecurity.ox.ac.uk

Appendix I: Validation study cyber security expert survey - Feasibility and Function

Online questionnaire hosted at: https://oxford.onlinesurveys.ac.uk/function-and-feasibility-survey

Page 1: General information about the study
Survey Objective: Evaluation of the function and feasibility of implementation of countermeasures against consumer Internet of Things threats to the media

I, Anjuli Shere (doctoral researcher in Cyber Security at the University of Oxford) am investigating Internet of Things threats to journalists and their sources. The "Internet of Things" here refers to networked devices that can collect and share data with each other. Examples do not include phones, laptops, or tablets, but do include: voice operated assistants (Alexa, Google Home), wearable smart technology (fitness trackers, smart watches), smart toys (gaming systems and smart TVs, children's toys, recreational use drones), internet-connected cars, internet-connected security systems, remote-access lighting systems, etc.

I have created a framework of possible protective measures that can be implemented by the media to counter these threats. This survey is intended to validate this framework.

Validation is an important stage in the academic process, which involves evaluation of a specific output - in this case a multi-column framework - to assess the content of the framework. Following validations, my research will build on this framework to create an interactive tool that can be used by members of the media as part of risk assessment and management practices.

Page 2: Informed consent
We appreciate your interest in participating in this online survey.

You have been invited to participate as you are over the age of 18 and have experience and expertise in cyber security. Please read through these terms before agreeing to participate by **ticking the 'yes' box below**. You may ask any questions before taking part by contacting the researcher (details below).

This survey will cover basic biographical information to establish your expertise and experience in cyber security, as well as questions about the countermeasures we have collected to protect against Internet of Things threats. It should take approximately 15 minutes to complete, if you are willing to spend time answering some of the open questions, with a deadline of **1st March 2022**.

Questions will be broken into sections for ease of response. The resultant data will be analysed by Anjuli Shere and will be accessible by her supervisors, Prof. Andrew Martin and Dr. Jason Nurse.

Do I have to take part?
Please note that your participation is voluntary. You may withdraw at any point during the questionnaire for any reason, before submitting your answers, by closing the browser.

How will your data be used?
Participants are welcome to request that their responses and data be pseudonymised, but I anticipate that attributing responses to individual participants will lend the final analytical product of this research more authority through transparency. Privacy options for participants are that they are named with

direct quotes, named with indirect quotes, pseudonymised with direct quotes, or pseudonymised with indirect quotes.

At the start of the survey, there are also biographical questions that specifically ask about your job title and company. If you do not feel comfortable revealing this information, please describe the answers in whatever amount of detail you feel comfortable disclosing. Although every reasonable effort has been taken, confidentiality during actual internet communication procedures cannot be guaranteed.

Your data will be stored in a password-protected file and may be used in academic publications. Your IP address will not be stored. If you prefer not to answer any open-ended questions, please just write "Prefer not to say" in the box provided.

Research data will be stored for a minimum of three years after publication or public release, according to university policy.

Who will have access to your data?
This survey is being conducted via 'Online Surveys,' which is fully compliant with all UK data protection laws. 'Online Surveys' is the data controller with respect to your personal data and, as such, will determine how your personal data is used. Please see their privacy notice here [https://www.onlinesurveys.ac.uk/terms-and-conditions/].

Your information may be shared with supervisors and members of the project. We would like your permission to use your responses in future studies. Any personal information that you provide that we feel to be sensitive will be removed or changed before files are shared with other researchers or results are made public. Responsible members of the University of Oxford and funders may be given access to data for monitoring and/or audit of the study to ensure we are complying with guidelines, or as otherwise required by law. This questionnaire is for a DPhil (doctoral) project. The principal researcher is Anjuli Shere, who is currently attached to the **Department of Computer Science** at the University of Oxford. This project is being completed under the supervision of **Prof. Andrew Martin and Dr. Jason R. C. Nurse**.

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee. **Reference number: CS_C1A_021_027**.

What if there is a problem?
If you have a concern about any aspect of this project, please speak to the researcher, Anjuli Shere (anjuli.shere@cybersecurity.ox.ac.uk), or their supervisors, Prof. Andrew Martin (andrew.martin@cs.ox.ac.uk) or Dr. Jason R. C. Nurse (j.r.c.nurse@kent.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant Chair of the Research Ethics Committee at the University of Oxford:
Chair of the Computer Science Departmental Research Ethics Committee; Email: ethics@cs.ox.ac.uk; Address: Wolfson Building, Parks Road, Oxford OX1 3QD. The Chair will seek to resolve the matter in a reasonably expeditious manner.

Please note that you may only participate in this survey if you are 18 years of age or over.
☐ **I certify that I am 18 years of age or over.**

If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started.

☐ **Yes, I agree to take part.**

We would like your consent to use some of your responses in any research output, e.g. published papers. If you consent to this, please check the box below.

☐ **Yes, I consent to my responses being used in any research output.**

Page 3: Survey Section 1: Professional Experience & Expertise

5. OPTIONAL: What is your name? *[text answer]*
6. How would you like the information you provide to be attributed in this research project? *[multiple-choice]*
    a. *Named with direct quotes*
    b. *Named with indirect quotes*
    c. *Pseudonymised with direct quotes*
    d. *Pseudonymised with indirect quotes*
7. Would you consider yourself to have expertise in cyber security? *[Y/N]*
    a. How would you describe the area of your expertise? *[text answer]*
8. For how many years have you worked and/or studied in the field of cyber security? *[numerical answer]*

Page 4: Section 2: Validating the framework - Explanation

The framework suggests 20 countermeasures that were found through 70+ interviews with experts, as well as reviewing academic literature and news articles. These countermeasures cover behaviours, actions and long-term goals that are likely to protect against and mitigate threats to the media from the Internet of Things.

On the following pages, you will be asked questions relating to (1) the function of each countermeasure, (2) the feasibility of implementation of each countermeasure.

In the final section of this survey, you will be asked open-ended questions regarding your thoughts on the content of the survey. Thank you in advance for your time.

Page 5: Section 3: Threats

This survey will refer to numbered threats posed by the Internet of Things to journalism. Please open the list of these threats, which can be found **here [**T2 for threats column of framework.pdf**]**. You must keep both the survey and this list open for the duration of the survey.

In the below questions, you'll see that countermeasures have been assigned threats already. These choices are based on my research so far. In the next section of this survey, you will be asked to state whether you agree with these matches.

☐ **Yes, I have opened the list of threats and will keep it open for the duration of this survey**

1. Please skim the list of threats and let us know if there are any that you would add/change.
    a. *No changes*
    b. *I would add/change the following: [text answer]*

Page 6: Section 4: Function of countermeasure scales

There are lots of potential angles to take in determining how to best explain how a countermeasure will mitigate a specific threat; one way is to group countermeasures into categories by similar functionalities. To utilise existing research as a foundation for these categorisations, the functions assigned to each countermeasure are categories created by Ahmad *et al*.

In this section, you will see that every countermeasure has a 1-9 numbered scale next to it. Each point on the scale relates to a description relating to function of the countermeasure:

6. Prevention (PREV): Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure
7. Deterrence (DETER): Deterrence employs disciplinary action to influence human behavior and attitude
8. Surveillance (SURV): Surveillance is the systematic monitoring of the security environment towards developing situational awareness to assist in adapting to fast-changing circumstances and threats
9. Detection (DETECT): Detection is an operational-level strategy aimed at identifying specific security behavior
10. Response (RESP): Response takes appropriate corrective actions against identified attacks
11. Deception (DECEP): Deception distracts an attacker's attention from critical information assets using decoys thereby leading the attacker to waste time and resources
12. Perimeter defense (PERI): Perimeter defense creates a boundary around information assets that is secured by regulating traffic at every incoming and outgoing information channel (choke points)
13. Compartmentalization (COMP): Compartmentalization reduces an attacker's opportunities by dividing the intended area of attack into zones that are secured separately
14. Layering (LAYER): Layering uses multiple countermeasures that function independently but increases the effectiveness of the defense when working together thereby posing a series of challenges to the attacker. The defensive system is designed to be resilient by overlapping the series of countermeasures, whereby each countermeasure complements the next so that if one fails another will back it up

Having read these descriptions, please assign each countermeasure the function that you think is most accurate. There will be an opportunity at the end of this survey to provide feedback on these function categories and the countermeasures themselves.

Example:

10. Having read these descriptions, please assign each countermeasure the function that you think is **most** accurate. It may help to remember that functions 1-6 (PREV to DECEP) are temporal, while 7-9 (PERI to LAYER) are spatial. There will be an opportunity at the end of this survey to provide feedback on these function categories and the countermeasures themselves.

** Required*

	Prevention (PREV)	Deterrence (DETER)	Surveillance (SURV)	Detection (DETECT)	Response (RESP)	Deception (DECEP)	Perimeter defense (PERI)	Compartmentalization (COMP)	Layering (LAYER)
Limit connectivity: Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.	○	○	○	○	○	○	○	○	○

Figure 24: Screenshot to show survey question about function

21. **Limit connectivity:** Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.
    a. *1-9 scale*
22. **IoT-free contingency plans:** Push for media stakeholders (e.g. news organisations) to create emergency/contingency plans that do not involve Internet of Things devices. These plans should acknowledge the risks associated with reliance on such devices to, for example, keep track of correspondents in dangerous environments.
    a. *1-9 scale*
23. **Transparency reporting:** Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices about device purchasing and can warn their sources about these devices.
    a. *1-9 scale*
24. **Travelling without local storage:** Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control.
    a. *1-9 scale*
25. **Network segmentation:** Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices.
    a. *1-9 scale*
26. **Aesthetic disguises:** Consider employing some methods of hiding one's face in ambient settings, through make-up, masks, clothing choices, etc.
    a. *1-9 scale*
27. **Audio obfuscation:** White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.
    a. *1-9 scale*

28. **Patching:** Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.
    a. *1-9 scale*
29. **Stronger passwords:** Internet of Things devices should not have default passwords (this is both an individual responsibility to change passwords upon purchase of a device, and also a necessary legislative shift to make sure that devices all have distinct default passwords).
    a. *1-9 scale*
30. **Wi-Fi security:** Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.
    a. *1-9 scale*
31. **Collaborative technology design:** News organisations and media-related civil society organisations could fund and collaborate with cyber security researchers and designers on the creation of cutting-edge intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become mandatory within press institutions.
    a. *1-9 scale*
32. **Firewalls:** If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.
    a. *1-9 scale*
33. **Physically cover cameras:** Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.
    a. *1-9 scale*
34. **Block the signal:** Faraday bags can be used to transport devices or temporarily block Internet of Things device capabilities.
    a. *1-9 scale*
35. **Research device security:** As with smartphones, if an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. If an individual member of the press must frequently use or be in spaces where Internet of Things devices exist, they should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.
    a. *1-9 scale*
36. **Intelligence sharing:** Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). Their goal is to share information on topics from best practices to threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.
    a. *1-9 scale*
37. **Top-down education:** Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.

    a. *1-9 scale*
38. **IoT-specific risk assessments:** Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.
    a. *1-9 scale*
39. **Legal scrutiny:** There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.
    a. *1-9 scale*
40. **No clear countermeasure yet:** Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.
    a. *1-9 scale*

Page 7: Section 5: Feasibility of implementation scales
Feasibility can help members of the media to make the decision about which countermeasures to implement first, or at all. Regarding these countermeasures, feasibility relates to ease of use (cost and knowledge) and time taken to implement an action.

In this section, you will see that every countermeasure has a 1-5 numbered scale next to it. Each point on the scale relates to a description relating to feasibility:

1. "quick win" (i.e. controls that can be swiftly implemented),
2. "mid-term effort" (i.e. takes weeks to months),
3. "long-term effort" (i.e. this work is unlikely to ever be finished),
4. "collective win" (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat),
5. "unicorn" (i.e. unlikely to be worth time and effort in most circumstances).

Having read these descriptions, please assign each countermeasure the level of feasibility that you think is most accurate. There will be an opportunity at the end of this survey to provide feedback on these feasibility categories and the countermeasures themselves.

For example: See Figure 23

41. **Limit connectivity:** Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.
    a. *1-5 scale*
42. **IoT-free contingency plans:** Push for media stakeholders (e.g. news organisations) to create emergency/contingency plans that do not involve Internet of Things devices. These plans should acknowledge the risks associated with reliance on such devices to, for example, keep track of correspondents in dangerous environments.
    a. *1-5 scale*
43. **Transparency reporting:** Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press,

can make informed choices about device purchasing and can warn their sources about these devices.

    a. *1-5 scale*

44. **Travelling without local storage:** Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control.
    a. *1-5 scale*
45. **Network segmentation:** Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices.
    a. *1-5 scale*
46. **Aesthetic disguises:** Consider employing some methods of hiding one's face in ambient settings, through make-up, masks, clothing choices, etc.
    a. *1-5 scale*
47. **Audio obfuscation:** White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.
    a. *1-5 scale*
48. **Patching:** Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.
    a. *1-5 scale*
49. **Stronger passwords:** Internet of Things devices should not have default passwords (this is both an individual responsibility to change passwords upon purchase of a device, and also a necessary legislative shift to make sure that devices all have distinct default passwords).
    a. *1-5 scale*
50. **Wi-Fi security:** Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.
    a. *1-5 scale*
51. **Collaborative technology design:** News organisations and media-related civil society organisations could fund and collaborate with cyber security researchers and designers on the creation of cutting-edge intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become mandatory within press institutions.
    a. *1-5 scale*
52. **Firewalls:** If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.
    a. *1-5 scale*
53. **Physically cover cameras:** Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.
    a. *1-5 scale*

54. **Block the signal:** Faraday bags can be used to transport devices or temporarily block Internet of Things device capabilities.
    a. *1-5 scale*
55. **Research device security:** As with smartphones, if an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. If an individual member of the press must frequently use or be in spaces where Internet of Things devices exist, they should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.
    a. *1-5 scale*
56. **Intelligence sharing:** Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). Their goal is to share information on topics from best practices to threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.
    a. *1-5 scale*
57. **Top-down education:** Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.
    a. *1-5 scale*
58. **IoT-specific risk assessments:** Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.
    a. *1-5 scale*
59. **Legal scrutiny:** There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.
    a. *1-5 scale*
60. **No clear countermeasure yet:** Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.
    a. *1-5 scale*

Page 8: Section 6: Optional open-ended contributions

1. Do you have any additional suggestions about protection or mitigations that could be useful to journalists against consumer IoT threats? *[text answer]*
2. Do you have any additional suggestions about how best to make lay people (e.g. journalists) aware of existing protection and mitigation materials, such as those included in this survey? *[text answer]*
3. Do you have any other feedback about the material covered in this survey? *[text answer]*

Page 9: Final Page - Thank you!

Thank you for your involvement in this survey! If you have any questions about the research or how your responses will be used, please contact the researcher Anjuli Shere at anjuli.shere@cybersecurity.ox.ac.uk

Appendix J: Validation study cyber security expert survey - Matching threats to countermeasures & countermeasures to disadvantages

Online questionnaire hosted at: https://oxford.onlinesurveys.ac.uk/threat-countermeasure-matching-survey

Page 1: General information about the study
Survey Objective: Evaluation of countermeasures against consumer Internet of Things threats to the media

I, Anjuli Shere (doctoral researcher in Cyber Security at the University of Oxford) am investigating Internet of Things threats to journalists and their sources. The "Internet of Things" here refers to networked devices that can collect and share data with each other. Examples do not include phones, laptops or tablets, but do include: voice operated assistants (Alexa, Google Home), wearable smart technology (fitness trackers, smart watches), smart toys (gaming systems and smart TVs, children's toys, recreational use drones), internet-connected cars, internet-connected security systems, remote-access lighting systems, etc.

I have created a framework of possible protective measures that can be implemented by the media to counter these threats. This survey is intended to validate this framework.

Validation is an important stage in the academic process, which involves evaluation of a specific output - in this case a multi-column framework - to assess the content of the framework. Following validations, my research will build on this framework to create an interactive tool that can be used by members of the media as part of risk assessment and management practices.

Page 2: Informed consent
We appreciate your interest in participating in this online survey.

You have been invited to participate as you are over the age of 18 and have experience and expertise in cyber security. Please read through these terms before agreeing to participate by **ticking the 'yes' box below**. You may ask any questions before taking part by contacting the researcher (details below).

This survey will include **[NUMBER]** questions, and will cover basic biographical information to establish your expertise and experience in cyber security, as well as questions about the countermeasures we have collected to protect against Internet of Things threats. It should take approximately 30 minutes to complete, if you are willing to spend time answering some of the open questions, with a deadline of **[DATE]**.

Questions will be broken into sections for ease of response. The resultant data will be analysed by Anjuli Shere and will be accessible by her supervisors, Prof. Andrew Martin and Dr. Jason Nurse.

Do I have to take part?
Please note that your participation is voluntary. You may withdraw at any point during the questionnaire for any reason, before submitting your answers, by closing the browser.

How will your data be used?

Participants are welcome to request that their responses and data be pseudonymised, but I anticipate that attributing responses to individual participants will lend the final analytical product of this research more authority through transparency. Privacy options for participants are that they are named with direct quotes, named with indirect quotes, pseudonymised with direct quotes, or pseudonymised with indirect quotes.

At the start of the survey, there are also biographical questions that specifically ask about your job title and company. If you do not feel comfortable revealing this information, please describe the answers in whatever amount of detail you feel comfortable disclosing. Although every reasonable effort has been taken, confidentiality during actual internet communication procedures cannot be guaranteed.

Your data will be stored in a password-protected file and may be used in academic publications. Your IP address will not be stored. If you prefer not to answer any open-ended questions, please just write "Prefer not to say" in the box provided.

Research data will be stored for a minimum of three years after publication or public release, according to university policy.

Who will have access to your data?
This survey is being conducted via 'Online Surveys,' which is fully compliant with all UK data protection laws. 'Online Surveys' is the data controller with respect to your personal data and, as such, will determine how your personal data is used. Please see their privacy notice here [https://www.onlinesurveys.ac.uk/terms-and-conditions/].

Your information may be shared with supervisors and members of the project. We would like your permission to use your responses in future studies. Any personal information that you provide that we feel to be sensitive will be removed or changed before files are shared with other researchers or results are made public. Responsible members of the University of Oxford and funders may be given access to data for monitoring and/or audit of the study to ensure we are complying with guidelines, or as otherwise required by law. This questionnaire is for a DPhil (doctoral) project. The principal researcher is Anjuli Shere, who is currently attached to the **Department of Computer Science** at the University of Oxford. This project is being completed under the supervision of **Prof. Andrew Martin and Dr. Jason R. C. Nurse**.

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee. **Reference number: CS_C1A_021_027**.

What if there is a problem?
If you have a concern about any aspect of this project, please speak to the researcher, Anjuli Shere (anjuli.shere@cybersecurity.ox.ac.uk), or their supervisors, Prof. Andrew Martin (andrew.martin@cs.ox.ac.uk) or Dr. Jason R. C. Nurse (j.r.c.nurse@kent.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant Chair of the Research Ethics Committee at the University of Oxford:
Chair of the Computer Science Departmental Research Ethics Committee; Email: ethics@cs.ox.ac.uk; Address: Wolfson Building, Parks Road, Oxford OX1 3QD. The Chair will seek to resolve the matter in a reasonably expeditious manner.

Please note that you may only participate in this survey if you are 18 years of age or over.

☐ **I certify that I am 18 years of age or over.**
If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started.
☐ **Yes, I agree to take part**
We would like your consent to use some of your responses in any research output, e.g. published papers. If you consent to this, please check the box below.
☐ **Yes, I consent to my responses being used in any research output**

Page 3: Survey Section 1: Professional Experience & Expertise

9. OPTIONAL: What is your name? *[text answer]*
10. How would you like the information you provide to be attributed in this research project? *[multiple-choice]*
    a. *Named with direct quotes*
    b. *Named with indirect quotes*
    c. *Pseudonymised with direct quotes*
    d. *Pseudonymised with indirect quotes*
11. Would you consider yourself to have expertise in cyber security? *[Y/N]*
    a. How would you describe the area of your expertise? *[text answer]*
12. For how many years have you worked and/or studied in the field of cyber security? *[numerical answer]*

Page 4: Section 2: Validating the framework - Explanation
The framework suggests 20 countermeasures that were found through 70+ interviews with experts, as well as reviewing academic literature and news articles. These countermeasures cover behaviours, actions and long-term goals that are likely to protect against and mitigate threats to the media from the Internet of Things.

On the following pages, you will be asked questions relating to the following topics:
(5) Matching countermeasures to threats
(6) Disadvantages of countermeasures

In the final section of this survey, you will be asked some open-ended questions regarding your thoughts on the content of the survey. Thank you in advance for your time.

Page 5: Section 2: Threats
This survey will refer to numbered threats posed by the Internet of Things to journalism. Please open the list of these threats, which can be found **here [**T2 for threats column of framework.pdf**]**. You must keep both the survey and this list open for the duration of the survey.

In the below questions, you'll be asked to match each of the countermeasures to the relevant threats.

☐ **Yes, I have opened the list of threats and will keep it open for the duration of this survey**

2. Please skim the list of threats and let us know if there are any that you would add/change.

c. *No changes*
d. *I would add/change the following: [text answer]*

Page 6: Section 3: Matching countermeasures to threats and disadvantages (each countermeasure is a new page)

1. **Limit connectivity:** Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats and the option to "select ALL"

Example:

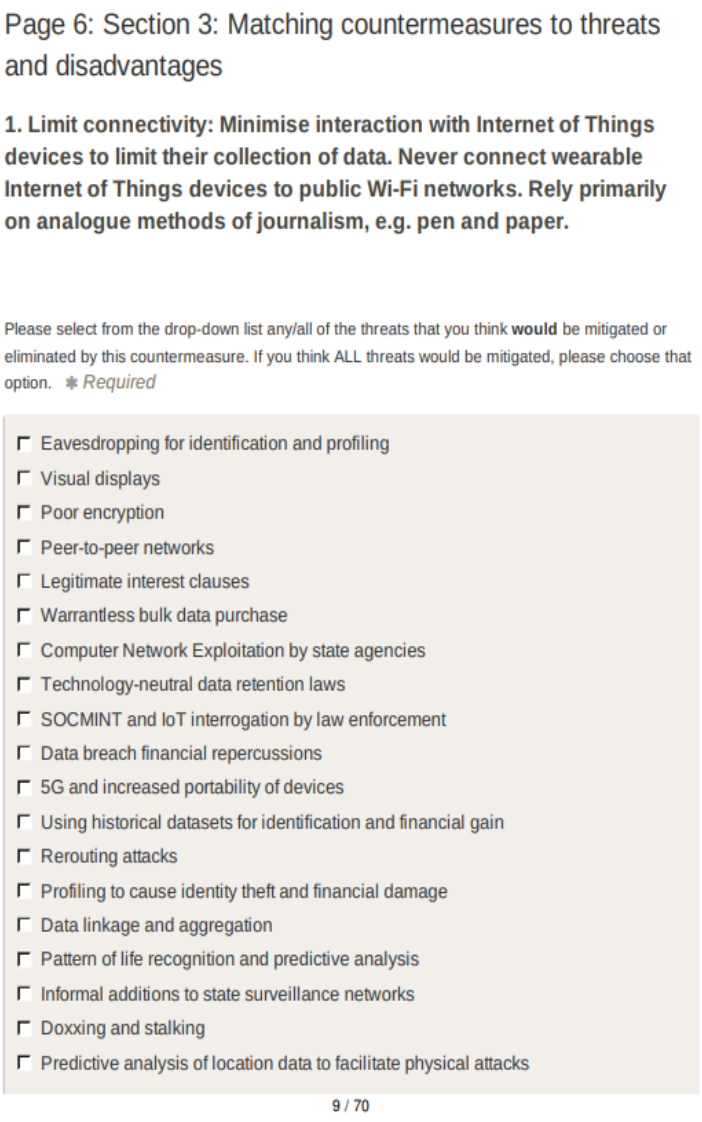


Figure 25: Screenshot of survey question matching threats to countermeasures

b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list. *[multiple-choice]*
    i. You don't get any of the benefits of IoT
    ii. Short-term solution as you won't be able to opt out of an environment that includes IoT features for long
    iii. This is time-consuming, you have to put a lot of effort into (e.g.) not being tracked (i.e. changes of clothes, makeup), or into not coming into contact with other people's IoT devices (i.e. you'd have to meet sources in isolated areas)
    iv. Decreased connectivity makes communication and organisation harder
    v. Increases likelihood of successful physical theft of information
    vi. Other *[open-text]*

Example:

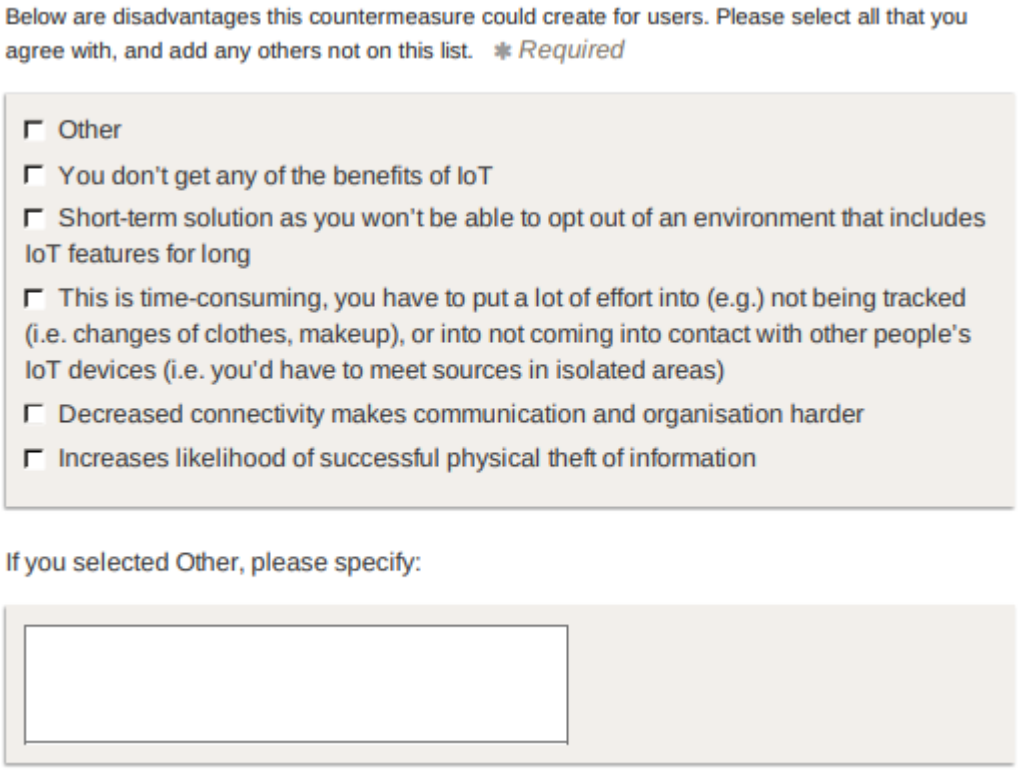


Figure 26: Screenshot of survey question assigning disadvantages to countermeasures

2. **IoT-free contingency plans:** Push for media stakeholders (e.g. news organisations) to create emergency/contingency plans that do not involve Internet of Things devices. These plans should acknowledge the risks associated with reliance on such devices to, for example, keep track of correspondents in dangerous environments.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*

i. Long-term solution so can't help in short-term
ii. Governments are historically slow with regulating new technology
iii. Relies on people actually obeying the law
iv. Other *[open-text]*

3. **Transparency reporting:** Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices about device purchasing and can warn their sources about these devices.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Increased information available for attackers about which companies are holding what types of data
        ii. Other *[open-text]*
4. **Travelling without local storage:** Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Deleted data can be recovered through a variety of digital forensics methods.
        ii. The purpose of some IoT technologies, such as fitness trackers, is to continually collect data. Therefore, disconnecting them and disabling their function would ultimately render them less useful.
        iii. Other *[open-text]*
5. **Network segmentation:** Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Not possible for every format, e.g. you can't airgap a phone or a smart vehicle
        ii. Human exploits can overcome airgaps; some functionality might be lost if the network is segmented
        iii. Air-gaps/network segmentation aren't infallible, especially to well-resourced attackers
        iv. Other *[open-text]*

6. **Aesthetic disguises:** Consider employing some methods of hiding one's face in ambient settings, through make-up, masks, clothing choices, etc.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Time-consuming
        ii. Hard to beat some systems (e.g. AI or thermal facial recognition)
        iii. Easy to spot by humans, even if they fool machines. Ill-proven
        iv. Other *[open-text]*
7. **Audio obfuscation:** White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. You don't know whether they're working until something goes wrong (analogy of the safety mechanism on a gun)
        ii. Unlikely to be implemented in practice
        iii. Under-researched technology, not proven to work
        iv. Other *[open-text]*
8. **Patching:** Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Not all IoT devices have this option
        ii. Other *[open-text]*
9. **Stronger passwords:** Internet of Things devices should not have default passwords (this is both an individual responsibility to change passwords upon purchase of a device, and also a necessary legislative shift to make sure that devices all have distinct default passwords).
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Not all IoT devices have this option (but this is changing in some markets)
        ii. Other *[open-text]*

10. **Wi-Fi security:** Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Effective network configuration may be difficult for lay-people
        ii. Other *[open-text]*
11. **Collaborative technology design:** News organisations and media-related civil society organisations could fund and collaborate with cyber security researchers and designers on the creation of cutting-edge intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become mandatory within press institutions.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. While this is a service that companies are beginning to provide, it is not a very mature space
        ii. Other *[open-text]*
12. **Firewalls:** If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. May be difficult for lay-people
        ii. You can't know all the scanners/websites that are indexing your devices
        iii. Other *[open-text]*
13. **Physically cover cameras:** Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*

i. Can't do this for cameras that aren't in your possession
ii. Other *[open-text]*

14. **Block the signal:** Faraday bags can be used to transport devices or temporarily block Internet of Things device capabilities.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. You don't know whether they're working until something goes wrong (analogy of the safety mechanism on a gun)
        ii. Can't do this for devices that aren't in your possession
        iii. Other *[open-text]*
15. **Research device security:** As with smartphones, if an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. If an individual member of the press must frequently use or be in spaces where Internet of Things devices exist, they should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Not all the information will be publicly available, or accessible to lay-people
        ii. Expensive
        iii. Other *[open-text]*
16. **Intelligence sharing:** Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). Their goal is to share information on topics from best practices to threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Long-term goal
        ii. Not all journalists are facing attackers with the same technical/legislative capabilities, some may be unable to access this information
        iii. Other *[open-text]*
17. **Top-down education:** Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.

a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
    i. Drop-down list of all 45 threats + ALL
b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
    i. Long-term goal
    ii. Other *[open-text]*

18. **IoT-specific risk assessments:** Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Expensive and novel so not many materials available
        ii. Other *[open-text]*
19. **Legal scrutiny:** There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.
    a. Please select from the drop-down list any/all of the threats that you think **would** be mitigated or eliminated by this countermeasure. If you think ALL threats would be mitigated, please choose that option.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. Long-term goal
        ii. Other *[open-text]*
20. **No clear countermeasure yet:** Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.
    a. Please select from the drop-down list all of the threats that you think **have no mitigation or elimination countermeasure**.
        i. Drop-down list of all 45 threats + ALL
    b. Below are disadvantages this countermeasure could create for users. Please select all that you agree with, and add any others not on this list: *[each is Agree/Disagree]*
        i. No countermeasure
        ii. Other *[open-text]*

Page 9: Section 5: Optional open-ended contributions

1. Do you have any additional suggestions about protection or mitigations that could be useful to journalists against consumer IoT threats? *[text answer]*

2. Do you have any additional suggestions about how best to make lay people (e.g. journalists) aware of existing protection and mitigation materials, such as those included in this survey? *[text answer]*
3. Do you have any other feedback about the material covered in this survey? *[text answer]*

Page 10: Thank you!

Thank you for your involvement in this survey! If you have any questions about the research or how your responses will be used, please contact the researcher Anjuli Shere at anjuli.shere@cybersecurity.ox.ac.uk

Appendix K: Validations study state capabilities' expert survey

Online questionnaire hosted at: https://oxford.onlinesurveys.ac.uk/states-capabilities-expert-survey

Page 1: General information about the study
Survey Objective: Evaluation of countermeasures against consumer Internet of Things threats to the press

I, Anjuli Shere (doctoral researcher in Cyber Security at the University of Oxford) am investigating Internet of Things threats to journalists and their sources. The "Internet of Things" here refers to networked devices that can collect and share data with each other. Examples do not include phones, laptops or tablets, but do include: voice operated assistants (Alexa, Google Home), wearable smart technology (fitness trackers, smart watches), smart toys (gaming systems and smart TVs, children's toys, recreational use drones), internet-connected cars, internet-connected security systems, remote-access lighting systems, etc.

I have created a framework of possible protective measures that can be implemented by the press to counter these threats. This survey is intended to validate this framework.

Validation is an important stage in the academic process, which involves evaluation of a specific output - in this case a multi-column framework - to assess the content of the framework. Following validations, my research will build on this framework to create an interactive tool that can be used by members of the press as part of risk assessment and management practices.

Page 2: Informed consent
We appreciate your interest in participating in this online survey.

You have been invited to participate as you are over the age of 18 and have experience and expertise in states' capabilities. Please read through these terms before agreeing to participate by **ticking the 'yes' box below**. You may ask any questions before taking part by contacting the researcher (details below). This survey will cover basic biographical information to establish your expertise and experience in state capabilities, as well as questions about the countermeasures we have collected to protect against Internet of Things threats. It should take approximately 10 minutes to complete, if you are willing to spend time answering some of the open questions, with a deadline of 1st March 2022.

Questions will be broken into sections for ease of response. The resultant data will be analysed by Anjuli Shere and will be accessible by her supervisors, Prof. Andrew Martin and Dr. Jason Nurse.

Do I have to take part?
Please note that your participation is voluntary. You may withdraw at any point during the questionnaire for any reason, before submitting your answers, by closing the browser.

How will your data be used?
Participants are welcome to request that their responses and data be pseudonymised, but I anticipate that attributing responses to individual participants will lend the final analytical product of this research more authority through transparency. Privacy options for participants are that they are named with direct quotes, named with indirect quotes, pseudonymised with direct quotes, or pseudonymised with indirect quotes.

At the start of the survey, there are also biographical questions that specifically ask about your job title and company. If you do not feel comfortable revealing this information, please describe the answers in whatever amount of detail you feel comfortable disclosing. Although every reasonable effort has been taken, confidentiality during actual internet communication procedures cannot be guaranteed.

Your data will be stored in a password-protected file and may be used in academic publications. Your IP address will not be stored. If you prefer not to answer any open-ended questions, please just write "Prefer not to say" in the box provided.

Research data will be stored for a minimum of three years after publication or public release, according to university policy.

Who will have access to your data?
This survey is being conducted via 'Online Surveys,' which is fully compliant with all UK data protection laws. 'Online Surveys' is the data controller with respect to your personal data and, as such, will determine how your personal data is used. Please see their privacy notice here [https://www.onlinesurveys.ac.uk/terms-and-conditions/].

Your information may be shared with supervisors and members of the project. We would like your permission to use your responses in future studies. Any personal information that you provide that we feel to be sensitive will be removed or changed before files are shared with other researchers or results are made public. Responsible members of the University of Oxford and funders may be given access to data for monitoring and/or audit of the study to ensure we are complying with guidelines, or as otherwise required by law. This questionnaire is for a DPhil (doctoral) project. The principal researcher is Anjuli Shere, who is currently attached to the **Department of Computer Science** at the University of Oxford. This project is being completed under the supervision of **Prof. Andrew Martin and Dr. Jason R. C. Nurse**.

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee. **Reference number: CS_C1A_021_027**.

What if there is a problem?
If you have a concern about any aspect of this project, please speak to the researcher, Anjuli Shere (anjuli.shere@cybersecurity.ox.ac.uk), or their supervisors, Prof. Andrew Martin (andrew.martin@cs.ox.ac.uk) or Dr. Jason R. C. Nurse (j.r.c.nurse@kent.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant Chair of the Research Ethics Committee at the University of Oxford:
Chair of the Computer Science Departmental Research Ethics Committee; Email: ethics@cs.ox.ac.uk; Address: Wolfson Building, Parks Road, Oxford OX1 3QD. The Chair will seek to resolve the matter in a reasonably expeditious manner.

Please note that you may only participate in this survey if you are 18 years of age or over.
☐ **I certify that I am 18 years of age or over.**

If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started.

☐ **Yes, I agree to take part**

We would like your consent to use some of your responses in any research output, e.g. published papers. If you consent to this, please check the box below.

☐ **Yes, I consent to my responses being used in any research output**

Page 3: Survey Section 1: Professional Experience & Expertise

13. OPTIONAL: What is your name? *[text answer]*
14. How would you like the information you provide to be attributed in this research project? *[multiple-choice]*
    a. *Named with direct quotes*
    b. *Named with indirect quotes*
    c. *Pseudonymised with direct quotes*
    d. *Pseudonymised with indirect quotes*
15. Would you consider yourself to have knowledge of the exploitative technological and/or related legal capabilities of one or more states? *[Y/N]*
16. How do you have this knowledge? (We understand that you may not be able to give details, please just provide us with a category of experience/expertise - e.g. "I worked as an intelligence analyst for a state agency") *[open-text]*
17. For how many years have you worked and/or studied in the field of cyber security? *[numerical answer]*

Page 4: Section 2: Threats

This survey will refer to numbered threats posed by the Internet of Things to journalism. Please open the list of these threats, which can be found **here [**T2 for threats column of framework.pdf**]**. **You must keep both the survey and this list open for the duration of the survey.**

☐ **Yes, I have opened the list of threats and will keep it open for the duration of this survey**

Please skim the list of threats and let us know if there are any that you would add/change.

e. *No changes*
f. *I would add/change the following: [text answer]*

Page 5: Section 3: Validating the framework - Explanation

The framework suggests 20 countermeasures that were found through 70+ interviews with experts, as well as reviewing academic literature and news articles. These countermeasures cover behaviours, actions and long-term goals that are likely to protect against and mitigate threats to the media from the Internet of Things.

On the following pages, you will be asked questions regarding your thoughts on the realism of these threats and the utility of the assigned countermeasures.
Thank you in advance for your time.

Pages 6-8: Likert matrix of threats x scale of current realism (15 threats per page)

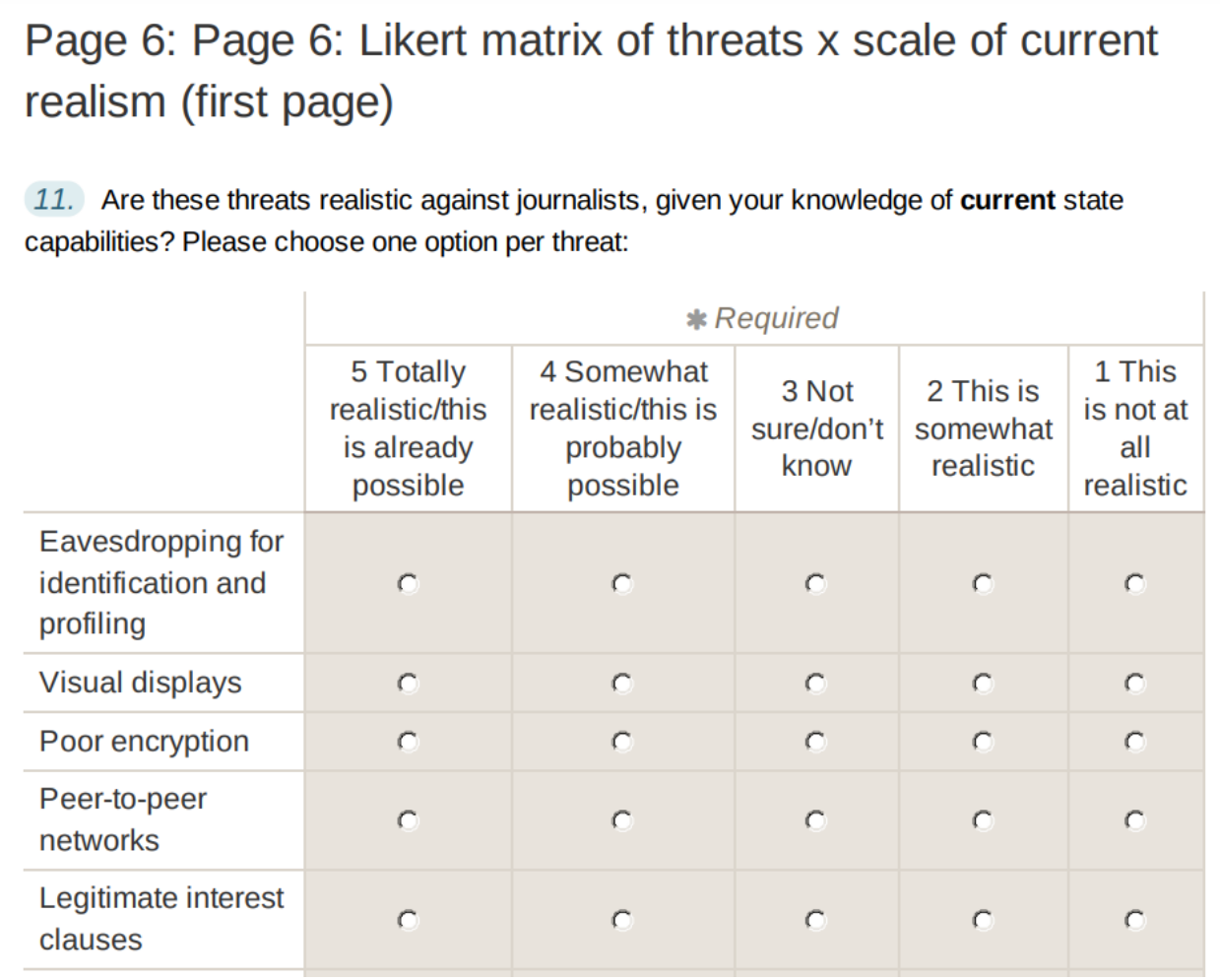
- Are these threats realistic against journalists, given your knowledge of **current** state capabilities? Please choose one option per threat:

[All 45 threats]

1. Eavesdropping for identification and profiling
2. Visual displays
3. Poor encryption
4. Peer-to-peer networks
5. Legitimate interest clauses
6. Warrantless bulk data purchase
7. Computer Network Exploitation by state agencies
8. Technology-neutral data retention laws
9. SOCMINT and IoT interrogation by law enforcement
10. Data breach financial repercussions
11. 5G and increased portability of devices
12. Using historical datasets for identification and financial gain
13. Rerouting attacks
14. Profiling to cause identity theft and financial damage
15. Data linkage and aggregation
16. Pattern of life recognition and predictive analysis
17. Informal additions to state surveillance networks
18. Doxxing and stalking
19. Predictive analysis of location data to facilitate physical attacks
20. Real-time vehicular hacking and tracking
21. Weak authorisation protocols facilitating third party data manipulation
22. Information Damage Level attacks against data confidentiality or integrity
23. Sybil attacks against data integrity
24. Consent requirements that include data manipulation
25. Malware-induced kinetic attacks
26. Altering health data
27. Falsifying timestamps to impede forensics
28. Altering user-facing device and data properties
29. Elevation of Privilege attacks
30. Hijacking connected accounts
31. Restrictive laws relating to ‘fake news’
32. Normalisation of monitoring of employees causing a decrease in reporting quality
33. Using health information to cause psychological pressure
34. Replay attack to manipulate devices with audio activation
35. Laser modulation to cause device activity
36. Exploitation of multiple devices to start and escalate an attack
37. Aggressive vehicular takeover
38. Changing the settings of essential devices
39. Involuntary data access
40. Restricting internet access
41. Device seizure
42. Spoofing to stop device actions
43. Denial of Service attacks
44. Botnet creation and use
45. Ransomware

- Scale of realism:
    - 5 Totally realistic/this is already possible
    - 4 Somewhat realistic/this is probably possible
    - 3 Not sure/don't know
    - 2 This is somewhat realistic
    - 1 This is not at all realistic

Example:



Page 6: Page 6: Likert matrix of threats x scale of current realism (first page)

11. Are these threats realistic against journalists, given your knowledge of **current** state capabilities? Please choose one option per threat:

✱ Required

	5 Totally realistic/this is already possible	4 Somewhat realistic/this is probably possible	3 Not sure/don't know	2 This is somewhat realistic	1 This is not at all realistic
Eavesdropping for identification and profiling	○	○	○	○	○
Visual displays	○	○	○	○	○
Poor encryption	○	○	○	○	○
Peer-to-peer networks	○	○	○	○	○
Legitimate interest clauses	○	○	○	○	○

Figure 27: Screenshot of survey question assigning current realism score to threats

Pages 9-11: Likert matrix of threats x scale of future realism (15 per page)

- Are these threats realistic against journalists, given your knowledge of **future** state capabilities? Please choose one option per threat:

[All 45 threats]

1. Eavesdropping for identification and profiling
2. Visual displays
3. Poor encryption
4. Peer-to-peer networks
5. Legitimate interest clauses

6. Warrantless bulk data purchase
7. Computer Network Exploitation by state agencies
8. Technology-neutral data retention laws
9. SOCMINT and IoT interrogation by law enforcement
10. Data breach financial repercussions
11. 5G and increased portability of devices
12. Using historical datasets for identification and financial gain
13. Rerouting attacks
14. Profiling to cause identity theft and financial damage
15. Data linkage and aggregation
16. Pattern of life recognition and predictive analysis
17. Informal additions to state surveillance networks
18. Doxxing and stalking
19. Predictive analysis of location data to facilitate physical attacks
20. Real-time vehicular hacking and tracking
21. Weak authorisation protocols facilitating third party data manipulation
22. Information Damage Level attacks against data confidentiality or integrity
23. Sybil attacks against data integrity
24. Consent requirements that include data manipulation
25. Malware-induced kinetic attacks
26. Altering health data
27. Falsifying timestamps to impede forensics
28. Altering user-facing device and data properties
29. Elevation of Privilege attacks
30. Hijacking connected accounts
31. Restrictive laws relating to 'fake news'
32. Normalisation of monitoring of employees causing a decrease in reporting quality
33. Using health information to cause psychological pressure
34. Replay attack to manipulate devices with audio activation
35. Laser modulation to cause device activity
36. Exploitation of multiple devices to start and escalate an attack
37. Aggressive vehicular takeover
38. Changing the settings of essential devices
39. Involuntary data access
40. Restricting internet access
41. Device seizure
42. Spoofing to stop device actions
43. Denial of Service attacks
44. Botnet creation and use
45. Ransomware

- Scale of realism:
    - 5 Totally realistic/this is already being planned/developed
    - 4 Somewhat realistic/this is likely to be already in the process of development
    - 3 Not sure/don't know
    - 2 This is somewhat possible
    - 1 This is not at all likely

Example:

Page 9: Page 9: Likert matrix of threats x scale of future realism (first page)

14. Are these threats realistic against journalists, given your knowledge of **future** state capabilities? Please choose one option per threat:

✱ *Required*

	5 Totally realistic/this is already being planned/developed	4 Somewhat realistic/this is likely to be already in the process of development	3 Not sure/don't know	2 This is somewhat possible	1 This is not at all likely
Eavesdropping for identification and profiling	○	○	○	○	○
Visual displays	○	○	○	○	○
Poor encryption	○	○	○	○	○
Peer-to-peer networks	○	○	○	○	○
Legitimate interest clauses	○	○	○	○	○

Figure 28: Screenshot of survey question assigning future realism score to threats

Page 12: Likert matrix of countermeasures x scale of current realism

- Could these countermeasures realistically be **usefully** implemented, given your knowledge of **current** state capabilities? Please choose one option per countermeasure:

[All 20 countermeasures]

1. **Limit connectivity:** Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.
2. **IoT-free contingency plans:** Push for media stakeholders (e.g. news organisations) to create emergency/contingency plans that do not involve Internet of Things devices. These plans should acknowledge the risks associated with reliance on such devices to, for example, keep track of correspondents in dangerous environments.

3. **Transparency reporting:** Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices about device purchasing and can warn their sources about these devices.
4. **Travelling without local storage:** Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control.
5. **Network segmentation:** Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices.
6. **Aesthetic disguises:** Consider employing some methods of hiding one's face in ambient settings, through make-up, masks, clothing choices, etc.
7. **Audio obfuscation:** White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.
8. **Patching:** Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.
9. **Stronger passwords:** Internet of Things devices should not have default passwords (this is both an individual responsibility to change passwords upon purchase of a device, and also a necessary legislative shift to make sure that devices all have distinct default passwords).
10. **Wi-Fi security:** Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.
11. **Collaborative technology design:** News organisations and media-related civil society organisations could fund and collaborate with cyber security researchers and designers on the creation of cutting-edge intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become mandatory within press institutions.
12. **Firewalls:** If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.
13. **Physically cover cameras:** Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.
14. **Block the signal:** Faraday bags can be used to transport devices or temporarily block Internet of Things device capabilities.
15. **Research device security:** As with smartphones, if an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. If an individual member of the press must frequently use or be in spaces where Internet of Things devices exist, they should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.
16. **Intelligence sharing:** Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts,

etc.). Their goal is to share information on topics from best practices to threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.

17. **Top-down education:** Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.
18. **IoT-specific risk assessments:** Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.
19. **Legal scrutiny:** There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.
20. **No clear countermeasure yet:** Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.

- Scale of realism:
    - 5 Totally realistic/this is already being effectively implemented by some people
    - 4 Somewhat realistic/this is likely to be already in the process of development
    - 3 Not sure/don't know
    - 2 This is somewhat possible
    - 1 This is not at all likely

Page 13: Likert matrix of countermeasures x scale of future realism

- Could these countermeasures realistically be **usefully** implemented, given your anticipation of **future** state capabilities? Please choose one option per countermeasure:

[All 20 countermeasures]

1. **Limit connectivity:** Minimise interaction with Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Rely primarily on analogue methods of journalism, e.g. pen and paper.
2. **IoT-free contingency plans:** Push for media stakeholders (e.g. news organisations) to create emergency/contingency plans that do not involve Internet of Things devices. These plans should acknowledge the risks associated with reliance on such devices to, for example, keep track of correspondents in dangerous environments.
3. **Transparency reporting:** Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices about device purchasing and can warn their sources about these devices.
4. **Travelling without local storage:** Ensure that travelling members of the press back up the information stored in their devices, including portable Internet of Things devices to their cloud service before they travel. They should delete the information from the local storage on all their devices, as well as logging out of the cloud. They would then have to re-download their work when past border control.

5. **Network segmentation:** Make sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. Use VLANs and firewalls, as well as air-gapping critical devices.
6. **Aesthetic disguises:** Consider employing some methods of hiding one's face in ambient settings, through make-up, masks, clothing choices, etc.
7. **Audio obfuscation:** White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.
8. **Patching:** Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.
9. **Stronger passwords:** Internet of Things devices should not have default passwords (this is both an individual responsibility to change passwords upon purchase of a device, and also a necessary legislative shift to make sure that devices all have distinct default passwords).
10. **Wi-Fi security:** Secure/configure Wi-Fi network security. Physically cover authentication details on devices, e.g. routers. Use a Virtual Private Network.
11. **Collaborative technology design:** News organisations and media-related civil society organisations could fund and collaborate with cyber security researchers and designers on the creation of cutting-edge intrusion prevention and anti-malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become mandatory within press institutions.
12. **Firewalls:** If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.
13. **Physically cover cameras:** Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.
14. **Block the signal:** Faraday bags can be used to transport devices or temporarily block Internet of Things device capabilities.
15. **Research device security:** As with smartphones, if an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently optimal security. If an individual member of the press must frequently use or be in spaces where Internet of Things devices exist, they should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.
16. **Intelligence sharing:** Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). Their goal is to share information on topics from best practices to threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.
17. **Top-down education:** Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.
18. **IoT-specific risk assessments:** Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.

19. **Legal scrutiny:** There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legitimate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc.
20. **No clear countermeasure yet:** Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. For these, it is important that journalists report as much as possible about these problems, so that other members of the press and the public become aware of and potentially address these issues. This is especially relevant to threats relating to a domestic democratic government's activities.

- Scale of realism:
    - 5 Totally realistic/this is already being implemented
    - 4 Somewhat realistic/this could be implemented
    - 3 Not sure/don't know
    - 2 This is somewhat possible
    - 1 This is not at all likely

Page 14: Additional optional questions

- [OPTIONAL] Do you have any additional comments or feedback regarding the threats and countermeasures discussed in this survey? (e.g. any missing threats or countermeasures) *[text answer]*

Page 15: Thank you!

Thank you for your involvement in this survey! If you have any questions about the research or how your responses will be used, please contact the researcher Anjuli Shere at anjuli.shere@cybersecurity.ox.ac.uk

Appendix L: Framework (static version)

Dynamic framework hosted at:
https://docs.google.com/spreadsheets/d/1PvE1rtYN4_6BvAf5TgVkWnTHElKU81AfWM8E6L0bmEU/edit#gid=986461345

#	Countermeasures (Protections & Mitigations)	Disadvantages to each countermeasure
A	**Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.**	• Relies on ability to opt-out of interaction with the IoT • Resource-intensive and time consuming • Increases likelihood of successful physical theft of information • Device functionality and so benefits of the IoT will be lost when the countermeasure is in force
B	**IoT-free contingency plans: Encourage media stakeholders (e.g. news organisations) to ensure that their emergency/contingency plans do not rely on Internet of Things devices.**	• Relies on people obeying the law • Difficulty enforcing for all necessary users • Ad hoc solution that requires training for sustained use • Long-term goal
C	**Transparency reporting: Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices and can warn their sources. This countermeasure could also include news organisations reporting on these lists so that their audiences, including their sources, can also make informed decisions.**	• Resource-intensive and time consuming • Increased information available for attackers about which companies hold specific data types
D	**Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).**	• Device functionality and so benefits of the IoT will be lost when the countermeasure is in force • Not possible for every type of IoT device • Requires technical skills
E	**Aesthetic disguises: Consider employing some methods of hiding one's face to protect against video-equipped devices in public spaces. For example, this can be done through make-up, masks, and/or clothing choices. If this is done, consider other ways of verifying one's identity when meeting with sources.**	• Resource-intensive and time consuming • Works against (some) machines, but unlikely to slip past human analysts

F	**Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.**	• Under-researched technology, not proven to work
G	**Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.**	• Resource-intensive and time consuming • Not possible for every type of IoT device
H	**Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.**	• Not possible for every type of IoT device • More passwords for individuals to manage
I	**Collaborative technology design: News organisations and media-related civil society organisations could collaborate with cyber security researchers and designers on the creation of cutting-edge, open and transparent standards for IoT protection. For example, developing intrusion prevention and an - malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become adopted within press institutions.**	• Resource-intensive and time consuming • Companies are only beginning to provide this service
J	**Firewalls: If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.**	• Geofencing is generally considered weak protection against attacks launched via proxy • Requires technical skills • You cannot know all the scanners/websites that are indexing your devices
K	**Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.**	• Not possible for every type of IoT device • Not possible for bystanders

L	**Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).**	• Not possible for bystanders
M	**Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently op mal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.**	• Resource-intensive and time consuming
N	**Intelligence sharing: Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). These groups can share information on topics including best practices and threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.**	• Resource-intensive and time consuming • Long-term goal
O	**Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.**	• Long-term goal
P	**IoT-specific risk assessments: Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.**	• Resource-intensive and time consuming • Risk assessments are administrative burdens
Q	**Legal scrutiny in favour of press freedom: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legi mate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc. A motivating factor behind the**	• Long-term goal

	scrutiny should be the risk posed by these clauses to press freedom.	
R	**No clear IoT-specific countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. With no specific countermeasure, it may be hard to target threats and mitigate them. However, it is important that journalists draw attention to these threats as much as possible, so that there is a sense of urgency to address them.**	1. n/a

Table 19: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), and 3 (disadvantages of countermeasure)

#	Countermeasures (Protections & Mitigations)	Threats addressed by each countermeasure
A	**Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.**	• Warrantless bulk data purchase • Abusing health and biometric information • Third party supply chain actors accessing data • Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Informal additions to state surveillance networks • Data manipulation as a result of consent requirements • Sensor-level attacks on data confidentiality or integrity • Predictive analysis of location data to facilitate physical attacks • Continuous surveillance • Weaponisation of financial penalties • Hijacking connected social media and communications accounts • Botnet creation • Denial of Service attacks • Manipulation of devices' physical activities • Data harvesting from decommissioned devices • Altering user-facing device and data attributes • Voice stealing

B	**IoT-free contingency plans: Encourage media stakeholders (e.g. news organisations) to ensure that their emergency/contingency plans do not rely on Internet of Things devices.**	• Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Informal additions to state surveillance networks • Sensor-level attacks on data confidentiality or integrity • Predictive analysis of location data to facilitate physical attacks • Weaponisation of financial penalties • Botnet creation • Manipulation of devices' physical activities • Altering user-facing device and data attributes
C	**Transparency reporting: Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices and can warn their sources. This countermeasure could also include news organisations reporting on these lists so that their audiences, including their sources, can also make informed decisions.**	• Warrantless bulk data purchase • Abuse of data and privacy laws • Informal additions to state surveillance networks
D	**Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).**	• Third party supply chain actors accessing data • SOCMINT and IoT interrogation by law enforcement • Sensor-level attacks on data confidentiality or integrity • Continuous surveillance • Botnet creation
E	**Aesthetic disguises: Consider employing some methods of hiding one's face to protect against video-equipped devices in public spaces. For example, this can be done through make-up, masks, and/or clothing choices. If this is done, consider other ways of verifying one's identity when meeting with sources.**	• Data linkage and aggregation • Informal additions to state surveillance networks
F	**Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.**	• Informal additions to state surveillance networks • Continuous surveillance
G	**Patching: Automatically install updates for Internet of Things devices. Remain aware of**	• SOCMINT and IoT interrogation by law enforcement

	when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.	• Data linkage and aggregation • Informal additions to state surveillance networks • Data manipulation as a result of consent requirements • Sensor-level attacks on data confidentiality or integrity • Continuous surveillance • Weaponisation of financial penalties • Hijacking connected social media and communications accounts • Botnet creation • Denial of Service attacks • Manipulation of devices' physical activities • Altering user-facing device and data attributes
H	**Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.**	• Abusing health and biometric information • SOCMINT and IoT interrogation by law enforcement • Informal additions to state surveillance networks • Sensor-level attacks on data confidentiality or integrity • Predictive analysis of location data to facilitate physical attacks • Continuous surveillance • Weaponisation of financial penalties • Botnet creation • Manipulation of devices' physical activities • Altering user-facing device and data attributes
I	**Collaborative technology design: News organisations and media-related civil society organisations could collaborate with cyber security researchers and designers on the creation of cutting-edge, open and transparent standards for IoT protection. For example, developing intrusion prevention and an - malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become adopted within press institutions.**	• Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Sensor-level attacks on data confidentiality or integrity • Weaponisation of financial penalties • Botnet creation • Denial of Service attacks • Manipulation of devices' physical activities

J	**Firewalls: If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.**	• Data linkage and aggregation • Informal additions to state surveillance networks • Sensor-level attacks on data confidentiality or integrity • Predictive analysis of location data to facilitate physical attacks • Weaponisation of financial penalties • Denial of Service attacks
K	**Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.**	• Informal additions to state surveillance networks • Continuous surveillance
L	**Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).**	• Third party supply chain actors accessing data • Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Predictive analysis of location data to facilitate physical attacks • Continuous surveillance • Botnet creation
M	**Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently op mal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.**	• SOCMINT and IoT interrogation by law enforcement • Sensor-level attacks on data confidentiality or integrity
N	**Intelligence sharing: Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). These groups can share information on topics including best practices and threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.**	• Warrantless bulk data purchase • Abusing health and biometric information • Third party supply chain actors accessing data • Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Informal additions to state surveillance networks

		• Data manipulation as a result of consent requirements • Sensor-level attacks on data confidentiality or integrity • Predictive analysis of location data to facilitate physical attacks • Continuous surveillance • Weaponisation of financial penalties • Hijacking connected social media and communications accounts • Botnet creation • Denial of Service attacks • Manipulation of devices' physical activities • Data harvesting from decommissioned devices • Altering user-facing device and data attributes • Voice stealing
O	**Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.**	• Warrantless bulk data purchase • Abusing health and biometric information • Third party supply chain actors accessing data • Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Informal additions to state surveillance networks • Data manipulation as a result of consent requirements • Sensor-level attacks on data confidentiality or integrity • Predictive analysis of location data to facilitate physical attacks • Continuous surveillance • Weaponisation of financial penalties • Hijacking connected social media and communications accounts • Botnet creation • Denial of Service attacks • Manipulation of devices' physical activities • Data harvesting from decommissioned devices

		• Altering user-facing device and data attributes • Voice stealing
P	**IoT-specific risk assessments: Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.**	• Warrantless bulk data purchase • Abusing health and biometric information • Third party supply chain actors accessing data • Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Informal additions to state surveillance networks • Data manipulation as a result of consent requirements • Sensor-level attacks on data confidentiality or integrity • Predictive analysis of location data to facilitate physical attacks • Continuous surveillance • Weaponisation of financial penalties • Hijacking connected social media and communications accounts • Botnet creation • Denial of Service attacks • Manipulation of devices' physical activities • Data harvesting from decommissioned devices • Altering user-facing device and data attributes • Voice stealing
Q	**Legal scrutiny in favour of press freedom: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legi mate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc. A motivating factor behind the scrutiny should be the risk posed by these clauses to press freedom.**	• Warrantless bulk data purchase • Abuse of data and privacy laws • SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Informal additions to state surveillance networks • Predictive analysis of location data to facilitate physical attacks
R	**No clear IoT-specific countermeasure yet: Some Internet of Things threats do not yet have clear**	• Warrantless bulk data purchase • Abuse of data and privacy laws

	protections or mitigative countermeasures. With no specific countermeasure, it may be hard to target threats and mitigate them. However, it is important that journalists draw attention to these threats as much as possible, so that there is a sense of urgency to address them.	• SOCMINT and IoT interrogation by law enforcement • Data linkage and aggregation • Informal additions to state surveillance networks

Table 20: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), and 4 (threats addressed by each countermeasure)

#	Countermeasures (Protections & Mitigations)	How is it estimated that this protection will best help against a given threat? (i.e. function of countermeasure)	Beneficiary (i.e. Is the countermeasure intended to most help an individual, a news organisation as a business, or the news media existentially?)
A	**Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.**	Prevention (PREV)	Individual members of the press and their sources
B	**IoT-free contingency plans: Encourage media stakeholders (e.g. news organisations) to ensure that their emergency/contingency plans do not rely on Internet of Things devices.**	Response (RESP)	News organisations as businesses
C	**Transparency reporting: Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices and can warn their sources. This countermeasure could also include news organisations reporting on these lists so that their audiences, including their sources, can also make informed decisions.**	Prevention (PREV)	The future of the news media existentially
D	**Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and**	Compartmentalization (COMP)	News organisations as businesses

	firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).		
E	**Aesthetic disguises: Consider employing some methods of hiding one's face to protect against video-equipped devices in public spaces. For example, this can be done through make-up, masks, and/or clothing choices. If this is done, consider other ways of verifying one's identity when meeting with sources.**	Deception (DECEP)	Individual members of the press and their sources
F	**Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.**	Deception (DECEP)	Individual members of the press and their sources
G	**Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.**	Prevention (PREV)	News organisations as businesses
H	**Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.**	Prevention (PREV)	News organisations as businesses
I	**Collaborative technology design: News organisations and media-related civil society organisations could collaborate with cyber security researchers and designers on the creation of cutting-edge, open and transparent standards for IoT protection. For example, developing intrusion prevention and an -malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become adopted within press institutions.**	Layering (LAYER)	The future of the news media existentially
J	**Firewalls: If a journalist or their colleagues tend to be targeted by malicious actors**	Perimeter defense (PERI)	Individual members of the

	based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.		press and their sources
K	**Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.**	Prevention (PREV)	Individual members of the press and their sources
L	**Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).**	Prevention (PREV)	Individual members of the press and their sources
M	**Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently op mal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.**	Surveillance (SURV) Layering (LAYER) Perimeter defense (PERI) Prevention (PREV)	News organisations as businesses
N	**Intelligence sharing: Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). These groups can share information on topics including best practices and threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.**	Response (RESP)	The future of the news media existentially

O	**Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.**	Prevention (PREV)	The future of the news media existentially
P	**IoT-specific risk assessments: Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.**	Surveillance (SURV) Prevention (PREV) Response (RESP) Layering (LAYER)	News organisations as businesses
Q	**Legal scrutiny in favour of press freedom: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legi mate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc. A motivating factor behind the scrutiny should be the risk posed by these clauses to press freedom.**	Layering (LAYER)	The future of the news media existentially
R	**No clear IoT-specific countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. With no specific countermeasure, it may be hard to target threats and mitigate them. However, it is important that journalists draw attention to these threats as much as possible, so that there is a sense of urgency to address them.**	Prevention (PREV)	n/a

Table 21: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), 5 (function of countermeasure), and 6 (beneficiaries of countermeasure)

#	Countermeasures (Protections & Mitigations)	Phase(s) of the editorial workflow to which this countermeasure is most relevant	Media roles that are most likely to be responsible for implementation of this countermeasure
A	**Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect**	Stage 2: Deploy, Gather, Acquire, Create	Editorial/Narrative Producers (inc. Programme

	wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or voice recorders that do not connect to the internet.		
B	**IoT-free contingency plans: Encourage media stakeholders (e.g. news organisations) to ensure that their emergency/contingency plans do not rely on Internet of Things devices.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Business/Corporate/Commercial/Organisation
C	**Transparency reporting: Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices and can warn their sources. This countermeasure could also include news organisations reporting on these lists so that their audiences, including their sources, can also make informed decisions.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Editorial/Narrative Producers (inc. Programme
D	**Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel Business/Corporate/Commercial/Organisation Technological Editorial Contributors
E	**Aesthetic disguises: Consider employing some methods of hiding one's face to protect against video-equipped devices in public spaces. For example, this can be**	Stage 2: Deploy, Gather, Acquire, Create	Editorial/Narrative Producers (inc. Programme

	done through make-up, masks, and/or clothing choices. If this is done, consider other ways of verifying one's identity when meeting with sources.		
F	**Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.**	Stage 2: Deploy, Gather, Acquire, Create	Editorial/Narrative Producers (inc. Programme
G	**Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel
H	**Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also be resolved by a legislative shift to make sure that devices all have distinct default passwords.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Editorial/Narrative Producers (inc. Programme Technological Editorial Contributors
I	**Collaborative technology design: News organisations and media-related civil society organisations could collaborate with cyber security researchers and designers on the creation of cutting-edge, open and transparent standards for IoT protection. For example, developing intrusion prevention and an -malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel

	created could then become adopted within press institutions.		
J	**Firewalls: If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel
K	**Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Editorial/Narrative Producers (inc. Programme
L	**Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Editorial/Narrative Producers (inc. Programme
M	**Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create	Risk Management Personnel Business/Corporate/Commercial/Organisation

	consistently op mal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.	Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	
N	**Intelligence sharing: Set up peer-to-peer information exchange groups across the media industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). These groups can share information on topics including best practices and threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Editorial/Narrative Producers (inc. Programme
O	**Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel
P	**IoT-specific risk assessments: Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Risk Management Personnel

Q	**Legal scrutiny in favour of press freedom: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legi mate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc. A motivating factor behind the scrutiny should be the risk posed by these clauses to press freedom.**	Stage 1: Pitch/Propose, Research, Plan, Develop Script Stage 2: Deploy, Gather, Acquire, Create Stage 3: Script Revisions, Assemble, Edit, Review Stage 4: Publish, Distribute, Curate Stage 5: Archive, Report, Legal Review, Complaints, Re-Use	Business/Corporate/Commercial/Organisation
R	**No clear IoT-specific countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. With no specific countermeasure, it may be hard to target threats and mitigate them. However, it is important that journalists draw attention to these threats as much as possible, so that there is a sense of urgency to address them.**	n/a	n/a

Table 22: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), 7 (editorial workflow phases to which countermeasure is most relevant), and 8 (media roles most likely to be responsible for implementation of countermeasure)

#	Countermeasures (Protections & Mitigations)	Feasibility of implementation of the countermeasure [Categories: 1. "quick win" (i.e. controls that can be swiftly implemented), 2. "mid-term effort" (i.e. takes months), 3. "long-term effort" (i.e. this work is unlikely to ever be finished), 4. "collective win" (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat), 5. "unicorn" (i.e. unlikely to be worth time and effort in most circumstances).]
A	**Limit connectivity: Minimise exposure to Internet of Things devices to limit their collection of data. Never connect wearable Internet of Things devices to public Wi-Fi networks. Where possible, use analogue methods of journalism, e.g. pen and paper, or**	1. "quick win" (i.e. controls that can be swiftly implemented)

	voice recorders that do not connect to the internet.	
B	**IoT-free contingency plans: Encourage media stakeholders (e.g. news organisations) to ensure that their emergency/contingency plans do not rely on Internet of Things devices.**	2. “mid-term effort” (i.e. takes weeks to months)
C	**Transparency reporting: Lobby governments to publish lists of companies that have provided data to government and related agencies so that consumers, including members of the press, can make informed choices and can warn their sources. This countermeasure could also include news organisations reporting on these lists so that their audiences, including their sources, can also make informed decisions.**	4. “collective win” (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat)
D	**Network Security: This primarily involves making sure that Internet of Things devices are not connected to the same Wi-Fi network as other devices. To connect these devices to the internet, VPNs, VLANs and firewalls should be employed. It also includes physically covering authentication details on devices, e.g. routers. Where possible, critical devices should be airgapped (i.e. not connected to any networks).**	2. “mid-term effort” (i.e. takes weeks to months)
E	**Aesthetic disguises: Consider employing some methods of hiding one’s face to protect against video-equipped devices in public spaces. For example, this can be done through make-up, masks, and/or clothing choices. If this is done, consider other ways of verifying one’s identity when meeting with sources.**	5. “unicorn” (i.e. unlikely to be worth time and effort in most circumstances)
F	**Audio obfuscation: White noise emitters and audio jammers may be used to prevent audio recordings by Internet of Things devices, even in public outdoor spaces.**	2. “mid-term effort” (i.e. takes weeks to months)
G	**Patching: Automatically install updates for Internet of Things devices. Remain aware of when manufacturers plan to stop releasing patches, as this will signal a likely increase in device vulnerabilities.**	2. “mid-term effort” (i.e. takes weeks to months)
H	**Create stronger passwords: Internet of Things devices should not have default passwords. Users should ensure passwords are changed on Internet of Things devices when purchased to avoid risks of default passwords. This would also**	1. “quick win” (i.e. controls that can be swiftly implemented)

	be resolved by a legislative shift to make sure that devices all have distinct default passwords.	
I	**Collaborative technology design: News organisations and media-related civil society organisations could collaborate with cyber security researchers and designers on the creation of cutting-edge, open and transparent standards for IoT protection. For example, developing intrusion prevention and an - malware systems for the Internet of Things, e.g. digital tripwires that detect threats coming into the network. The deployment of any tools created could then become adopted within press institutions.**	4. "collective win" (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat)
J	**Firewalls: If a journalist or their colleagues tend to be targeted by malicious actors based in specific countries, configure firewalls to include GeoIP filters which block incoming traffic from certain countries from accessing an individual's devices and their information. Set up host definitions in a firewall to filter for scanners belonging to search engines (e.g. Shodan) that index vulnerable Internet of Things devices. Create a firewall rule to block this list. This should block these scanners from being able to index machines.**	2. "mid-term effort" (i.e. takes weeks to months)
K	**Physically cover cameras: Any Internet of Things devices that intermittently use a camera should have a removable cover placed over the camera, to prevent this from being used to monitor anyone within the field of vision of the device.**	1. "quick win" (i.e. controls that can be swiftly implemented)
L	**Block the signal: Carry and use Faraday bags (i.e. pouches that shield anything inside from external electromagnetic radiation, which temporarily blocks Internet of Things device capabilities).**	1. "quick win" (i.e. controls that can be swiftly implemented)
M	**Corporate maintenance of device security: If an Internet of Things device is deemed essential by corporate IT, it should be purchased and maintained by the news organisation, to ensure consistently op mal security. They should research communications protocols and vulnerabilities of these devices, and should attempt to change or remove these devices as soon as public vulnerabilities become known.**	3. "long-term effort" (i.e. this work is unlikely to ever be finished)
N	**Intelligence sharing: Set up peer-to-peer information exchange groups across the media**	4. "collective win" (i.e. collective actions such as lobbying for policy

	industry, both within and across different roles (of journalists, media lawyers, security experts, etc.). These groups can share information on topics including best practices and threat intelligence, which would establish a minimum standard of education and awareness of emerging Internet of Things threats.	changes that would remove or comprehensively alter a specified threat)
O	**Top-down education: Ensure that news organisations, professional unions, and civil society organisations who assist journalists keep up-to-date on Internet of Things devices threats and potential protection strategies. They must effectively communicate this information to both the press and the public, to raise awareness and influence individual security behaviours.**	4. “collective win” (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat)
P	**IoT-specific risk assessments: Internet of Things devices should be included in all risk assessments and risk management strategies, not simply as assets but also as potential threats.**	3. “long-term effort” (i.e. this work is unlikely to ever be finished)
Q	**Legal scrutiny in favour of press freedom: There should be more legal, political and media (including international) scrutiny of outdated or ambiguous legal clauses that enable exploitation of Internet of Things capabilities, e.g. in 'technology-neutral' or surveillance-focused laws. These can include legi mate interest clauses that allow access to data, data retention laws that are vague about what constitutes metadata, etc. A motivating factor behind the scrutiny should be the risk posed by these clauses to press freedom.**	4. “collective win” (i.e. collective actions such as lobbying for policy changes that would remove or comprehensively alter a specified threat)
R	**No clear IoT-specific countermeasure yet: Some Internet of Things threats do not yet have clear protections or mitigative countermeasures. With no specific countermeasure, it may be hard to target threats and mitigate them. However, it is important that journalists draw attention to these threats as much as possible, so that there is a sense of urgency to address them.**	3. “long-term effort” (i.e. this work is unlikely to ever be finished)

Table 23: Table showing columns 1 (countermeasure identifier), 2 (countermeasure), and 9 (feasibility of implementation of the countermeasure)

Bibliography

Abdi N, Ramokapane KM and Such JM (2019) More than smart speakers: security and privacy perceptions of smart home personal assistants. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, USA, 12 August 2019, pp. 451–466. SOUPS'19. USENIX Association.

Abrams KM, Wang Z, Song YJ, et al. (2015) Data Richness Trade-Offs Between Face-to-Face, Online Audiovisual, and Online Text-Only Focus Groups. *Social Science Computer Review* 33(1). SAGE Publications Inc: 80–96. DOI: 10.1177/0894439313519733.

Abramson K (2014) TURNING UP THE LIGHTS ON GASLIGHTING. *Philosophical Perspectives* 28. [Ridgeview Publishing Company, Wiley]: 1–30.

Access Now (2018) *A first look at digital security digital as of March 2018*. March. Access Now. Available at: https://www.accessnow.org/cms/assets/uploads/2018/03/A-first-look-at-digital-security-digital-copy.pdf (accessed 9 September 2019).

Access Now (2020) New world disorder: digital attacks on freedom of assembly. In: *Access Now*. Available at: https://www.accessnow.org/new-world-disorder-digital-attacks-on-freedom-of-assembly/ (accessed 11 September 2020).

Ackerman S (2012) CIA Chief: We'll Spy on You Through Your Dishwasher. *Wired*, 15 March. Available at: https://www.wired.com/2012/03/petraeus-tv-remote/ (accessed 9 September 2019).

Ackerman S and Thielman S (2016) US intelligence chief: we might use the internet of things to spy on you. *The Guardian*, 9 February. Available at: https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper (accessed 26 October 2020).

Agence France-Presse (AFP) (2014) Hackers use 'smart' refrigerator to send 750,000 virus-laced emails. *Raw Story*, 17 January. Available at: https://www.rawstory.com/2014/01/hackers-use-smart-refrigerator-to-send-750000-virus-laced-emails/ (accessed 23 October 2020).

Agrafiotis I, Nurse JRC, Goldsmith M, et al. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1). Oxford Academic. DOI: 10.1093/cybsec/tyy006.

Ahmad A, Maynard SB and Park S (2014) Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing* 25(2): 357–370. DOI: 10.1007/s10845-012-0683-0.

Ahmad I, Akter T, Buher Z, et al. (2022) Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW2): 364:1-364:31. DOI: 10.1145/3555089.

Aksu H, Babun L, Conti M, et al. (2018) Advertising in the IoT Era: Vision and Challenges. *arXiv:1802.04102 [cs]*. Available at: http://arxiv.org/abs/1802.04102 (accessed 11 September 2020).

Aktypi A, Nurse JRC and Goldsmith M (2017) Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In: *Proceedings of the 2017 on Multimedia Privacy and Security*, New York, NY, USA, 2017, pp. 1–11. MPS '17. ACM. DOI: 10.1145/3137616.3137617.

Alkhabbas F, Spalazzese R and Davidsson P (2019) Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. *Internet of Things* 7: 100084. DOI: 10.1016/j.iot.2019.100084.

Alladi T, Chamola V, Sikdar B, et al. (2020) Consumer IoT: Security Vulnerability Case Studies and Solutions. *IEEE Consumer Electronics Magazine* 9(2): 17–25. DOI: 10.1109/MCE.2019.2953740.

Allam S (2018) An Exploratory Survey of Hadoop Log Analysis Tools. *International Journal of Creative Research Thoughts* 6(3): 801–804.

Alliance for Journalists' Freedom (2019) *White Paper: Press Freedom in Australia*. May. Queensland, Australia: Alliance for Journalists' Freedom. Available at: https://www.journalistsfreedom.com/wp-content/uploads/2019/06/AJF-Press-Freedom-In-Australia-2019.pdf (accessed 31 December 2020).

Alqhatani A and Lipford HR (2019) 'There is nothing that i need to keep secret': sharing practices and concerns of wearable fitness data. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, USA, 12 August 2019, pp. 421–434. SOUPS'19. USENIX Association.

Alrawi O, Lever C, Antonakakis M, et al. (2019) SoK: Security Evaluation of Home-Based IoT Deployments. In: *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 1362–1380. IEEE. DOI: 10.1109/SP.2019.00013.

Ambrose D (2019) The Erosion of Democracy: Can We Muster Enough Wisdom to Stop It? In: Sternberg RJ, Nusbaum HC, and Glück J (eds) *Applying Wisdom to Contemporary World Problems*. Cham: Palgrave Macmillan, pp. 21–50. DOI: 10.1007/978-3-030-20287-3_2.

Anderson D (2015) *A question of trust: report of the investigatory powers review*. London: HM Government. Available at: https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review (accessed 3 March 2020).

Ando R, Shima S and Takemura T (2016) Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment. *IEICE TRANSACTIONS on Information and Systems* E99-D(8). The Institute of Electronics, Information and Communication Engineers: 1974–1981.

Anell S, Grober L and Krombholz K (2020) End User and Expert Perceptions of Threats and Potential Countermeasures. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 10. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Anell.pdf.

Aratani L (2022) Concern as US media hit with wave of layoffs amid rise of disinformation. *The Guardian*, 10 December. Available at: https://www.theguardian.com/media/2022/dec/10/media-layoffs-cnn-buzzfeed-gannett-recount-protocol (accessed 7 February 2023).

Archibald MM, Ambagtsheer RC, Casey MG, et al. (2019) Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants. *International Journal of Qualitative Methods* 18. SAGE Publications Inc: 1609406919874596. DOI: 10.1177/1609406919874596.

Arroub A, Zahi B, Sabir E, et al. (2016) A literature review on Smart Cities: Paradigms, opportunities and open problems. In: *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, October 2016, pp. 180–186. DOI: 10.1109/WINCOM.2016.7777211.

Article 12 Right of access | Directive 95/46/EC - Data Protection Directive | Better Regulation (2018). Available at: https://service.betterregulation.com/document/198705 (accessed 21 April 2020).

Article 19 (2017) DOA for IoT at ITU-T Study Group 20: Dead on Arrival, or Return of the Living Dead? Available at: https://www.article19.org/resources/doa-for-iot-at-itu-t-study-group-20-dead-on-arrival-or-return-of-the-living-dead/ (accessed 9 September 2019).

Ashdown N and Shere ARK (2021) The Security Implications of Robotic Surveillance Pigeons – Sciences Po Cybersecurity Association. *The Sciences Po Cybersecurity Association's Academic Journal* 1(1). Available

at: https://scpo-cybersecurityassociation.com/index.php/2021/03/29/the-security-implications-of-robotic-surveillance-pigeons/ (accessed 27 September 2022).
Ashton K (2009) That 'Internet of Things' Thing. *RFID Journal*. Available at: https://www.rfidjournal.com/that-internet-of-things-thing (accessed 8 February 2020).
Aspinwall N (2019) Taiwan Shaken by Concerns Over Chinese Influence in Media, Press Freedom. Available at: https://thediplomat.com/2019/07/taiwan-shaken-by-concerns-over-chinese-influence-in-media-press-freedom/ (accessed 31 December 2020).
Association for Computing Machinery (ACM) (2020) ACM Proceedings Digital Library. Available at: https://dl.acm.org/proceedings (accessed 14 April 2020).
Atamli AW and Martin A (2014) Threat-Based Security Analysis for the Internet of Things. In: *2014 International Workshop on Secure Internet of Things*, September 2014, pp. 35–43. DOI: 10.1109/SIoT.2014.10.
Attfield S and Dowell J (2003) Information seeking and use by newspaper journalists. *Journal of Documentation* 59(2). MCB UP Ltd: 187–204. DOI: 10.1108/00220410310463860.
Austin L and Lie D (2021) Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust. *Surveillance & Society* 19(2): 255–261. DOI: 10.24908/ss.v19i2.14409.
Australia Desk (2019) Australian newspapers black out front pages in 'secrecy' protest. *BBC News*, 21 October. Available at: https://www.bbc.com/news/world-australia-50119559 (accessed 31 December 2020).
Australian Bureau of Statistics (2018a) Household use of information technology, 2016-17 financial year. Available at: https://www.abs.gov.au/statistics/industry/technology-and-innovation/household-use-information-technology/latest-release (accessed 31 December 2020).
Australian Bureau of Statistics (2018b) Internet Activity, Australia, June 2018. Available at: https://www.abs.gov.au/statistics/industry/technology-and-innovation/internet-activity-australia/latest-release (accessed 31 December 2020).
Australian Council of Professors and Heads of IS (2019) Australian Council of Professors and Heads of Information Systems (ACPHIS) Journal Ranking. Available at: https://www.acphis.org.au (accessed 14 April 2020).
Australian Cyber Security Centre and Australian Signals Directorate (2020) *Australian Government Information Security Manual (October 2020)*. October. Australia: Australian Signals Directorate. Available at: https://www.cyber.gov.au/sites/default/files/2020-10/Australian%20Government%20Information%20Security%20Manual%20%28October%202020%29.pdf (accessed 31 December 2020).
Australian Federal Police (2016) What We Do: Operational Support: Forensics. Available at: https://www.afp.gov.au/what-we-do/operational-support/forensics (accessed 31 December 2020).
Australian Government (2015) Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015. Attorney-General's Department. Available at: https://www.legislation.gov.au/Details/C2015A00039/Html/Text, http://www.legislation.gov.au/Details/C2015A00039 (accessed 26 February 2020).
Australian Government: Australian Law Reform Commission (2010) The number and scope of exemptions. Available at: https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/33-overview-exemptions-from-the-privacy-act/the-number-and-scope-of-exemptions/ (accessed 25 October 2022).

Australian Government Department of Foreign Affairs and Trade (2021) Australia-Taiwan relationship. Available at: https://www.dfat.gov.au/geo/taiwan/Pages/australia-taiwan-relationship (accessed 2 March 2021).

Australian Government: Office of the Australian Information Commissioner (2019) Freedom of information Guidelines: Part 5 — Exemptions. Available at: https://www.oaic.gov.au/freedom-of-information/foi-guidelines/part-5-exemptions (accessed 25 October 2022).

Australian Law Reform Commission (2014) A common law action for breach of privacy in Australia? Available at: https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/3-overview-of-current-law-2/a-common-law-action-for-breach-of-privacy-in-australia-2/ (accessed 31 December 2020).

Australian Right To Know (ARTK) (2020) Make and browse Freedom of Information (FOI) requests. Available at: https://www.righttoknow.org.au/ (accessed 31 December 2020).

Autry T (2019) *Secure IoT Compliance Behaviors Among Teleworkers*. D.I.T. Capella University, United States -- Minnesota. Available at: https://search.proquest.com/docview/2313671125/abstract/462C5E8E633348B0PQ/1 (accessed 27 February 2020).

Avilés JAG and Carvajal M (2008) Integrated and Cross-Media Newsroom Convergence: Two Models of Multimedia News Production — The Cases of Novotécnica and La Verdad Multimedia in Spain. *Convergence* 14(2). SAGE Publications Ltd: 221–239. DOI: 10.1177/1354856507087945.

Ayres RU (1993) Cowboys, cornucopians and long-run sustainability. *Ecological Economics* 8(3): 189–207. DOI: 10.1016/0921-8009(93)90058-E.

Baker J (2019) Rethinking Encryption. *Lawfare*, 22 October. Available at: https://www.lawfareblog.com/rethinking-encryption (accessed 31 December 2020).

Ball J (2015) GCHQ captured emails of journalists from top international media. *The Guardian*, 19 January. Available at: https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post (accessed 9 September 2019).

Ball K and Snider L (2013) *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. Routledge.

Banasiński C and Rojszczak M (2021) Cybersecurity of consumer products against the background of the EU model of cyberspace protection. *Journal of Cybersecurity* 7(tyab011). DOI: 10.1093/cybsec/tyab011.

Bandara W, Miskon S and Fielt E (2011) A systematic, tool-supported method for conducting literature reviews in information systems. In: *ECIS 2011 Proceedings* (eds M Rossi and J Nandhakumar), Brisbane, Australia, 2011, pp. 1–13. Queensland University of Technology. Available at: https://eprints.qut.edu.au/42184/1/42184c.pdf.

Barbosa NM, Zhang Z and Wang Y (2020) Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In: *Proceedings of the Sixteenth USENIX Symposium on Usable Privacy and Security*, Virtual, 9 August 2020, pp. 417–435. USENIX Association. Available at: https://www.usenix.org/conference/soups2020/presentation/barbosa (accessed 9 February 2021).

Barcena MB, Wueest C and Lau H (2014) *How safe is your quantified self?* Security Response, Whitepaper, 11 August. Symantec. Available at: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf.

Barlett L and Vavrus F (2016) *Rethinking Case Study Research : A Comparative Approach*. 1st ed. New York: Routledge. DOI: 10.4324/9781315674889.

Barrett B (2019) The Latest Julian Assange Indictment Is an Assault on Press Freedom. *Wired*, 23 May. Available at: https://www.wired.com/story/julian-assange-espionage-act-threaten-press-freedom/ (accessed 11 September 2020).

Barstow BA, Vice J, Bowman S, et al. (2019) Examining perceptions of existing and newly created accessibility symbols. *Disability and Health Journal* 12(2): 180–186. DOI: 10.1016/j.dhjo.2018.11.012.

Barth A, Datta A, Mitchell JC, et al. (2006) Privacy and contextual integrity: Framework and applications. In: *Proceedings - 2006 IEEE Symposium on Security and Privacy, S+P 2006*, 2006, pp. 184–198. DOI: 10.1109/SP.2006.32.

Bastians D (2021) For Sri Lankan reporters, the ghosts of violence and intimidation loom again. *The Guardian*, 4 March. Available at: http://www.theguardian.com/global-development/2021/mar/04/for-sri-lankan-reporters-the-ghosts-of-violence-and-intimidation-loom-again (accessed 5 March 2021).

Bazeley P (2009) Editorial: Integrating Data Analyses in Mixed Methods Research. *Journal of Mixed Methods Research* 3(3). SAGE Publications: 203–207. DOI: 10.1177/1558689809334443.

BBC News (2019a) Journalist's home raided over spying report. *BBC News*, 4 June. Available at: https://www.bbc.com/news/world-australia-48511217 (accessed 9 September 2019).

BBC News (2019b) Security gadgets 'making people more vulnerable'. Available at: https://www.bbc.com/news/av/uk-england-beds-bucks-herts-49801267/security-gadgets-making-people-more-vulnerable-from-hackers (accessed 4 March 2020).

Beaudoin D (2012) Serious Lessons from the Commercial Games Industry. In: Cruz-Cunha MM (ed.) *Handbook of Research on Serious Games as Educational, Business and Research Tools*. Michigan: IGI Global, pp. 272–278.

Becker S, Bryman A and Ferguson H (eds) (2012) *Understanding Research for Social Policy and Social Work*. 2nd Revised edition edition. Bristol: Policy Press.

Bellman C and van Oorschot PC (2020) Best Practices for IoT Security: What Does That Even Mean? *arXiv:2004.12179 [cs]*. Available at: http://arxiv.org/abs/2004.12179 (accessed 7 June 2021).

Ben-Daya M, Hassini E and Bahroun Z (2019) Internet of things and supply chain management: a literature review. *International Journal of Production Research* 57(15–16). Taylor & Francis: 4719–4742. DOI: 10.1080/00207543.2017.1402140.

Bendovschi A (2015) Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance* 28. 7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015, 7th ICFC 2015, 13-14 April 2015,Wadham College, Oxford University, United Kingdom: 24–31. DOI: 10.1016/S2212-5671(15)01077-1.

Benjakob O (2022) This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure - National Security & Cyber - Haaretz.com. *Haaretz*, 26 December. Available at: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000 (accessed 12 January 2023).

Bentham J (2012) *The Works of Jeremy Bentham, Vol. 4* (ed. J Bowring). RareBooksClub.com.

Berdan K (2021) *CLTC Report: An Evaluation of Online Security Guides for Journalists*. 20 January. California, USA: CLTC UC Berkeley Center for Long-Term Cybersecurity. Available at:

https://cltc.berkeley.edu/2021/01/20/cltc-report-an-evaluation-of-online-security-guides-for-journalists/ (accessed 1 March 2021).
Berger G (2018) Is There a Future for Journalism? *Journalism Practice* 12(8). Routledge: 939–953. DOI: 10.1080/17512786.2018.1516117.
Bergman R and Shane S (2019) The Case of the Bumbling Spy: A Watchdog Group Gets Him on Camera. *The New York Times*, 28 January. Available at: https://www.nytimes.com/2019/01/28/world/black-cube-nso-citizen-lab-intelligence.html (accessed 9 September 2019).
Bertino E (2016) Data Security and Privacy in the IoT. In: *Proceedings of the 19th International Conference on Extending Database Technology (EDBT 16)*, Bordeaux, France, 15 March 2016, p. 3. Series ISSN: 2367-2005. Open Proceedings. DOI: 10.5441/002/edbt.2016.02.
Besen SM and Verveer PL (2021) Section 230 and the Problem of Social Cost. *Journal of Law and Policy* 30: 68.
Bhartiya S (2017) Your smart fridge may kill you: The dark side of IoT. Available at: https://www.infoworld.com/article/3176673/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html (accessed 18 November 2020).
Binns A (2017) Fair game? Journalists' experiences of online abuse. *Journal of Applied Journalism & Media Studies* 6(2): 183–206. DOI: 10.1386/ajms.6.2.183_1.
Bischoff P (2020) Surveillance Camera Statistics: Which City has the Most CCTV Cameras? Available at: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (accessed 31 December 2020).
Black E (2001) *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. 1st ed. New York: Crown Publishers.
Blanchard T (2017) *Journalists in Distress: Assessing the Digital Viability of a Global Emergency Assistance Network*. The Digital Security of Journalists in Distress Report 3, 23 January. Toronto, Canada: Canadian Journalists For Free Expression. Available at: https://d3n8a8pro7vhmx.cloudfront.net/cjfe/pages/2913/attachments/original/1484964569/Report_3_-_The_Digital_Security_of_Journalists_in_Distress.pdf?1484964569 (accessed 11 January 2020).
Bloomberg Business Wire (2019) Electronic Manufacturing Services Industry Procurement Intelligence Report | Evolving Opportunities with Foxconn Electronics and PEGATRON in the Electronic Manufacturing Services Market. *Bloomberg*, 9 December. London. Available at: https://www.bloomberg.com/press-releases/2019-12-09/electronic-manufacturing-services-industry-procurement-intelligence-report-evolving-opportunities-with-foxconn-electronics-and (accessed 31 December 2020).
Blythe JM and Johnson SD (2019) A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*. DOI: 10.1057/s41284-019-00211-8.
Blythe JM, Sombatruang N and Johnson SD (2019) What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity* 5(1). DOI: 10.1093/cybsec/tyz005.
Bobric G-D (2020) STUDY REGARDING THE CYBER THREATS TO THE NATIONAL SECURITY. *BULETIN ŞTIINŢIFIC* 1(49): 18–25. DOI: 10.2478/bsaft-2020-0003.
Bourgeault I, Dingwall R and Vries R de (2010) *The SAGE Handbook of Qualitative Methods in Health Research*. London, UK: SAGE Publications Ltd.

Bowcott O (2016) Terrorism Act incompatible with human rights, court rules in David Miranda case. Available at: https://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case (accessed 31 December 2020).

Bowcott O (2019) 'Bulk hacking' by UK spy agencies is illegal, high court told. Available at: http://www.theguardian.com/technology/2019/jun/17/liberty-mounts-latest-court-challenge-to-snoopers-charter-mi5-gchq (accessed 31 December 2020).

Bowling NA, Huang JL, Brower CK, et al. (2021) The Quick and the Careless: The Construct Validity of Page Time as a Measure of Insufficient Effort Responding to Surveys. *Organizational Research Methods*. SAGE Publications Inc: 10944281211056520. DOI: 10.1177/10944281211056520.

Bradshaw P (2014) Why every journalist should have a threat model (with cats). In: *Online Journalism Blog*. Available at: https://onlinejournalismblog.com/2014/07/16/why-every-journalist-should-have-a-threat-model-with-cats/ (accessed 11 September 2020).

Branch P (2015) How will data retention laws cope with the Internet of Things? Available at: http://theconversation.com/how-will-data-retention-laws-cope-with-the-internet-of-things-36885 (accessed 26 February 2020).

Brandom R (2018) GDPR launches today. Here's what you need to know. Available at: https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice (accessed 21 April 2020).

Braue D (2020) Mathematically-secure Australian seL4 microkernel gains global boost. Available at: https://www.csoonline.com/article/3537589/mathematically-secure-australian-sel4-microkernel-gains-global-boost.html (accessed 31 December 2020).

Braun T, Fung BCM, Iqbal F, et al. (2018) Security and privacy challenges in smart cities. *Sustainable Cities and Society* 39: 499–507. DOI: 10.1016/j.scs.2018.02.039.

Braun V and Clarke V (2013) *Successful Qualitative Research: A Practical Guide for Beginners*. London, UK: SAGE Publications Ltd.

Braun V, Clarke V, Boulton E, et al. (2021) The online survey as a qualitative research tool. *International Journal of Social Research Methodology* 24(6). Routledge: 641–654. DOI: 10.1080/13645579.2020.1805550.

Brevini B (2017) Metadata Laws, Journalism and Resistance in Australia. *Media and Communication* 5(1). 1: 76–83. DOI: 10.17645/mac.v5i1.810.

Brewster T (2020) Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's 'Private' Web And Phone Use. Available at: https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/ (accessed 31 December 2020).

Brinkerhoff DW and Crosby B (2002) *Managing Policy Reform: Concepts and Tools for Decision-Makers in Developing and Transitioning Countries*. United States of America: Kumarian Press.

Brown D (2020) A Review of the PubMed PICO Tool: Using Evidence-Based Practice in Health Education. *Health Promotion Practice* 21(4): 496–498. DOI: 10.1177/1524839919893361.

Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, Massachusetts: The MIT Press.

Brunton F and Nissenbaum H (2019) The Fantasy of Opting Out. In: *The MIT Press Reader*. Available at: https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/ (accessed 9 November 2019).

Bryans JW (2017) The Internet of Automotive Things: vulnerabilities, risks and policy implications. *Journal of Cyber Policy* 2(2). Routledge: 185–194. DOI: 10.1080/23738871.2017.1360926.

Brysk A (2020) Constructing rights in Taiwan: the feminist factor, democratization, and the quest for global citizenship. *The Pacific Review* 0(0). Routledge: 1–33. DOI: 10.1080/09512748.2020.1784985.

Bugeja J (2021) *On Privacy and Security in Smart Connected Homes: Malmö University, Studies in Computer Science No 14*. Doctoral Dissertation. Malmö University, Malmö, Sweden. Available at: https://mau.diva-portal.org/smash/get/diva2:1520701/SUMMARY01.pdf (accessed 18 February 2021).

Bugeja Joseph, Jacobsson A and Davidsson P (2018) An Empirical Analysis of Smart Connected Home Data. In: *Internet of Things – ICIOT 2018* (eds D Georgakopoulos and L-J Zhang), Cham, 2018, pp. 134–149. Lecture Notes in Computer Science. Springer International Publishing. DOI: 10.1007/978-3-319-94370-1_10.

Bugeja J., Jönsson D and Jacobsson A (2018) An Investigation of Vulnerabilities in Smart Connected Cameras. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, March 2018, pp. 537–542. IEEE. DOI: 10.1109/PERCOMW.2018.8480184.

Bugeja J., Davidsson P and Jacobsson A (2018) Functional Classification and Quantitative Analysis of Smart Connected Home Devices. In: *2018 Global Internet of Things Summit (GIoTS)*, Bilbao, June 2018, pp. 1–6. IEEE. DOI: 10.1109/GIOTS.2018.8534563.

Bugeja J, Jacobsson A and Davidsson P (2020) Is Your Home Becoming a Spy? A Data-Centered Analysis and Classification of Smart Connected Home Systems. In: 2020, p. 8.

Bühlmann M, Merkel W, Müller L, et al. (2012) The Democracy Barometer: A New Instrument to Measure the Quality of Democracy and its Potential for Comparative Research. *European Political Science* 11(4): 519–536. DOI: 10.1057/eps.2011.46.

Burdon M and Cohen T (2021) Modulation Harms and The Google Home. *Surveillance & Society* 19(2): 154–167. DOI: 10.24908/ss.v19i2.14299.

Burgess J and Hurcombe E (2019) Digital Journalism as Symptom, Response, and Agent of Change in the Platformed Media Environment. *Digital Journalism* 7(3). Routledge: 359–367. DOI: 10.1080/21670811.2018.1556313.

Burgess M (2019) What is GDPR? The summary guide to GDPR compliance in the UK. *Wired UK*, 21 January. Available at: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (accessed 28 May 2019).

Buttarelli G (2016) The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law* 6(2): 77–78. DOI: 10.1093/idpl/ipw006.

Byrne E and Doran M (2020) 'Far from over': News Corp journalist Annika Smethurst says High Court judgement a small victory. Available at: https://www.abc.net.au/news/2020-04-15/annika-smethurst-wins-afp-fight-high-court/12147706 (accessed 11 September 2020).

Calacci D, Shen JJ and Pentland A (2022) The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW2): 400:1-400:47. DOI: 10.1145/3555125.

Calvo-Valderrama MG, Marroquín-Rivera A, Burn E, et al. (2021) Adapting a Mental Health Intervention for Adolescents During the COVID-19 Pandemic: Web-Based Synchronous Focus Group Study. *JMIR formative research* 5(11): e30293. DOI: 10.2196/30293.

Camilli E (2016) OSINT, Big Data & Critical Infrastructures Protection (CIP). In: Niglia A (ed.) *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges*. Proceedings from NATO Advanced Research Workshop (ARW) 'Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges', held in Stockholm, Sweden, in May 2016. Amsterdam, Netherlands: IOS Press, pp. 35–42.

Cammaerts B and Carpentier N (2007) *Reclaiming the Media: Communication Rights and Democratic Media Roles*. Bristol, UK: Intellect Books.

Campbell S, Greenwood M, Prior S, et al. (2020) Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing* 25(8). SAGE Publications Ltd: 652–661. DOI: 10.1177/1744987120927206.

Cannell CF, Miller PV and Oksenberg L (1981) Research on Interviewing Techniques. *Sociological Methodology* 12. [American Sociological Association, Wiley, Sage Publications, Inc.]: 389–437. DOI: 10.2307/270748.

Cap P (2016) *The Language of Fear: Communicating Threat in Public Discourse*. London, UK: Springer.

Capurro R and Britz JB (2010) In search of a code of global information ethics: The road travelled and new horizons. *Ethical space: the international journal of communication ethics* 7(2/3): 28–36.

Carlo S and Kamphuis A (2014) *Information Security for Journalists v1.1*. Centre for Investigative Journalism. Available at: https://files.gendo.ch/Books/InfoSec_for_Journalists_V1.1.pdf (accessed 9 September 2019).

Carlon K (2016) Runkeeper is secretly tracking you around the clock and sending your data to advertisers. Available at: https://www.androidauthority.com/runkeeper-user-location-tracking-data-advertisers-692346/ (accessed 26 October 2020).

Carney D (1999) Summary: Security and Freedom through Encryption (SAFE) Act in 106th Congress. Available at: http://www.techlawjournal.com/cong106/encrypt/Default.htm (accessed 31 December 2020).

Carpentier N (2003) Journalism, Media, and Democracy. In: Cammaerts B and Carpentier N (eds) *Reclaiming the Media: Communication Rights and Democratic Media Roles*. Bristol, UK: Intellect Books, pp. 151–156. Available at: https://www.researchgate.net/profile/Nico_Carpentier/publication/242577897_Journalism_Media_and_Democracy/links/02e7e53885c7f4ce67000000/Journalism-Media-and-Democracy.pdf.

Carrión G, Huerta M and Barzallo B (2018) Monitoring and irrigation of an urban garden using IoT. In: *2018 IEEE Colombian Conference on Communications and Computing (COLCOM)*, Colombia, May 2018, pp. 1–6. IEEE. DOI: 10.1109/ColComCon.2018.8466722.

Carvalho R (2019) *Enhancing the investigation of malware-related crimes using semantic technologies*. http://purl.org/dc/dcmitype/Text. University of Oxford, Oxford, United Kingdom. Available at: https://ora.ox.ac.uk/objects/uuid:5abeb135-ff33-42b4-8847-0aefe8e82c8f (accessed 9 August 2022).

Casanovas P, De Koker L, Mendelson D, et al. (2017) Regulation of Big Data: Perspectives on strategy, policy, law and privacy. *Health and Technology* 7(4): 335–349. DOI: 10.1007/s12553-017-0190-6.

Castillo R (2011) *Jamison v. Summer Infant (Usa), Inc., 778 F. Supp. 2d 900*. No. 09 C 7513 - 778 F. Supp. 2d 900 (N.D. Ill. 2011) 74 U.C.C. Rep. Serv. 2d 408. Available at: https://casetext.com/case/jamison-v-summer-infant-usa (accessed 1 January 2021).

Castro D and New J (2016) *Everything the U.S. Government Is Doing to Help the Private Sector Build the Internet of Things*. 12 December. USA: Center for Data Innovation. Available at: https://www2.datainnovation.org/2016-federal-support-iot.pdf (accessed 1 January 2021).

Cavoukian A (2010) *Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. May. Toronto, Ontario, Canada: Information and Privacy Commissioner of Ontario. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf.

CBP Public Affairs (2017) CBP Releases Statistics on Electronic Device Searches. Available at: https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0 (accessed 9 September 2019).

Central Intelligence Agency (CIA) (2020) Country Comparison: Internet users — The World Factbook. Available at: https://www.cia.gov/library/publications/the-world-factbook/fields/204rank.html#TW (accessed 31 December 2020).

Cha S-C, Hsu T-Y, Xiang Y, et al. (2019) Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal* 6(2): 2159–2187. DOI: 10.1109/JIOT.2018.2878658.

Chalhoub G, Flechais I, Nthala N, et al. (2020) Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In: *Proceedings of the Sixteenth USENIX Symposium on Usable Privacy and Security*, Virtual, 9 August 2020, p. 21. USENIX Association.

Chapman E and Uren T (2018) *The Internet of Insecure Things*. #ICPCIoT, 19 March. Canberra, Australia: Australian Strategic Policy Institute. Available at: https://www.aspi.org.au/report/InternetOfInsecureThings (accessed 26 February 2020).

Charlesworth A (2021) Smart doorbells: how to use them without infringing a neighbour's privacy. *The Conversation*, 1 November. Available at: http://theconversation.com/smart-doorbells-how-to-use-them-without-infringing-a-neighbours-privacy-170180 (accessed 9 November 2021).

Chen J and Urquhart L (2021) 'They're all about pushing the products and shiny things rather than fundamental security': Mapping socio-technical challenges in securing the smart home. *Information & Communications Technology Law* 0(0). Routledge: 1–24. DOI: 10.1080/13600834.2021.1957193.

Chen P-K (2020) Taiwan's 'people-centered' New Southbound Policy and its impact on US–Taiwan relations. *The Pacific Review* 33(5). Routledge: 813–841. DOI: 10.1080/09512748.2019.1594349.

Chester E (2019) 7 best video doorbells to add smart security to your home. Available at: https://www.independent.co.uk/extras/indybest/gadgets-tech/best-video-doorbells-a9135211.html (accessed 11 September 2020).

Chhetri C and Genaro Motti V (2022) User-Centric Privacy Controls for Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW2): 349:1-349:36. DOI: 10.1145/3555769.

Chiou W-T (2020) Limits and Prospects of the Right to Be Forgotten in Taiwan. In: Werro F (ed.) *The Right To Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia*. Ius Comparatum - Global Studies in Comparative Law. Cham: Springer International Publishing, pp. 311–318. DOI: 10.1007/978-3-030-33512-0_16.

Choudhury SR (2019) Amazon says its facial recognition can now identify fear. *CNBC*, 14 August. Available at: https://www.cnbc.com/2019/08/14/amazon-says-its-facial-recognition-can-now-identify-fear.html (accessed 9 September 2019).

Christensen AT, Olesen H and Sørensen L (2021) On the Value of the Counterfactual and How the Smart Home Informs It. *Surveillance & Society* 19(2): 241–243. DOI: 10.24908/ss.v19i2.14301.

Christians CG, Glasser T, McQuail D, et al. (2009) *Normative Theories of the Media: Journalism in Democratic Societies*. Urbana and Chicago: University of Illinois Press.

Chu PM and Chien V (2019) The new era of the telecom industry: discussing the opportunities and challenges after the Telecommunication Management Act passed | Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=e3f35118-193b-4b7e-b5b9-a69acf67681a (accessed 31 December 2020).

Cimpanu C (2016) A Massive Botnet of CCTV Cameras Involved in Ferocious DDoS Attacks. *softpedia*, 27 June. Available at: https://news.softpedia.com/news/a-massive-botnet-of-cctv-cameras-involved-in-ferocious-ddos-attacks-505722.shtml (accessed 23 October 2020).

Cimpanu C (2019) Microsoft: Russian state hackers are using IoT devices to breach enterprise networks. *ZDNet*, 5 August. Available at: https://www.zdnet.com/article/microsoft-russian-state-hackers-are-using-iot-devices-to-breach-enterprise-networks/ (accessed 9 September 2019).

Clarke L (2020) UK publishes framework for post-Brexit EU data adequacy agreement. *New Statesman*, 18 March. Available at: https://tech.newstatesman.com/policy/uk-framework-data-adequacy-agreement (accessed 3 August 2020).

Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512. DOI: 10.1145/42411.42413.

Clayton J and Dyer J (2022) Apple AirTags - 'A perfect tool for stalking'. *BBC News*, 20 January. Available at: https://www.bbc.com/news/technology-60004257 (accessed 5 December 2022).

Clinic to End Tech Abuse (CETA), Cornell Tech (2020a) Tech Disconnect: Checklist. Clinic to End Tech Abuse, Cornell Tech. Available at: https://82beb9a6-b7db-490a-88be-9f149bafe221.filesusr.com/ugd/c4e6d5_20fe31daffd74b2fb4b4735d703dad6a.pdf (accessed 19 October 2021).

Clinic to End Tech Abuse (CETA), Cornell Tech (2020b) Technology Assessment Questionnaire (TAQ) v5. Clinic to End Tech Abuse, Cornell Tech. Available at: https://9aa4dcb3-08e0-4365-9068-df09709ff0ca.filesusr.com/ugd/884c63_280fab3bd82e44348691bbc9b9038a7d.pdf (accessed 19 October 2021).

Clinic to End Tech Abuse (CETA), Cornell Tech (2021) Resources. Available at: https://www.ceta.tech.cornell.edu (accessed 7 June 2021).

Cobbe J (2018) Big Data, Surveillance, and the Digital Citizen. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3234984.

Coleman WTJ (1984) Free Press: The Need to Ensure an Unfettered Check on Democratic Government between Elections. *Tulane Law Review* 59: 243.

Collinson P (2017) Is your smart meter spying on you? *The Guardian*, 24 June. Available at: https://www.theguardian.com/money/2017/jun/24/smart-meters-spying-collecting-private-data-french-british (accessed 9 September 2019).

Columbus L (2016) Roundup Of Internet Of Things Forecasts And Market Estimates, 2016. Available at: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/ (accessed 9 September 2019).

COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (2015) *Final Report Summary - VIRTUOSO (Versatile InfoRmation Toolkit for end-Users oriented Open Sources explOitation)*. 18 May. European Commission. Available at: https://cordis.europa.eu/project/rcn/94446/reporting/en (accessed 28 May 2019).

CommonWealth Magazine (2020) Taiwan's Tesla Boom, and Looking for More. Available at: https://topics.amcham.com.tw/2020/10/taiwan-tesla-boom/ (accessed 31 December 2020).

Communications Alliance (2020) *Government Must Support Security Committee Recommendations And Repair The Data Retention Regime*. 2020 Media Release 31, 29 October. Sydney, Australia: Communications Alliance. Available at: https://www.commsalliance.com.au/Documents/releases/2020-media-release-31 (accessed 31 December 2020).

Computer Security Division ITL (2020) NIST Releases FPD SP 800-53 Rev. 5 | CSRC. Available at: https://csrc.nist.gov/News/2020/nist-releases-fpd-sp-800-53-rev-5 (accessed 22 March 2020).

Constance E (2017) The Internet of Things: preparing for the revolution. *Journal of Cyber Policy* 2(2). Routledge: 152–154. DOI: 10.1080/23738871.2017.1361890.

Constantin L (2015a) Samsung smart TVs don't encrypt the voice data they collect. Available at: https://www.computerworld.com/article/2885775/samsung-smart-tvs-dont-encrypt-the-voice-data-they-collect.html (accessed 26 October 2020).

Constantin L (2015b) Smart TVs raise privacy concerns. Available at: https://www.computerworld.com/article/2881715/smart-tvs-raise-privacy-concerns.html (accessed 26 October 2020).

Conti M, Dehghantanha A, Franke K, et al. (2018) Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems* 78(2). Elsevier Ltd.: 544–546. DOI: 10.1016/j.future.2017.07.060.

Cornia A, Sehl A and Nielsen RK (2020) 'We no longer live in a time of separation': A comparative analysis of how editorial and commercial integration became a norm. *Journalism* 21(2). SAGE Publications: 172–190. DOI: 10.1177/1464884918779919.

Coulton P, Lindley JG and Cooper R (2018) *The Little Book of Design Fiction for the Internet of Things*. PETRAS Little Book Series. Lancaster: ImaginationLancaster, Lancaster University.

Council of Europe (2019a) Journalist Roberto Saviano Threatened with Withdrawal of his Police Protection. Available at: https://www.coe.int/en/web/media-freedom/detail-alert?p_p_id=sojdashboard_WAR_coesojportlet&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2&_sojdashboard_WAR_coesojportlet_alertId=48859415 (accessed 8 November 2020).

Council of Europe (2019b) *The 2019 Annual Report by the partner organisations of the Council of Europe's Platform for the Protection of Journalism and Safety of Journalists: 'Democracy at Risk: threats and attacks against media freedom in Europe'*. Annual Report by the partner organisations of the Council of Europe's Platform for the Protection of Journalism and Safety of Journalists, February. Council of Europe, Avenue de l'Europe F-67075 Strasbourg Cedex, France: Council of Europe. Available at: https://rm.coe.int/annual-report-2018-democracy-in-danger-threats-and-attacks-media-freed/1680926453 (accessed 11 January 2020).

Council on Foreign Relations (CFR) (2015) *Connect the Dots on State-Sponsored Cyber Incidents - Compromise of TV5 Monde*. Cyber Operations, April. New York, NY, USA: Council on Foreign Relations (CFR). Available at: https://www.cfr.org/cyber-operations/compromise-tv5-monde (accessed 13 September 2022).

Court of Justice of the European Union (2020) *Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield*. PRESS RELEASE No 91/20, 16

July. Luxembourg: Court of Justice of the European Union. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (accessed 21 September 2020).
Coventry University (2020) Computer misuse in the IoT. Available at: https://www.futurelearn.com/info/courses/the-rise-of-connected-devices/0/steps/68488 (accessed 31 December 2020).
Cox G (2019) Managing the risks of shadow IoT. *Network Security* 2019(1): 14–17. DOI: 10.1016/S1353-4858(19)30010-8.
Cox J (2019) Facebook Quietly Changes Search Tool Used by Investigators, Abused By Companies. In: *Vice*. Available at: https://www.vice.com/en_us/article/zmpgmx/facebook-stops-graph-search (accessed 3 March 2020).
Cox J (2020a) Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal. Available at: https://www.vice.com/en_ca/article/k7qyv3/customs-border-protection-venntel-location-data-dhs (accessed 11 September 2020).
Cox J (2020b) The Loophole the DMV Uses to Sell Your Data to Private Investigators. *VICE*, 27 August. Available at: https://www.vice.com/en_us/article/ep47na/dmv-dppa-drivers-privacy-protection-act-buy-data-private-investigators (accessed 11 September 2020).
Cox J (2021) Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras. *Motherboard*, 3 March. Available at: https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader (accessed 3 March 2021).
Crawford D and Sherman J (2018) Gaps in United States federal government IoT security and privacy policies. *Journal of Cyber Policy* 3(2). Routledge: 187–200. DOI: 10.1080/23738871.2018.1514061.
Creswell JW and Clark VLP (2017) *Designing and Conducting Mixed Methods Research*. United States of America: SAGE Publications.
Crete-Nishihata M, Oliver J, Parsons C, et al. (2020) The Information Security Cultures of Journalism. *Digital Journalism* 0(0). Routledge: 1–24. DOI: 10.1080/21670811.2020.1777882.
Cronk RJ and Shapiro SS (2021) Quantitative Privacy Risk Analysis. In: *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, September 2021, pp. 340–350. DOI: 10.1109/EuroSPW54576.2021.00043.
Crown Prosecution Service (2019a) Media: Assessing the Public Interest in Cases Affecting the Media | The Crown Prosecution Service. Available at: https://www.cps.gov.uk/legal-guidance/media-assessing-public-interest-cases-affecting-media (accessed 31 December 2020).
Crown Prosecution Service (2019b) Media: Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists | The Crown Prosecution Service. Available at: https://www.cps.gov.uk/legal-guidance/media-prosecuting-cases-where-public-servants-have-disclosed-confidential#c5 (accessed 31 December 2020).
Cuijpers C (2013) Legal aspects of open source intelligence – Results of the VIRTUOSO project. *Computer Law & Security Review* 29(6): 642–653. DOI: 10.1016/j.clsr.2013.09.002.
Cuthbertson A (2019) Google defends listening to private conversations on Google Home – but what intimate moments are recorded? *The Independent*, 12 July. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-home-recordings-listen-privacy-amazon-alexa-hack-a9002096.html (accessed 9 September 2019).

Cyber Independent Testing Lab (2019) Binary Hardening in IoT products. Available at: http://localhost:4000/2019/08/26/iot-data-writeup.html (accessed 11 September 2020).

D. Haggerty, Richard V. Ericson K (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605–622. DOI: 10.1080/00071310020015280.

Daly A, Robinson E and McMenemy D (2022) *Cyber security, surveillance and journalism in Scotland*. Science, Policy and Law Series 1, Leverhulme Research Centre for Forensic Science, 27 September. Dundee, Scotland: University of Dundee. Available at: https://discovery.dundee.ac.uk/ws/files/81462869/CyberSecurity_DigitalReport_1.0.pdf.

Danbury R (2018) Investigative Journalism and Terrorism: the Proactive Legal Duty to Report. In: Price S (ed.) *Investigative Journalism: Global Perspectives*. London: Routledge - Taylor and Francis Limited. Available at: https://dora.dmu.ac.uk/handle/2086/14926 (accessed 26 April 2021).

Data Protection and Privacy Commissioners (2010) Resolution on Privacy by Design. In: *32nd International Conference of Data Protection and Privacy Commissioners*, Jerusalem, Israel, 27 October 2010, p. 2. Available at: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

Datta A (2020) Governments of the world just ramped up spying on reporters. Available at: https://www.cjr.org/first_person/ft-nations-surveillance-attacks.php (accessed 18 February 2020).

Datta P, Namin AS and Chatterjee M (2018) A Survey of Privacy Concerns in Wearable Devices. In: *2018 IEEE International Conference on Big Data (Big Data)*, December 2018, pp. 4549–4553. DOI: 10.1109/BigData.2018.8622110.

Davies S (2016) The Data Protection Regulation: A Triumph of Pragmatism over Principle? *European Data Protection Law Review* 2(3): 290–296. DOI: 10.21552/EDPL/2016/3/5.

Davis R (2019) Thank You to Michael Bazzell with IntelTechniques — New Hope Investigations. In: *New Hope Investigations: PI Blog*. Available at: https://newhopeinvestigations.com/blog/thank-you-to-michael-bazzell-with-inteltechniques/2019/6/9 (accessed 3 March 2020).

De Groot J (2019) The History of Data Breaches. Available at: https://digitalguardian.com/blog/history-data-breaches (accessed 11 February 2020).

De Roure D, Hooper C, Page K, et al. (2015) Observing Social Machines Part 2: How to Observe? In: *Proceedings of the ACM Web Science Conference*, New York, NY, USA, 28 June 2015, pp. 1–5. WebSci '15. Association for Computing Machinery. DOI: 10.1145/2786451.2786475.

de Souza BP, Motta RC and Travassos GH (2019) Towards the Description and Representation of Smartness in IoT Scenarios Specification. In: *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*, Salvador, Brazil, 23 September 2019, pp. 511–516. SBES 2019. Association for Computing Machinery. DOI: 10.1145/3350768.3351797.

Deibert RJ (2020) *Reset: Reclaiming the Internet for Civil Society*. 1st ed. United Kingdom: September Publishing.

Deleuze G (2006) Chapter 3: Postscript on the Societies of Control*. In: *Surveillance, Crime and Social Control*. 1st ed. London, UK: Routledge.

DeNardis L and Raymond M (2017) The Internet of Things as a Global Policy Frontier. *UC Davis Law Review* 51(2): 23.

DeNisco Rayome A (2019) How to choose the right cybersecurity framework. Available at: https://www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ (accessed 23 March 2020).

Department for Business, Energy & Industrial Strategy (2016) *Smart Meters Implementation Programme 2016 progress update*. Department for Business, Energy & Industrial Strategy. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671929/Smart_Meters_2016_progress_update.pdf (accessed 9 September 2019).

Department for Digital, Culture, Media & Sport (2017) Press release: Government to strengthen UK data protection law. Available at: https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law (accessed 28 May 2019).

Department for Digital, Culture, Media & Sport (2018a) *Code of Practice for Consumer IoT Security*. 14 October. London, UK: Department for Digital, Culture, Media & Sport. Available at: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security (accessed 31 December 2020).

Department for Digital, Culture, Media & Sport (2018b) *Secure by Design: Improving the cyber security of consumer Internet of Things Report*. 7 March. London, UK: Department for Digital, Culture, Media & Sport. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf (accessed 5 February 2020).

Department for Digital, Culture, Media & Sport (2018c) Smart devices: using them safely in your home. Available at: https://www.gov.uk/government/publications/smart-devices-using-them-safely-in-your-home/smart-devices-using-them-safely-in-your-home (accessed 4 March 2020).

Department for Digital, Culture, Media & Sport (2020) Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation. Available at: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation (accessed 28 January 2020).

Department for Digital, Culture, Media & Sport (2021a) Government publishes first ever national action plan to protect journalists. Available at: https://www.gov.uk/government/news/government-publishes-first-ever-national-action-plan-to-protect-journalists (accessed 9 March 2021).

Department for Digital, Culture, Media & Sport (2021b) *Policy Paper: Government response to the call for views on consumer connected product cyber security legislation*. 21 April. London: Department for Digital, Culture, Media & Sport. Available at: https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation (accessed 19 May 2021).

Department for Digital, Culture, Media & Sport (2021c) The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet. Available at: https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet (accessed 15 November 2022).

Department for Digital, Culture, Media & Sport and Lopez (MP) J (2022) Secure connected places (smart cities) guidance collection. Available at: https://www.gov.uk/government/publications/secure-connected-places-smart-cities-guidance-collection (accessed 5 December 2022).

Department for Digital, Culture, Media & Sport and Warman MP M (2021) Press release: New cyber security laws to protect smart devices amid pandemic sales surge. In: *GOV.UK*. Available at: https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge (accessed 19 May 2021).

Department of Home Affairs (2020) Voluntary Code of Practice: Securing the Internet of Things for Consumers . Available at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice (accessed 31 December 2020).

Department of Investment Service, Ministry of Economic Affairs (2019) Key Industries: The Internet of Things. Department of Investment Service, Ministry of Economic Affairs. Available at: https://www.contacttaiwan.tw/ (accessed 31 December 2020).

Deutsche Welle (2020) Morocco arrests journalist on rape and spy charges. Available at: https://www.dw.com/en/omar-radi-morocco-journalist/a-54372595 (accessed 11 September 2020).

Deuze M (2005) What is journalism?: Professional identity and ideology of journalists reconsidered. *Journalism* 6(4): 442–464. DOI: 10.1177/1464884905056815.

@DFRLab (2018) Data and Defense: The Case of Strava. Available at: https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2 (accessed 9 August 2019).

Dhanjani N (2015) *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*. Sebastopol, CA, USA: O'Reilly Media, Inc.

Di Salvo P (2021) "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice* 0(0). Routledge: 1–18. DOI: 10.1080/17512786.2021.2014346.

Di Salvo P (2022) Information security and journalism: Mapping a nascent research field. *Sociology Compass* 16(3). John Wiley & Sons, Ltd: e12961. DOI: 10.1111/soc4.12961.

Digital Defenders Partnership (2019) The Digital First Aid Kit – Introduction. In: *Digital Defenders Partnership: Hivos International*. Available at: https://digitalfirstaid.org/en/index.html (accessed 9 September 2019).

Digital Shadows Ltd. (2021) *Cyber Threat Intelligence Solutions and Best Practices Guide*. 29 March. London, UK: Digital Shadows Ltd. Available at: https://resources.digitalshadows.com/digitalshadows/cyber-threat-intelligence-solutions-guide (accessed 10 June 2021).

Dixon T (2019) Here's how we solve the global crisis of tribalism and democratic decay. Available at: https://www.weforum.org/agenda/2019/01/can-globalization-tackle-tribalism-and-democratic-decay/ (accessed 7 February 2020).

DLA Piper (2019a) Law in Australia. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=AU&c2= (accessed 26 January 2020).

DLA Piper (2019b) Law in Taiwan, China. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=TW (accessed 26 January 2020).

DLA Piper (2019c) Law in United States. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2= (accessed 26 January 2020).

Doctorow C (2016) A lightbulb worm could take over every smart light in a city in minutes. In: *Boing Boing*. Available at: https://boingboing.net/2016/11/09/a-lightbulb-worm-could-take-ov.html (accessed 9 September 2019).

Doctorow C (2019) Discarded smart lightbulbs reveal your wifi passwords, stored in the clear. Available at: https://boingboing.net/2019/01/29/fiat-lux.html (accessed 5 December 2022).

Dodd M and Hanna M (2018) *McNae's Essential Law for Journalists*. 24th ed. Oxford: Oxford University Press.

Dooley B and Ueno H (2022) Where a Thousand Digital Eyes Keep Watch Over the Elderly. *The New York Times*, 2 February. Available at: https://www.nytimes.com/2022/02/02/business/japan-elderly-surveillance.html (accessed 5 December 2022).

Dorsemaine B, Gaulier J-P, Wary J-P, et al. (2015) Internet of Things: A Definition Taxonomy. In: *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Cambridge, UK, 9 September 2015, pp. 72–77. IEEE. DOI: 10.1109/NGMAST.2015.71.

Dubberley S, Koenig A and Murray D (2020) *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford University Press.

Dubois DJ, Kolcun R, Mandalari AM, et al. (2020) When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers. *Proceedings on Privacy Enhancing Technologies* 2020(4). Sciendo: 255–276. DOI: 10.2478/popets-2020-0072.

Duffy A (2021) Out of the shadows: The editor as a defining characteristic of journalism. *Journalism* 22(3). SAGE Publications: 634–649. DOI: 10.1177/1464884919826818.

Dullea E and Bowman B (2020) Privacy Attorneys | Internet of Things (IoT) Cybersecurity Improvement Act. Available at: https://www.bytebacklaw.com/2020/12/congress-passes-the-internet-of-things-iot-cybersecurity-improvement-act/ (accessed 31 December 2020).

Dumas JS and Redish JC (1999) *A Practical Guide to Usability Testing*. 1st ed. UK: Intellect Books.

Edu JS, Such JM and Suarez-Tangil G (2019) Smart Home Personal Assistants: A Security and Privacy Review. *arXiv:1903.05593 [cs]*. Available at: http://arxiv.org/abs/1903.05593 (accessed 21 August 2020).

Edwards L and Urquhart L (2016) Privacy in public spaces: what expectations of privacy do we have in social media intelligence? *International Journal of Law and Information Technology* 24(3): 279–310. DOI: 10.1093/ijlit/eaw007.

Eisenhardt KM (1989) Building Theories from Case Study Research. *The Academy of Management Review* 14(4). Academy of Management: 532–550. DOI: 10.2307/258557.

Elder J (2019) How Kevin Ashton named The Internet of Things. Available at: https://blog.avast.com/kevin-ashton-named-the-internet-of-things (accessed 11 May 2022).

Electronic Frontier Foundation (2019) Surveillance Self-Defense: Tips, Tools and How-Tos for Safer Online Communications. Available at: https://ssd.eff.org/en (accessed 11 September 2020).

Electronic Frontier Foundation (2020) Threat model. Available at: https://ssd.eff.org/en/glossary/threat-model (accessed 11 September 2020).

Ellao JAJ (2019) What you need to know about the ongoing cyber-attacks vs. alternative news Bulatlat. In: *Bulatlat*. Available at: https://www.bulatlat.com/2019/02/07/what-you-need-to-know-about-the-ongoing-cyber-attacks-vs-alternative-news-bulatlat/ (accessed 4 March 2020).

Elliott V (2021) Four ways governments disrupt internet access. Available at: https://restofworld.org/2021/four-ways-governments-disrupt-internet-access/ (accessed 4 May 2021).

Elmer G (2003) A Diagram of Panoptic Surveillance. *New Media & Society* 5(2). SAGE Publications: 231–247. DOI: 10.1177/1461444803005002005.

Erlingsson C and Brysiewicz P (2017) A hands-on guide to doing content analysis. *African Journal of Emergency Medicine* 7(3): 93–99. DOI: 10.1016/j.afjem.2017.08.001.

eSafety Commissioner (2020) eSafety Commissioner. Available at: https://www.esafety.gov.au/homepage (accessed 31 December 2020).

Ess C (2005) 'Lost in Translation'?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia). *Ethics and Information Technology; Dordrecht* 7(1). Dordrecht, Netherlands, Dordrecht: Springer Nature B.V.: 1–6. DOI: http://dx.doi.org/10.1007/s10676-005-0454-0.

E&T editorial staff (2017) IoT devices could communicate using ambient radio waves. Available at: https://eandt.theiet.org/content/articles/2017/05/iot-devices-could-communicate-using-ambient-radio-waves/ (accessed 9 September 2019).

E&T editorial staff (2019) Laser pointer could hack voice-controlled virtual assistants. Available at: https://eandt.theiet.org/content/articles/2019/11/laser-pointer-could-hack-voice-controlled-virtual-assistants/ (accessed 11 September 2020).

Etherington D and Conger K (2016) Large DDoS attacks cause outages at Twitter, Spotify, and other sites. In: *TechCrunch*. Available at: http://social.techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/ (accessed 9 September 2019).

ETSI (2019) *CYBER; Cyber Security for Consumer Internet of Things*. CYBER ETSI TS 103 645 V1.1.1 (2019-02), February. Sophia-Antipolis, France: European Telecommunications Standards Institute (ETSI). Available at: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (accessed 10 September 2019).

European Centre for Press & Media Freedom (2017) Ukraine: Authorities block journalists as threats to national security. In: *Mapping Media Freedom*. Available at: https://mappingmediafreedom.org/index.php/2017/09/13/ukraine-journalists-threat-national-security/ (accessed 9 September 2019).

European Commission (2012) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). European Commission. Available at: https://web.archive.org/web/20121203024154/http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 28 May 2019).

European Commission (2018) What are Data Protection Authorities (DPAs)? Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (accessed 28 May 2019).

European Commission (2020) What is personal data? Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (accessed 28 May 2019).

European Court of Human Rights and Council of Europe (1998) *European Convention on Human Rights*. 1 November.

European Data Protection Board (2019) *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3): Version 2.0*. 12 November. European Union: European Data Protection Board. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf (accessed 3 August 2020).

European Parliament and Council of the European Union (2018) General Data Protection Regulation (GDPR) – Official Legal Text. Available at: https://gdpr-info.eu/ (accessed 3 March 2020).

European Union Agency For Network and Information Security (ENISA) (2014) *Privacy and Data Protection by Design - from policy to engineering*. Report/Study, December. Athens, Greece: European Union Agency For Network and Information Security (ENISA). Available at:

https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (accessed 18 February 2020).

European Union Agency For Network and Information Security (ENISA) (2019) *ENISA Threat Landscape Report 2018*. Report/Study, 28 January. Athens, Greece: European Union Agency For Network and Information Security (ENISA). Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed 15 January 2020).

Ezzy D (2002) Chapter 6: Writing about qualitative data. In: *Qualitative Analysis: Practice and Innovation*. London, UK: Routledge, pp. 138–163.

Falco G, Eling M, Jablanski D, et al. (2019) Cyber risk research impeded by disciplinary barriers. *Science* 366(6469): 1066–1069. DOI: 10.1126/science.aaz4795.

Federal Aviation Administration (2013) Press Release – FAA to Allow Airlines to Expand Use of Personal Electronics. Available at: https://www.faa.gov/news/press_releases/news_story.cfm?cid=TW189&newsId=15254 (accessed 9 September 2019).

Federal Bureau of Investigation (FBI) (2017) *Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*. Internet Crime Complaint Center (IC3) Alert Number I-071717 (Revised)-PSA, 17 July. USA: Federal Bureau of Investigation (FBI). Available at: https://www.ic3.gov/Media/Y2017/PSA170717 (accessed 7 January 2021).

Federal Data Protection and Information Commissioner (FDPIC) (2020) *Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 Para. 1 Swiss Federal Act on Data Protection*. 8 September. Switzerland: Federal Data Protection and Information Commissioner (FDPIC). Available at: https://aboutblaw.com/S17 (accessed 21 September 2020).

Feldman D (1994) Secrecy, Dignity, or Autonomy? Views of Privacy as a Civil Liberty. *Current Legal Problems* 47(Part_2): 41–71. DOI: 10.1093/clp/47.Part_2.41.

Fickling D (2004) Australia seen as 'America's deputy sheriff'. Available at: http://www.theguardian.com/world/2004/sep/10/indonesia.australia (accessed 1 January 2021).

Finley K (2014) Why Tech's Best Minds Are Very Worried About the Internet of Things. *Wired*, 19 May. Available at: https://www.wired.com/2014/05/iot-report/ (accessed 26 October 2020).

Firesmith DG (2003) Security Use Cases. *Journal of Object Technology* 2(3): 53–64.

Flammer I (2016) Genteel Wearables: Bystander-Centered Design. *IEEE Security Privacy* 14(5): 73–79. DOI: 10.1109/MSP.2016.91.

Focus Taiwan: CNA English News (2020) Microsoft plans to establish IoT Center of Excellence in Taiwan. Available at: https://focustaiwan.tw/sci-tech/202008200014 (accessed 31 December 2020).

Foucault M (1977) *DISCIPLINE AND PUNISH: The Birth of the Prison*. New York: Knopf Doubleday Publishing Group.

Franceschi-Bicchierai L (2015) One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids. *Motherboard*, 27 November. Available at: https://www.vice.com/en/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids (accessed 26 October 2020).

Freund J (2020) Threat-Modeling Basics Using MITRE ATT&CK. Available at: https://www.darkreading.com/risk/threat-modeling-basics-using-mitre-attandck/a/d-id/1337728 (accessed 11 September 2020).

Frost C (2015) *Journalism Ethics and Regulation*. Oxford, United Kingdom: Routledge.
Frost J and Hamlin A (2020) Ransomware - A Strategic Threat to Organizations. *Mountain Plains Journal of Business and Technology* 21(2). Available at: https://openspaces.unk.edu/mpjbt/vol21/iss2/6.
Fruhlinger J (2020a) The CIA triad: Definition, components and examples. In: *CSO Online*. Available at: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html (accessed 14 April 2020).
Fruhlinger J (2020b) Threat modeling explained: A process for anticipating cyber attacks. Available at: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html (accessed 11 September 2020).
Furszyfer Del Rio DD, Sovacool BK and Griffiths S (2021) Culture, energy and climate sustainability, and smart home technologies: A mixed methods comparison of four countries. *Energy and Climate Change*: 100035. DOI: 10.1016/j.egycc.2021.100035.
Gabbai A (2015) Kevin Ashton Describes 'the Internet of Things'. Available at: https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/ (accessed 11 May 2022).
Gaber I and Tiffen R (2018) Politics and the media in Australia and the United Kingdom: parallels and contrasts. *Media International Australia* 167(1). SAGE Publications Ltd: 27–40. DOI: 10.1177/1329878X18766721.
Galič M, Timan T and Koops B-J (2017) Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology* 30(1): 9–37. DOI: 10.1007/s13347-016-0219-1.
Galtung J and Ruge MH (1965) The Structure of Foreign News: The Presentation of the Congo, Cuba and Cyprus Crises in Four Norwegian Newspapers. *Journal of Peace Research* 2(1): 64–90. DOI: 10.1177/002234336500200104.
Garcia D (2017) Leaking privacy and shadow profiles in online social networks. *Science Advances* 3(8): e1701172. DOI: 10.1126/sciadv.1701172.
Garside J (2015) Twitter puts trillions of tweets up for sale to data miners. *The Guardian*, 18 March. Available at: https://www.theguardian.com/technology/2015/mar/18/twitter-puts-trillions-tweets-for-sale-data-miners (accessed 3 March 2020).
Garside J (2020) English law 'abused by the powerful to threaten foreign journalists'. *The Guardian*, 2 November. Available at: https://www.theguardian.com/law/2020/nov/02/english-law-abused-by-the-powerful-to-threaten-foreign-journalists (accessed 20 November 2020).
GCHQ (2019) The Equities Process. Available at: https://www.gchq.gov.uk/information/equities-process (accessed 31 December 2020).
Geeng C and Roesner F (2019) Who's In Control? Interactions In Multi-User Smart Homes. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2 May 2019, pp. 1–13. CHI '19. Association for Computing Machinery. DOI: 10.1145/3290605.3300498.
George AL and Bennett A (2005) *Case Studies and Theory Development in the Social Sciences*. 1st ed. Belfer Center for Science and International Affairs. Cambridge, Massachusetts: MIT Press.
Giering C, Miller J, Raggi M, et al. (2022) *Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media*. 11 July. USA: Proofpoint US. Available at:

https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists (accessed 27 September 2022).
Ginsburg T and Huq AZ (2018) *How to Save a Constitutional Democracy*. First edition. Chicago; London: University of Chicago Press. Available at: https://www.press.uchicago.edu/ucp/books/book/chicago/H/bo28381225.html.
Giurgiu A and Larsen TA (2016) Roles and Powers of National Data Protection Authorities. *European Data Protection Law Review* 2(3): 342–352. DOI: 10.21552/EDPL/2016/3/9.
GJS (2019) Digital Safety Curriculum for Newsrooms. Available at: https://www.gjs-security.com/digital-safety-curriculum-for-newsrooms/ (accessed 9 September 2019).
Glassman M and Kang MJ (2012) Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior* 28(2): 673–682. DOI: 10.1016/j.chb.2011.11.014.
Global Cyber Alliance (2020) Global Cyber Alliance Provides Cybersecurity Toolkit for Journalists. In: *GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk*. Available at: https://www.globalcyberalliance.org/global-cyber-alliance-provides-cybersecurity-toolkit-for-journalists/ (accessed 26 September 2022).
Goggin B (2019) 3,200 people have lost their jobs so far this year in a media landslide. Available at: https://www.businessinsider.com/2019-media-layoffs-job-cuts-at-buzzfeed-huffpost-vice-details-2019-2 (accessed 9 September 2019).
Gomez J (2004) Dumbing Down Democracy: Trends in Internet Regulation, Surveillance and Control in Asia. *ASIARIGHTS* (1). Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.512.9523&rep=rep1&type=pdf.
Goodin D (2015) Man-in-the-middle attack on Vizio TVs coughs up owners' viewing habits. Available at: https://arstechnica.com/information-technology/2015/11/man-in-the-middle-attack-on-vizio-tvs-coughs-up-owners-viewing-habits/ (accessed 26 October 2020).
Goodrick D (2014) *Comparative Case Studies: Methodological Briefs - Impact Evaluation No. 9*. Methodological Briefs. Florence, Italy: UNICEF-IRC. Available at: https://www.unicef-irc.org/publications/754-comparative-case-studies-methodological-briefs-impact-evaluation-no-9.html (accessed 21 March 2020).
Goodwin B (2020) NI police unable to delete data seized unlawfully from journalists for 10 years. Available at: https://www.computerweekly.com/news/252489306/NI-Police-unable-to-delete-data-seized-unlawfully-from-journalists-for-10-years (accessed 28 October 2022).
Goulden M, Tolmie P, Mortier R, et al. (2018) Living with interpersonal data: Observability and accountability in the age of pervasive ICT. *New Media & Society* 20(4). SAGE Publications: 1580–1599. DOI: 10.1177/1461444817700154.
Goumagias N, Whalley J, Dilaver O, et al. (2021) Making sense of the internet of things: a critical review of internet of things definitions between 2005 and 2019. *Internet Research* 31(5). Emerald Publishing Limited: 1583–1610. DOI: 10.1108/INTR-01-2020-0013.
Government of Canada (2021) Measures of central tendency: Calculating the mode. Available at: https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch11/mode/5214873-eng.htm (accessed 13 September 2022).

GOV.UK (2019) Consumer Protection: Secure by Design. Available at: https://www.gov.uk/government/collections/secure-by-design (accessed 10 September 2019).
Gradinar A, Van Kleek M, Pschetz L, et al. (2019) *The Little Book of the Internet of Things for the Home*. Lancaster: Lancaster University. DOI: https://eprints.lancs.ac.uk/id/eprint/136910/1/Little_Book_of_IoT_Home_Online.pdf.
Graham L (2019) The Walkley Foundation's Submission to the Inquiry Into the Impact of The Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press. Available at: https://docslib.org/doc/11350449/the-walkley-foundations-submission-to-the-inquiry-into-the-impact-of-the (accessed 26 September 2022).
Gravitas Desk (2020) Now, China attacks journalists abroad, targets Australian journalist Bang Xiao. Available at: https://www.wionews.com/world/now-china-attacks-journalists-abroad-targets-australian-journalist-bang-xiao-345160 (accessed 31 December 2020).
Greenberg A (2019) This Tesla Mod Turns a Model S Into a Mobile 'Surveillance Station'. *Wired*, 9 August. Available at: https://www.wired.com/story/tesla-surveillance-detection-scout/ (accessed 9 September 2019).
Greenberg A (2020) Hackers Broke Into Real News Sites to Plant Fake Stories. *Wired*, 29 July. Available at: https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/ (accessed 19 October 2020).
Greenleaf G, Johnston A, Arnold B, et al. (2019) *Digital platforms: The need to restrict surveillance capitalism*. Digital Platforms Inquiry—preliminary report, 22 February. Australian Privacy Foundation submission to the ACCC.
Greenslade R (2015) The D-notice system: a typically British fudge that has survived a century. Available at: http://www.theguardian.com/media/2015/jul/31/d-notice-system-state-media-press-freedom (accessed 31 December 2020).
Griffiths J (2020) Philippines journalist Maria Ressa found guilty of 'cyber libel' in latest blow to free press. *CNN*, 15 June. Available at: https://www.cnn.com/2020/06/14/asia/maria-ressa-philippines-cyber-libel-intl-hnk/index.html (accessed 20 November 2020).
Griffiths L (2005) The Implied Freedom of Political Communication: The State of the Law Post Coleman and Mulholland. *James Cook University Law Review* 12: 93.
Grunbaum B (1975) Venn Diagrams and Independent Families of Sets. *Mathematics Magazine* 48(1). Mathematical Association of America: 12–23. DOI: 10.2307/2689288.
Guardian staff (2017) Paradise Papers legal action against BBC and Guardian condemned. Available at: http://www.theguardian.com/uk-news/2017/dec/19/paradise-papers-legal-action-against-bbc-and-guardian-condemned (accessed 31 December 2020).
Guariglia JK and M (2022) Ring Reveals They Give Videos to Police Without User Consent or a Warrant. Available at: https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant (accessed 5 December 2022).
Guariglia M (2019) Amazon's Ring Is a Perfect Storm of Privacy Threats. Available at: https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats (accessed 9 September 2019).
Gude K (2022) Encryption Helps Ukrainians Resist Russia's Invasion, but a European Plan Threatens the Underlying Trust Any Tech User Needs. *Just Security*, 17 November. Available at:

https://www.justsecurity.org/84156/encryption-helps-ukrainians-resist-russias-invasion-but-a-european-plan-threatens-the-underlying-trust-any-tech-user-needs/ (accessed 20 November 2022).
Gulzar M and Abbas G (2019) Internet of Things Security: A Survey and Taxonomy. In: *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, February 2019, pp. 1–6. IEEE. DOI: 10.1109/CEET1.2019.8711834.
Gunashekar S, Spisak A, Dean K, et al. (2016) *Accelerating the Internet of Things in the UK: Using policy to support practice*. 4 October. Santa Monica, CA: RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR1492.html (accessed 31 December 2020).
Halliday M, Mill D, Johnson J, et al. (2021) Let's talk virtual! Online focus group facilitation for the modern researcher. *Research in Social and Administrative Pharmacy* 17(12): 2145–2150. DOI: 10.1016/j.sapharm.2021.02.003.
Hamilton E (2020) Eric Hamilton on Twitter: 'Here's a thing that happened today. I was recently -- and falsely -- linked to an article I didn't write, because the author who DID write it happens to share the same name/byline as I do. I'm not going to link to it because it's complete garbage.' Available at: https://twitter.com/OnetheycallEric/status/1270857748092239872 (accessed 13 September 2020).
Hancock B, Ockleford E and Windridge K (2009) *An Introduction to Qualitative Research: Presenting Qualitative Research*. UK: The NIHR Research Design Service for Yorkshire & the Humber. Available at: https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/5_Introduction-to-qualitative-research-2009.pdf (accessed 21 December 2022).
Haner JK and Knake RK (2021) Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity. *Journal of Cybersecurity* 7(tyab003). DOI: 10.1093/cybsec/tyab003.
Harcup T and O'Neill D (2017) What is News? *Journalism Studies* 18(12). Routledge: 1470–1488. DOI: 10.1080/1461670X.2016.1150193.
Hare K (2020) Here are the newsroom layoffs, furloughs and closures caused by the coronavirus. In: *Poynter*. Available at: https://www.poynter.org/business-work/2020/here-are-the-newsroom-layoffs-furloughs-and-closures-caused-by-the-coronavirus/ (accessed 1 January 2021).
Harkin D and Mann M (2022) *Securing Australian Journalism from Surveillance*. ACCAN Grants Program, August. Australia: Deakin University. Available at: https://blogs.deakin.edu.au/criminology/wp-content/uploads/sites/2/2022/09/Deakin_Report_Electronic-surveillance_V03-1.pdf (accessed 15 November 2022).
Harmon SHE, Haddow G and Gilman L (2015) New risks inadequately managed: the case of smart implants and medical device regulation. *Law, Innovation and Technology* 7(2). Routledge: 231–252. DOI: 10.1080/17579961.2015.1106107.
Harper C (2020) In China, smart locks are being used to track citizens and enforce lockdowns. In: *Reclaim The Net*. Available at: https://reclaimthenet.org/in-china-smart-locks-are-being-used-to-track-citizens/ (accessed 6 October 2020).
Harrington D (2022) U.S. Privacy Laws: The Complete Guide. Available at: https://www.varonis.com/blog/us-privacy-laws (accessed 15 November 2022).
Harrison RL, Reilly TM and Creswell JW (2020) Methodological Rigor in Mixed Methods: An Application in Management Studies. *Journal of Mixed Methods Research* 14(4). SAGE Publications: 473–495. DOI: 10.1177/1558689819900585.

Hartley J (2004) Case Study Research. In: Cassell C and Symon G (eds) *Essential Guide to Qualitative Methods in Organizational Research*. London: SAGE Publications Ltd., pp. 323–333. DOI: 10.4135/9781446280119.

Hasan R, Crandall D, Fritz M, et al. (2019) Understanding and Recognizing Bystanders in Images for Privacy Protection. In: *19th Privacy Enhancing Technologies Symposium*, KTH, Stockholm, Sweden, 15 July 2019, p. 2.

Hashem IAT, Chang V, Anuar NB, et al. (2016) The role of big data in smart city. *International Journal of Information Management* 36(5): 748–758. DOI: 10.1016/j.ijinfomgt.2016.05.002.

Haskins C (2019) Amazon Told Police It Has Partnered With 200 Law Enforcement Agencies. In: *Vice*. Available at: https://www.vice.com/en_us/article/j5wyjy/amazon-told-police-it-has-partnered-with-200-law-enforcement-agencies (accessed 10 September 2019).

Hassan WU, Hussain S and Bates A (2018) Analysis of Privacy Protections in Fitness Tracking Social Networks - or- You can run, but can you hide? In: *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 497–512. Available at: https://www.usenix.org/conference/usenixsecurity18/presentation/hassan (accessed 19 April 2022).

He H, Maple C, Watson T, et al. (2016) The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing other computational intelligence. In: *2016 IEEE Congress on Evolutionary Computation (CEC)*, Vancouver, BC, July 2016, pp. 1015–1021. IEEE. DOI: 10.1109/CEC.2016.7743900.

Hearing on 'OPM: Data Breach': Opening Statement (2015) Washington DC. Available at: https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2471%20-%20Color%20Copier%40mail.house_.gov_20150616_081132.pdf (accessed 28 May 2019).

Heartfield R, Loukas G, Budimir S, et al. (2018) A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78: 398–428. DOI: 10.1016/j.cose.2018.07.011.

Heer T, Garcia-Morchon O, Hummen R, et al. (2011) Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications* 61(3): 527–542. DOI: 10.1007/s11277-011-0385-5.

Henrichsen J, Betz M and Lisosky JM (2015) *Building Digital Safety for Journalism: A Survey of Selected Issues*. UNESCO Series on Internet Freedom. Paris: UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000232358.

Henrichsen JR (2019) Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. *Digital Journalism* 0(0): 1–19. DOI: 10.1080/21670811.2019.1653207.

Henrichsen JR (2021) Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice* 0(0). Routledge: 1–20. DOI: 10.1080/17512786.2021.1927802.

Henrie M (2013) Cyber Security Risk Management in the SCADA Critical Infrastructure Environment. *Engineering Management Journal* 25(2). Taylor & Francis: 38–45. DOI: 10.1080/10429247.2013.11431973.

Henze M, Hermerschmidt L, Kerpen D, et al. (2014) User-Driven Privacy Enforcement for Cloud-Based Services in the Internet of Things. In: *2014 International Conference on Future Internet of Things and Cloud*, August 2014, pp. 191–196. DOI: 10.1109/FiCloud.2014.38.

Herian R (2020) Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology* 12(1). Routledge: 156–174. DOI: 10.1080/17579961.2020.1727094.

Hermann E and McChesney RW (2001) *Global Media: The New Missionaries of Global Capitalism*. United Kingdom: Bloomsbury Academic. Available at: https://www.google.co.uk/books/edition/Global_Media/NJu27PeypxYC?hl=en&gbpv=1.

Hermida A (2010) Twittering the News. *Journalism Practice* 4(3): 297–308. DOI: 10.1080/17512781003640703.

Hern A (2018) Most GDPR emails unnecessary and some illegal, say experts. *The Guardian*, 21 May. Available at: https://www.theguardian.com/technology/2018/may/21/gdpr-emails-mostly-unnecessary-and-in-some-cases-illegal-say-experts (accessed 28 May 2019).

Hernandez A (2021) What Can Your Connected Car Reveal About You? In: *Dark Reading*. Available at: https://www.darkreading.com/vulnerabilities---threats/what-can-your-connected-car-reveal-about-you/a/d-id/1340145 (accessed 3 March 2021).

Hernández Ramos JL, Bernabé JB and Skarmeta AF (2014) Towards Privacy-Preserving Data Sharing in Smart Environments. In: *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, July 2014, pp. 334–339. DOI: 10.1109/IMIS.2014.44.

Herrman J (2019) The Tools for Covering Tech Are the Same as in 2009. *The New York Times*, 31 July. Available at: https://www.nytimes.com/2019/07/31/technology/personaltech/tools-covering-tech-same-2009.html (accessed 9 September 2019).

Hesse-Biber SN and Johnson RB (2015) *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*. Oxford, United Kingdom: Oxford University Press, Incorporated. Available at: http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=2044599 (accessed 6 July 2020).

Hickman T (2015) *In The Investigatory Powers Tribunal Between: Privacy International, Greennet Limited, Riseup Networks Inc, Mango Email Service, Korean Progressive Network ("Jinbonet"), Greenhost Media Jumpstart Inc., Chaos Computer Club And (1) Secretary Of State For Foreign And Commonwealth Affairs (2) Government Communication Headquarters: Skeleton Argument Served On Behalf Of The Claimants - For Hearing: Tuesday 1 December 2015*. Case Nos. IPT 14/85, 120-126/CH, 7 October. London, UK: Investigatory Powers Tribunal. Available at: https://privacyinternational.org/sites/default/files/2018-03/2015.10.07%20PI%20Greennet%20Skeleton%20FINAL.pdf (accessed 31 December 2020).

Hicks M (2018) *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing*. History of computing. Cambridge, MA London, UK: MIT Press.

Higgins JPT, Thomas J, Chandler J, et al. (2019) *Cochrane Handbook for Systematic Reviews of Interventions*. 2nd edition. Hoboken, NJ: John Wiley & Sons.

High Court of Australia (1937) *Victoria Park Racing & Recreation Grounds Co Ltd v Taylor [1937] HCA 45; (1937) 58 CLR 479 (26 August 1937)*. 45. Available at: http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/1937/45.html (accessed 31 March 2021).

High Court of Australia (1997) *Lange v Australian Broadcasting Corporation ('Political Free Speech case')*. 25. Available at: http://www7.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/1997/25.html (accessed 31 December 2020).

Hildebrandt M (2020a) *Law for Computer Scientists and Other Folk*. UK: Oxford University Press.

Hildebrandt M (2020b) *Law for Computer Scientists and Other Folk*. 1st ed. New York, NY, USA: Oxford University Press.

Hill C (2015) Wearables – the future of biometric technology? *Biometric Technology Today* 2015(8): 5–9. DOI: 10.1016/S0969-4765(15)30138-7.

Hill K (2020) Activate This 'Bracelet of Silence,' and Alexa Can't Eavesdrop. *The New York Times*, 14 February. Available at: https://www.nytimes.com/2020/02/14/technology/alexa-jamming-bracelet-privacy-armor.html (accessed 17 February 2020).

Hille K (2019) US and Taiwan host security exercise to boost cyber defence. *Financial Times*, 4 November. Available at: https://www.ft.com/content/7d6c78cc-fec8-11e9-b7bc-f3fa4e77dd47 (accessed 31 December 2020).

Hinkes C (2021) Key aspects to consider when conducting synchronous text-based online focus groups – a research note. *International Journal of Social Research Methodology* 24(6). Routledge: 753–759. DOI: 10.1080/13645579.2020.1801277.

Ho C (2019) Configuration of the Notion of Privacy as a Fundamental Right in Taiwan—A Comparative Study of International Treaties and EU Rules. In: Cohen JA, Alford WP, and Lo C (eds) *Taiwan and International Human Rights: A Story of Transformation*. Economics, Law, and Institutions in Asia Pacific. Singapore: Springer, pp. 423–436. DOI: 10.1007/978-981-13-0350-0_24.

Hoepman J-H (2014) Privacy Design Strategies. In: *ICT Systems Security and Privacy Protection* (eds N Cuppens-Boulahia, F Cuppens, S Jajodia, et al.), Berlin, Heidelberg, 2014, pp. 446–459. IFIP Advances in Information and Communication Technology. Springer. DOI: 10.1007/978-3-642-55415-5_38.

Hoffmann S (2018) *IoT Security Architecture and Policy for the Home - a Hub Based Approach*. 15 November. Oxford, United Kingdom: IoT Security Foundation. Available at: https://oxil.uk/publications/iotsf-security-architecture-home/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf (accessed 12 August 2020).

Holcomb J and Mitchell A (2015) Adoption of Digital Security Tools. In: *Pew Research Center's Journalism Project*. Available at: https://www.pewresearch.org/journalism/2015/02/05/adoption-of-digital-security-tools/ (accessed 9 December 2022).

Holcomb J, Mitchell A and Page D (2015) *Investigative journalists and digital security: Perceptions of vulnerability and changes in behavior*. Investigative journalists and digital security, 5 February. Columbia University, New York: Pew Research Center in association with Columbia University's Tow Center for Digital Journalism. Available at: https://www.journalism.org/wp-content/uploads/sites/8/2015/02/PJ_InvestigativeJournalists_0205152.pdf.

Honeywell L (2020) Leigh Honeywell @ 🏠 on Twitter: 'Btw this Eric Hamilton is _not_ the author of the shitty stalker article, just has the misfortune of the same name and profession'. Available at: https://twitter.com/hypatiadotca/status/1270978645327110145 (accessed 13 September 2020).

Honeywood CA (2016) Britain's Approach to Balancing Counter-Terrorism Laws with Human Rights. *Journal of Strategic Security* 9(3). University of South Florida Board of Trustees: 28–48.

House of Commons: Home Affairs Committee (2008) *HC 58-I: A Surveillance Society?* Volume I Fifth Report of Session 2007–08, 8 June. Available at: https://publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf (accessed 28 May 2019).

House of Commons: Science and Technology Committee (2016a) House of Commons - Evidence Check: Smart metering of electricity and gas - Science and Technology Committee. Available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/161/16108.htm#footnote-019 (accessed 14 March 2020).

House of Commons: Science and Technology Committee (2016b) *The big data dilemma*. Fourth Report of Session 2015–16 (HC 468), 10 February. London: The Stationery Office Limited: House of Commons. Available at: https://publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf.

House TW (2022) FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/ (accessed 27 October 2022).

Hribar G, Podbregar I and Ivanuša T (2014) OSINT: A "Grey Zone"? *International Journal of Intelligence and CounterIntelligence* 27(3): 529–549. DOI: 10.1080/08850607.2014.900295.

Huang DY, Apthorpe N, Li F, et al. (2020) IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4(2): 1–21. DOI: 10.1145/3397333.

Huang J-N (2016) *Liberalization, Economic Dependence, and the Paradox of Taiwan's Press Freedom*. UC Riverside, California, USA. Available at: https://escholarship.org/uc/item/3j53d4r1 (accessed 23 April 2021).

Huang T (2020) Taiwan's digital minister says personal data protection agency needed for digital ID | Taiwan News | 2020/07/30. Available at: https://www.taiwannews.com.tw/en/news/3976854 (accessed 31 December 2020).

Hulnick AS (2002) The Downside of Open Source Intelligence. *International Journal of Intelligence and CounterIntelligence* 15(4): 565–579. DOI: 10.1080/08850600290101767.

Huntley S and Marquis-Boire M (2014) Tomorrow's news is today's intel: Journalists as targets and compromise vectors. Singapore. Available at: https://www.blackhat.com/docs/asia-14/materials/Huntley/BH_Asia_2014_Boire_Huntley.pdf.

Hurst (2020) UK and US lock in behind Australia in China row. Available at: http://www.theguardian.com/australia-news/2020/dec/02/uk-and-us-lock-in-behind-australia-in-china-row (accessed 1 January 2021).

Hypponen M and Nyman L (2017) The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. *Technology Innovation Management Review* 7(4): 7.

ICIJ (2016) The Panama Papers: Exposing the Rogue Offshore Finance Industry - ICIJ. Available at: https://www.icij.org/investigations/panama-papers/ (accessed 9 September 2019).

IGIS (2020) Inspector-General of Intelligence and Security | IGIS. Available at: https://www.igis.gov.au/ (accessed 31 December 2020).

In The High Court Of Justice In Northern Ireland, Queen's Bench Division (Judicial Review), In The Matter Of An Application By Fine Point Films And Trevor Birney For Judicial Review And In The Matter Of An Application By Barry Mccaffrey And In The Matter Of An Application By PSNI And Durham Constabulary For Search Warrants (2020) Ref: MOR11288. Available at: https://www.judiciaryni.uk/sites/judiciary/files/decisions/Fine%20Point%20Films%20and%20Birney,%20McCaffrey%20and%20PSNI%20and%20Durham%20Constabulary%20Applications.pdf.

Indu K and Aswatha KM (2019) A Study on Machine Learning Techniques for Internet of Things in Societal Applications. In: *2019 International Conference on Data Science and Communication (IconDSC)*, March 2019, pp. 1–6. DOI: 10.1109/IconDSC.2019.8816970.

Information Commissioner's Office (2018) The ICO's relationship with the Department for Digital, Culture Media and Sport. Available at: https://ico.org.uk/about-the-ico/who-we-are/relationship-with-the-dcms/ (accessed 28 May 2019).
Information Commissioner's Office (2019a) Data Protection Act 2018: For Organisations. Available at: https://ico.org.uk/for-organisations/data-protection-act-2018/ (accessed 28 May 2019).
Information Commissioner's Office (2019b) Data protection by design and default. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (accessed 18 February 2020).
Information Commissioner's Office (2019c) Guide to the General Data Protection Regulation (GDPR): Lawful basis for processing: Legitimate interests. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (accessed 9 September 2019).
Information Commissioner's Office and Department for Digital, Culture, Media & Sport (2018) *Information Commissioner's Office: Management Agreement 2018-2021*. London, UK: Information Commissioner's Office. Available at: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf (accessed 21 April 2020).
INSLM (2020) Independent National Security Legislation Monitor | INSLM. Available at: https://www.inslm.gov.au/ (accessed 31 December 2020).
Institute of Electrical and Electronics Engineers (IEEE) (2020) IEEE Xplore Digital Library. Available at: https://ieeexplore.ieee.org/Xplore/guesthome.jsp?utm_source=mm_link&utm_campaign=vix&utm_medium=pubs&utm_term=Xplore%20guest (accessed 14 April 2020).
International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) (2013) ISO/IEC 27002:2013. Available at: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54533.html (accessed 22 March 2020).
Internet Law Treatise (2013) Computer Fraud and Abuse Act (CFAA). Available at: https://ilt.eff.org/Computer_Fraud_and_Abuse_Act_(CFAA).html (accessed 28 October 2022).
Ireton C and Posetti J (2018) *Journalism, 'Fake News' & Disinformation: Handbook for Journalism Education and Training*. UNESCO Series on Journalism Education. UNESCO. Available at: http://unesdoc.unesco.org/images/0026/002655/265552E.pdf (accessed 9 September 2019).
Ismail N (2017) IoT boom and GDPR raise the stakes of a cyber security breach. In: *Information Age*. Available at: https://www.information-age.com/iot-gdpr-raise-stakes-cyber-security-breach-123464318/ (accessed 31 December 2020).
Ismail Y (2019) *Introductory Chapter: Internet of Things (IoT) Importance and Its Applications*. London: IntechOpen. DOI: 10.5772/intechopen.90022.
Itkin E (2020) *Don't be silly - it's only a lightbulb*. 7 August. Tel Aviv, Israel: Check Point Institute for Information Security (CPIIS) in Tel Aviv University. Available at: https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/ (accessed 3 December 2022).
Jamil S (2020) Artificial Intelligence and Journalistic Practice: The Crossroads of Obstacles and Opportunities for the Pakistani Journalists. *Journalism Practice* 0(0). Routledge: 1–23. DOI: 10.1080/17512786.2020.1788412.

Janeček V (2018) Ownership of personal data in the Internet of Things. *Computer Law & Security Review* 34(5). Elsevier Ltd.: 1039–1052.

Jayasuriya K and Cannon D (2015) State transformation and resource politics: Australia and the regional political economy. *The Pacific Review* 28(3). Routledge: 391–410. DOI: 10.1080/09512748.2015.1011211.

Johnson B and Odhner K (2021) Focus groups from home: Conducting virtual focus groups during the COVID-19 pandemic and beyond. *College & Research Libraries News*. DOI: https://doi.org/10.5860/crln.82.6.258.

Jokela T, Väätäjä H and Koponen T (2009) Mobile Journalist Toolkit: a field study on producing news articles with a mobile device. In: *Proceedings of the 13th International MindTrek Conference: Everyday Life in the Ubiquitous Era*, Tampere, Finland, 30 September 2009, pp. 45–52. MindTrek '09. Association for Computing Machinery. DOI: 10.1145/1621841.1621851.

Jones DM (2018) Intelligence and the management of national security: the post 9/11 evolution of an Australian National Security Community. *Intelligence and National Security* 33(1). Routledge: 1–20. DOI: 10.1080/02684527.2016.1259796.

Kajjo S (2020) Secondary Targets | When You Can't Punish a Journalist, Family Will Do Just Fine | VOA Special Report. *VOA News*, 21 November. Available at: https://projects.voanews.com/press-freedom/secondary-targets/ (accessed 31 December 2020).

Käll J (2020) The Materiality of Data as Property. *Harvard International Law Journal* 61: 1–11.

Kamalipour YR (ed.) (2019) *Global Communication: A Multicultural Perspective*. 3rd edition. Rowman & Littlefield Publishers.

Karp P and Taylor J (2019) Police made illegal metadata searches and obtained invalid warrants targeting journalists. Available at: http://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists (accessed 31 December 2020).

Kassam N and McGregor R (2020) *Taiwan's 2020 elections*. 7 January. Sydney, Australia: Lowy Institute. Available at: https://www.lowyinstitute.org/publications/taiwan-s-2020-elections (accessed 11 January 2020).

Kazansky B (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society* 8(1). SAGE Publications Ltd: 2053951720985557. DOI: 10.1177/2053951720985557.

Kazansky B and Milan S (2021) "Bodies not templates": Contesting dominant algorithmic imaginaries. *New Media & Society* 23(2). SAGE Publications: 363–381. DOI: 10.1177/1461444820929316.

Kebande VR, Karie NM, Michael A, et al. (2017) How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. In: *2017 IST-Africa Week Conference (IST-Africa)*, May 2017, pp. 1–10. DOI: 10.23919/ISTAFRICA.2017.8102362.

Keeble R (2019) Secret, repressive states worldwide and the threat to journalism. *Journalism* 20(1). SAGE Publications: 114–117. DOI: 10.1177/1464884918807594.

Keller N (2018a) Identify: NIST Cybersecurity Framework. Available at: https://www.nist.gov/cyberframework/identify (accessed 11 September 2020).

Keller N (2018b) The Five Functions. Available at: https://www.nist.gov/cyberframework/online-learning/five-functions (accessed 23 January 2020).

Kelly RL (2020) *Text - H.R.1668 - 116th Congress (2019-2020): IoT Cybersecurity Improvement Act of 2020*. Available at: https://www.congress.gov/bill/116th-congress/house-bill/1668/text (accessed 31 December 2020).

Kennett P (2001) *Comparative Social Policy: Theory and Research*. Buckingham; Philadelphia: Open University Press.

Kenyon M (2019) Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes. *The Citizen Lab*, 1 April. Available at: https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/ (accessed 9 September 2019).

Kercher B (2020) *An Unruly Child: A History of Law in Australia*. New York, NY, USA: Routledge.

Kerr THD (2004) Australia's Legislative Response to Terrorism: Strengthening Arbitrary Executive Power at the Expense of the Rule of Law. *Alternative Law Journal* 29(3). SAGE Publications Ltd: 131–134. DOI: 10.1177/1037969X0402900305.

Keymolen E and Hof SV der (2019) Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. *Journal of Cyber Policy* 4(2): 143–159. DOI: 10.1080/23738871.2019.1586970.

Khilji A (2019) Warrantless Searches of Electronic Devices at U.S. Borders: Securing The Nation or Violating Digital Liberty? *Catholic University Journal of Law and Technology* 27(2): 173–206.

Kielbowicz RB (2015) Regulating Timeliness: Technologies, Laws, and the News, 1840–1970. *Journalism & Communication Monographs* 17(1). SAGE Publications Inc: 5–83. DOI: 10.1177/1077699014566380.

King G, Keohane RO and Verba S (1994a) Causality and Causal Inference. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 75–114. Available at: https://www.jstor.org/stable/j.ctt7sfxj.6 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994b) Descriptive Inference. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 34–74. Available at: https://www.jstor.org/stable/j.ctt7sfxj.5 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994c) Determining What to Observe. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 115–149. Available at: https://www.jstor.org/stable/j.ctt7sfxj.7 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994d) Front Matter. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. i–iv. Available at: https://www.jstor.org/stable/j.ctt7sfxj.1 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994e) Increasing the Number of Observations. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 208–230. Available at: https://www.jstor.org/stable/j.ctt7sfxj.9 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994f) Index. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 239–247. Available at: https://www.jstor.org/stable/j.ctt7sfxj.11 (accessed 25 January 2020).

King G, Keohanne RO, Verba S, et al. (1994) Preface. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. ix–2. Available at: https://www.jstor.org/stable/j.ctt7sfxj.3 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994g) References. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 231–238. Available at: https://www.jstor.org/stable/j.ctt7sfxj.10 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994h) Table of Contents. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. v–viii. Available at: https://www.jstor.org/stable/j.ctt7sfxj.2 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994i) The Science in Social Science. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 3–33. Available at: https://www.jstor.org/stable/j.ctt7sfxj.4 (accessed 25 January 2020).

King G, Keohane RO and Verba S (1994j) Understanding What to Avoid. In: *Designing Social Inquiry*. STU-Student edition. Scientific Inference in Qualitative Research. Princeton University Press, pp. 150–207. Available at: https://www.jstor.org/stable/j.ctt7sfxj.8 (accessed 25 January 2020).

Kitchin R (2016) The ethics of smart cities and urban science. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374(2083): 20160115. DOI: 10.1098/rsta.2016.0115.

Kite J and Phongsavan P (2017) Insights for conducting real-time focus groups online using a web conferencing service. *F1000Research* 6: 122. DOI: 10.12688/f1000research.10427.1.

Kitzinger J (1995) Qualitative Research: Introducing focus groups. *BMJ* 311(7000). British Medical Journal Publishing Group: 299–302. DOI: 10.1136/bmj.311.7000.299.

Klein N (2021) Naomi Klein: how big tech helps India target climate activists. *The Guardian*, 4 March. Available at: http://www.theguardian.com/news/2021/mar/04/how-big-tech-helps-india-target-climate-activists-naomi-klein (accessed 5 March 2021).

Kleis Nielsen R, Newman N, Fletcher R, et al. (2019) *Reuters Institute Digital News Report 2019*. Oxford: Reuters Institute for the Study of Journalism (RISJ).

Kliem F (2020) Why Quasi-Alliances Will Persist in the Indo-Pacific? The Fall and Rise of the Quad. *Journal of Asian Security and International Affairs* 7(3). SAGE Publications India: 271–304. DOI: 10.1177/2347797020962620.

Knapp ED and Langill JT (2015) Chapter 7 - Hacking Industrial Control Systems. In: Knapp ED and Langill JT (eds) *Industrial Network Security (Second Edition)*. Boston: Syngress, pp. 171–207. DOI: 10.1016/B978-0-12-420114-9.00007-1.

Knaus C (2019) Witness K and the 'outrageous' spy scandal that failed to shame Australia. *The Guardian*, 9 August. Available at: http://www.theguardian.com/australia-news/2019/aug/10/witness-k-and-the-outrageous-spy-scandal-that-failed-to-shame-australia (accessed 31 December 2020).

Knight R and Nurse JRC (2020) A framework for effective corporate communication after cyber security incidents. *Computers & Security* 99: 102036. DOI: 10.1016/j.cose.2020.102036.

Kolcun R, Popescu DA, Safronov V, et al. (2020) *The case for retraining of ML models for IoT device identification at the edge*. Working Paper, 17 November. arXiv. Available at: http://spiral.imperial.ac.uk/handle/10044/1/84617 (accessed 3 June 2021).

Kolias C, Kambourakis G, Stavrou A, et al. (2017) DDoS in the IoT: Mirai and other botnets. *Computer* 50: 80–84. DOI: 10.1109/MC.2017.201.

Köllner P (2021) Australia and New Zealand recalibrate their China policies: convergence and divergence. *The Pacific Review* 34(3). Routledge: 405–436. DOI: 10.1080/09512748.2019.1683598.

Koops B-J and Leenes R (2014) Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology* 28(2): 159–171. DOI: 10.1080/13600869.2013.801589.

Kostyuk N and Landau S (2022) Dueling over Dual_EC_DRGB: The Consequences of Corrupting a Cryptographic Standardization Process. *Harvard National Security Journal* 13(2): 1–61.

Kraemer MJ, Seymour W, Binns R, et al. (2019) Informing The Future of Data Protection in Smart Homes. In: *CHI'19 Workshop on New Directions for the IoT: Automate, Share, Build, and Care*, Glasgow UK, 17 June 2019. Association for Computing Machinery. Available at: http://arxiv.org/abs/1910.01973 (accessed 31 January 2020).

Krebs B (2016a) KrebsOnSecurity Hit With Record DDoS — Krebs on Security. Available at: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (accessed 23 October 2020).

Krebs B (2016b) This is Why People Fear the 'Internet of Things'. In: *Krebs on Security*. Available at: https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/comment-page-1/#comments (accessed 31 December 2020).

Kroon RW (2010) *A/V A to Z: An Encyclopedic Dictionary of Media, Entertainment and Other Audiovisual Terms*. North Carolina: McFarland. Available at: https://www.google.com/books/edition/A_V_A_to_Z/HjmNAgAAQBAJ?hl=en&gbpv=1.

Krüger F (2017) What should journalism do in a new democracy? *Communicatio* 43(2): 23–38. DOI: 10.1080/02500167.2017.1327875.

Kurlantzick J (2019) *In Brief: How China Is Interfering in Taiwan's Election*. 7 November. New York, NY, USA: Council on Foreign Relations (CFR). Available at: https://www.cfr.org/in-brief/how-china-interfering-taiwans-election (accessed 31 December 2020).

Lambe P (2007) *Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness*. Oxford: Chandos Publishing (Oxford) Limited.

Lashmar P (2017) No More Sources? *Journalism Practice* 11(6). Routledge: 665–688. DOI: 10.1080/17512786.2016.1179587.

Lashmar P (2020) *Spies, Spin and the Fourth Estate: British Intelligence and the Media*. Edinburgh, Scotland: Edinburgh University Press.

Laughlin A (2021) How a smart home could be at risk from hackers - Which? News. *Which?*, 2 July. Available at: https://www.which.co.uk/news/article/how-the-smart-home-could-be-at-risk-from-hackers-akeR18s9eBHU (accessed 4 December 2022).

Lawler R (2015) Vizio IPO plan shows how its TVs track what you're watching. Available at: https://www.engadget.com/2015-07-24-vizio-ipo-inscape-acr.html (accessed 26 October 2020).

Lawson S (2012) Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday* 17(7). DOI: 10.5210/fm.v17i7.3848.

Layton P (2017) As China's Sphere of Influence Expands, Australia Has a Choice. In: *War on the Rocks*. Available at: https://warontherocks.com/2017/06/as-chinas-sphere-of-influence-expands-australia-has-a-choice/ (accessed 1 January 2021).

Lee Y (2019) Taiwan has 'urgent' need for infiltration law in face of China - president. *Reuters*, 27 December. Available at: https://uk.reuters.com/article/uk-taiwan-election-idUKKBN1YV141 (accessed 31 December 2020).

Levinson C (2021) Senior Israeli Security Official Reveals State Secrets as He Runs, Bikes. *Haaretz*, 17 December. Israel. Available at: https://www.haaretz.com/israel-news/2021-12-17/ty-article/shin-bet-

bodyguard-broadcasts-state-secrets-as-he-runs-bikes-off-hours/0000017f-e389-d568-ad7f-f3ebb69e0000 (accessed 5 December 2022).
Levy I (2017) Hacked doll 'could open front door'. *BBC News*, 14 February. Available at: https://www.bbc.co.uk/news/av/technology-38966285 (accessed 13 September 2020).
Levy I (2022) Scanning the internet for fun and profit. Available at: https://www.ncsc.gov.uk/blog-post/scanning-the-internet-for-fun-and-profit (accessed 15 November 2022).
Levy K and Schneier B (2020) Privacy threats in intimate relationships. *Journal of Cybersecurity* 6(1). Oxford Academic. DOI: 10.1093/cybsec/tyaa006.
Levy Y and Ellis TJ (2006) A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: The International Journal of an Emerging Transdiscipline* 9: 181–212. DOI: 10.28945/479.
Lewis J (2018) Fitness-Tracker App Exposes Security Flaw at Taiwan's Missile Command Center. *The Daily Beast*, 29 January. Available at: https://www.thedailybeast.com/strava-fitness-tracker-app-exposes-taiwans-missile-command-center (accessed 31 December 2020).
Lewis SC and Westlund O (2015a) Actors, Actants, Audiences, and Activities in Cross-Media News Work. *Digital Journalism* 3(1). Routledge: 19–37. DOI: 10.1080/21670811.2014.927986.
Lewis SC and Westlund O (2015b) Big Data and Journalism. *Digital Journalism* 3(3). Routledge: 447–466. DOI: 10.1080/21670811.2014.976418.
Li C and Palanisamy B (2019) Privacy in Internet of Things: From Principles to Technologies. *IEEE Internet of Things Journal* 6(1): 488–505. DOI: 10.1109/JIOT.2018.2864168.
Lin L (2018) Reuters Institute Digital News Report: Taiwan. Available at: https://www.digitalnewsreport.org/survey/2018/taiwan-2018/ (accessed 31 December 2020).
Lindqvist J (2018) New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International Journal of Law and Information Technology* 26(1): 45–63. DOI: 10.1093/ijlit/eax024.
Lindsay G, Woods B and Corman J (2016) *Issue Brief: Smart Homes and the Internet of Things*. March. Washington, D.C.: The Atlantic Council: the Brent Scowcroft Center on International Security. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2016/03/Smart_Homes_0317_web.pdf (accessed 28 March 2022).
Lisosky JM and Henrichsen JR (2011) *War on Words: Who Should Protect Journalists?* Washington, USA: Praeger.
Liu F and Li T (2018) A Clustering K-Anonymity Privacy-Preserving Method for Wearable IoT Devices. *Security and Communication Networks* Volume 2018: 8. DOI: https://doi.org/10.1155/2018/4945152.
Liu S (2020) Internet of Things (IoT) - Statistics & Facts. Available at: https://www.statista.com/topics/2637/internet-of-things/ (accessed 17 September 2020).
Liverpool L (2020) Voice assistant recordings could reveal what someone nearby is typing. *New Scientist*, 4 December. Available at: https://www.newscientist.com/article/2261844-voice-assistant-recordings-could-reveal-what-someone-nearby-is-typing/ (accessed 1 January 2021).
Lobe B and Morgan DL (2021) Assessing the effectiveness of video-based interviewing: a systematic comparison of video-conferencing based dyadic interviews and focus groups. *International Journal of Social Research Methodology* 24(3). Routledge: 301–312. DOI: 10.1080/13645579.2020.1785763.

Lochmiller C (2021) Conducting Thematic Analysis with Qualitative Data. *The Qualitative Report* 26(6): 2029–2044. DOI: 10.46743/2160-3715/2021.5008.

Lomas N (2020) Mass surveillance for national security does conflict with EU privacy rights, court advisor suggests. In: *TechCrunch*. Available at: https://social.techcrunch.com/2020/01/15/mass-surveillance-for-national-security-does-conflict-with-eu-privacy-rights-court-advisor-suggests/ (accessed 3 August 2020).

Lopez J, Rios R, Bao F, et al. (2017) Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems* 75: 46–57. DOI: 10.1016/j.future.2017.04.045.

Lopez-Neira I, Patel T, Parkin S, et al. (2019) *'Internet of Things': How Abuse is Getting Smarter*. ID 3350615, SSRN Scholarly Paper, 11 March. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.3350615.

Lowenthal T (2015) Surveillance forces journalists to think and act like spies. Available at: https://cpj.org/2015/04/attacks-on-the-press-surveillance-forces-journalists-to-think-act-like-spies.php (accessed 9 September 2019).

Ludvigsen KR, Nagaraja S and Daly A (2022) Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis. In: *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*, New York, NY, USA, 8 November 2022, pp. 25–34. SCORED'22. Association for Computing Machinery. DOI: 10.1145/3560835.3564552.

Lyon D (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham England ; Philadelphia: Open University Press.

Lyon D (2007) *Surveillance Studies: An Overview*. Cambridge, UK ; Malden, MA: Polity Press.

Lyon D (2018) *The Culture of Surveillance: Watching as a Way of Life*. 1st ed. Cambridge, UK: Polity Press. Available at: https://www.wiley.com/en-us/The+Culture+of+Surveillance%3A+Watching+as+a+Way+of+Life-p-9780745671734 (accessed 28 May 2019).

Lyons J (2019) AFP raid on ABC reveals investigative journalism being put in same category as criminality. *ABC News*, 15 July. Available at: https://www.abc.net.au/news/2019-07-15/abc-raids-australian-federal-police-press-freedom/11309810 (accessed 31 December 2020).

Magcamit MI (2015) Games, Changes and Fears: Exploring Taiwan's Cross-Strait Dilemma in the Twenty-first Century. *Journal of Asian Security and International Affairs* 2(1). SAGE Publications India: 92–115. DOI: 10.1177/2347797014565297.

Magcamit MI and Tan AC (2015) Crouching tiger, lurking dragon: understanding Taiwan's sovereignty and trade linkages in the twenty-first century. *International Relations of the Asia-Pacific* 15(1): 81–112. DOI: 10.1093/irap/lcu013.

Mahalle PN, Thakre PA, Prasad NR, et al. (2013) A fuzzy approach to trust based access control in internet of things. In: *Wireless VITAE 2013*, June 2013, pp. 1–5. DOI: 10.1109/VITAE.2013.6617083.

Mahase E (2019) Kashmir communications blackout is putting patients at risk, doctors warn. *BMJ* 366. British Medical Journal Publishing Group: l5204. DOI: 10.1136/bmj.l5204.

Mahler J and Rutenberg J (2019) How Rupert Murdoch's Empire of Influence Remade the World. *The New York Times*, 3 April.

Mahr A, Cichon M, Mateo S, et al. (2021) Zooming into the pandemic! A forensic analysis of the Zoom Application. *Forensic Science International: Digital Investigation* 36: 301107. DOI: 10.1016/j.fsidi.2021.301107.

Mai V and Khalil I (2017) Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. *Future Generation Computer Systems* 72: 327–338. DOI: 10.1016/j.future.2016.06.003.

Maiti A and Jadliwala M (2018) *Light Ears: Information Leakage via Smart Lights*. 23 August. University of Texas at San Antonio: arXiv:1808.07814 [cs]. Available at: http://arxiv.org/abs/1808.07814 (accessed 9 September 2019).

Malina L, Srivastava G, Dzurenda P, et al. (2019) A Privacy-Enhancing Framework for Internet of Things Services. In: *Network and System Security* (eds JK Liu and X Huang), Cham, 2019, pp. 77–97. Lecture Notes in Computer Science. Springer International Publishing. DOI: 10.1007/978-3-030-36938-5_5.

Mandalari AM, Dubois DJ, Kolcun R, et al. (2021) *Blocking without breaking: identification and mitigation of non-essential IoT traffic*. Working Paper, 11 May. arXiv. Available at: http://spiral.imperial.ac.uk/handle/10044/1/88830 (accessed 3 June 2021).

Mann M, Daly A and Molnar A (2020) Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications. *Internet Policy Review* 9(3). Available at: https://policyreview.info/articles/analysis/regulatory-arbitrage-and-transnational-surveillance-australias-extraterritorial (accessed 16 November 2022).

Mann S (2016) Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself). In: *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Toronto, Ontario, Canada, June 2016, pp. 1408–1417. IEEE Computer Society. DOI: 10.1109/CVPRW.2016.177.

Manokha I (2020) The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace. *Surveillance & Society* 18(4): 540–554. DOI: 10.24908/ss.v18i4.13776.

Manthorpe R (2020) Coronavirus: Police planning their own contact tracing system over concerns about government's version. *Sky News*, 5 June. UK. Available at: https://news.sky.com/story/coronavirus-police-fear-govts-contact-tracing-scheme-could-endanger-officers-12000761 (accessed 1 January 2021).

Maple C (2017) Security and privacy in the internet of things. *Journal of Cyber Policy* 2(2): 155–184. DOI: 10.1080/23738871.2017.1366536.

Marczak B, Scott-Railton J, Senft A, et al. (2018) *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*. Citizen Lab Research Report No. 115, 1 October. The Citizen Lab: University of Toronto. Available at: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/ (accessed 12 April 2022).

Mare S, Roesner F and Kohno T (2020) Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020(2): 436–458. DOI: 10.2478/popets-2020-0035.

Marques ICDS, Theiss LM, Johnson CY, et al. (2021) Implementation of virtual focus groups for qualitative data collection in a global pandemic. *The American Journal of Surgery* 221(5). Elsevier: 918–922. DOI: 10.1016/j.amjsurg.2020.10.009.

Martin A, Rashid A, Chivers H, et al. (2021) The Cyber Security Body of Knowledge v1.1.0, 2021. University of Bristol. Available at: https://www.cybok.org/.

Massey OT (2011) A proposed model for the analysis and interpretation of focus groups in evaluation research. *Evaluation and Program Planning* 34(1): 21–28. DOI: 10.1016/j.evalprogplan.2010.06.003.

Mathews Hunt K (2018) *consumeR-IOT: where every thing collides Promoting consumer internet of things protection in Australia.* Faculty of Law. Bond University, Robina, Gold Coast, Queensland. Available at:

https://research.bond.edu.au/en/studentTheses/consumer-iot-where-every-thing-collides-promoting-consumer-intern (accessed 23 April 2021).
Mauldin W (2020) Voice of America Director Resigns After Clashing With Trump Administration. *Wall Street Journal*, 15 June. Available at: https://www.wsj.com/articles/voice-of-america-director-resigns-after-clashing-with-trump-administration-11592259031 (accessed 31 December 2020).
Mayhew F (2019) Youtube downs Bellingcat channel for four hours without warning. In: *Press Gazette*. Available at: https://pressgazette.co.uk/youtube-downs-bellingcat-channel-for-four-hours-without-warning/ (accessed 3 March 2020).
McGregor S (2016) Why DDoS attacks matter for journalists. Available at: https://www.cjr.org/tow_center/journalists_ddos_hack_passwords.php (accessed 15 November 2020).
McGregor S, Roesner F and Caine K (2016) Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proceedings on Privacy Enhancing Technologies* 2016. DOI: 10.1515/popets-2016-0048.
McGregor SE (2021) *Information Security Essentials*. 1st ed. New York, NY, USA: Columbia University Press.
McGregor SE and Watkins EA (2016) "Security by Obscurity": Journalists' Mental Models of Information Security. *#ISOJ* 6(1). The Multimedia Edition of the Official Research Journal of the International Symposium on Online Journalism. Available at: https://isojjournal.wordpress.com/2016/04/14/security-by-obscurity-journalists-mental-models-of-information-security/ (accessed 15 February 2020).
McGregor SE, Charters P, Holliday T, et al. (2015) Investigating the Computer Security Practices and Needs of Journalists. In: *Proceedings of the 24th USENIX Security Symposium*, Washington, D.C., 12 August 2015, p. 17. USENIX Association.
McGregor SE, Watkins EA, Al-Ameen MN, et al. (2017) When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. In: *Proceedings of the 26th USENIX Security Symposium*, Vancouver, BC, Canada, 16 August 2017, p. 19. USENIX Association. Available at: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-mcgregor.pdf.
McLaughlin J (2016) NSA Looking to Exploit Internet of Things, Including Biomedical Devices, Official Says. In: *The Intercept*. Available at: https://theintercept.com/2016/06/10/nsa-looking-to-exploit-internet-of-things-including-biomedical-devices-official-says/ (accessed 26 October 2020).
McMillan R and Knutson R (2017) Yahoo Triples Estimate of Breached Accounts to 3 Billion. *Wall Street Journal*, 4 October. Available at: https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804 (accessed 28 May 2019).
McPherson E, Guenette Thornton I and Mahmoudi M (2020) Open Source Investigations and the Technology-Driven Knowledge Controversy in Human Rights Fact-Finding. In: Dubberley S, Koenig A, and Murray D (eds) *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. UK: Oxford University Press. DOI: 10.17863/CAM.36709.
McStay A (2017) *Privacy and the Media*. London: SAGE.
MEAA (2019) Journalist Information Warrants. Available at: https://pressfreedom.org.au/journalist-information-warrants-d47b402ae071 (accessed 31 December 2020).
Medaglia CM and Serbanati A (2010) An Overview of Privacy and Security Issues in the Internet of Things. In: *The Internet of Things* (eds D Giusto, A Iera, G Morabito, et al.), New York, NY, 2010, pp. 389–395. Springer. DOI: 10.1007/978-1-4419-1674-7_38.

Media Freedom Coalition (2022) Coalition Objectives. Available at: https://mediafreedomcoalition.org/about/objectives/coalition-objectives (accessed 13 September 2022).

Menary J, Stetkiewicz S, Nair A, et al. (2021) Going virtual: adapting in-person interactive focus groups to the online environment. *Emerald Open Research*. DOI: 10.35241/emeraldopenres.14163.2.

Meteriz Ü, Fazıl Yıldıran N, Kim J, et al. (2020) Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In: *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, November 2020, pp. 464–473. DOI: 10.1109/ICDCS47774.2020.00063.

Michel MCK and King MC (2019) Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In: *2019 IEEE International Symposium on Technology and Society (ISTAS)*, Medford, MA, USA, 15 November 2019, pp. 1–7. IEEE. DOI: 10.1109/ISTAS48451.2019.8938009.

Michéle B and Karpow A (2014) Watch and be watched: Compromising all Smart TV generations. In: *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, January 2014, pp. 351–356. IEEE. DOI: 10.1109/CCNC.2014.6866594.

Middleton L (2020) Woman 'hacked into ex-boyfriend's Alexa and told his new girlfriend to leave'. *Metro*, 12 October. Available at: https://metro.co.uk/2020/10/12/woman-hacked-into-ex-boyfriends-alexa-and-told-his-new-girlfriend-to-leave-13407458/ (accessed 19 October 2020).

Mignerat M, Mirabeau L and Proulx K (2019) Autonomous Strategic Behaviours and Institutional Pressures: the case of BYOD. *Systèmes d'Information et Management (French Journal of Management Information Systems)* 24(2): 7–46. DOI: 10.9876/sim.v24i2.900.

Miller C and Taylor H (2017) Can economic interests trump ethnic hostility? Trading ties versus outgroup hostility in Australian perceptions of China as a security threat. *International Relations of the Asia-Pacific* 17(1): 67–99. DOI: 10.1093/irap/lcw001.

Miller KW, Voas J and Hurlburt GF (2012) BYOD: Security and Privacy Considerations. *IT Professional* 14(5): 53–55. DOI: 10.1109/MITP.2012.93.

Mills A and Sarikakis K (2016) Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism. *Big Data & Society* 3(2): 2053951716669381. DOI: 10.1177/2053951716669381.

Mills A, Durepos G and Wiebe E (eds) (2010) Comparative Case Study. In: *Encyclopedia of Case Study Research*. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. DOI: 10.4135/9781412957397.n64.

Mills J, Pellanda E and Pase A (2017) New Interactions. *Journalism Practice* 11(8). Routledge: 980–999. DOI: 10.1080/17512786.2016.1224679.

Milosavljević M and Vobič I (2019) 'Our task is to demystify fears': Analysing newsroom management of automation in journalism. *Journalism*. SAGE Publications: 1464884919861598. DOI: 10.1177/1464884919861598.

Milosavljević M, Amon Prodnik J and Kučić LJ (2015) Securing the Communication of Journalists with their Sources as a Form of Source Protection – Editorial Policy of Slovenian Media Regarding Communication and Technology. *Teorija in praksa* 52(4): 612–630.

Minda News (2019) STATEMENT: DDoS attacks on NUJP, alternative media continue. *MindaNews*, 11 February. Available at: https://www.mindanews.com/statements/2019/02/statement-ddos-attacks-on-nujp-alternative-media-continue/ (accessed 4 March 2020).

Minerva R, Biru A and Rotondi D (2015) *Towards a definition of the Internet of Things (IoT)*. IEEE Internet Initiative, 27 May. IEEE. Available at: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed 9 September 2019).

Minshall K, Geoghegan R and Rex H (2015) Policing and the Internet of Things | Tech UK. Available at: https://www.techuk.org/index.php?option=com_techuksecurity&task=security.download&file=Policing_and_IOT_Digital_FINAL.pdf&id=10985&Itemid=177&return=aHR0cDovL3d3dy50ZWNodWsub3JnL2luc2lnaHRzL25ld3MvaXRlbS8xMDk4NS1vcHBvcnR1bml0aWVzLW91dHdlaWdoLXRoZS1jaGFsbGVuZ2VzLXBvc2VkLWJ5LXRoZS1pbnRlcm5ldC1vZi10aGluZ3MtaW4tcG9saWNpbg== (accessed 9 August 2019).

Miorandi D, Sicari S, De Pellegrini F, et al. (2012) Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10(7): 1497–1516. DOI: 10.1016/j.adhoc.2012.02.016.

Missel R (2019) This Runner Is a Hitman. His GPS Watch Tied Him to a Mob Boss Murder. Available at: https://www.runnersworld.com/news/a25924256/mark-fellows-runner-hitman-murder/ (accessed 9 September 2019).

Mitchell P, Rowley L, Sherman J, et al. (2022) *Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem*. 26 September. Washington, D.C.: The Atlantic Council's Cyber Statecraft Initiative, under the Digital Forensic Research Lab (DFRLab). Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/ (accessed 24 October 2022).

Mohamad Noor M binti and Hassan WH (2019) Current research on Internet of Things (IoT) security: A survey. *Computer Networks* 148: 283–294. DOI: 10.1016/j.comnet.2018.11.025.

Molloy S (2019a) Woman's chilling hidden camera discovery. *Daily Mercury*, 25 June. Available at: https://www.dailymercury.com.au/news/womans-chilling-hidden-camera-discovery/3762755/ (accessed 31 December 2020).

Molloy S (2019b) World's media condemns police raids of the ABC and Annika Smethurst's home as 'attack on press freedom'. *Australasian Policing*. Available at: https://search.informit.org/doi/abs/10.3316/informit.614688793653346 (accessed 23 April 2021).

Monteiro M (2019) *Ruined by Design: How Designers Destroyed the World, and What We Can Do to Fix It*.

Moody G (2020) The enemy within: welcome to the Internet of gaslighting. Available at: https://www.privateinternetaccess.com/blog/the-enemy-within-welcome-to-the-internet-of-gaslighting/ (accessed 11 September 2020).

Moore A (2022) 'I didn't want it anywhere near me': how the Apple AirTag became a gift to stalkers. *The Guardian*, 5 September. Available at: https://www.theguardian.com/technology/2022/sep/05/i-didnt-want-it-anywhere-near-me-how-the-apple-airtag-became-a-gift-to-stalkers (accessed 15 September 2022).

Morabito V (2015) *Big Data and Analytics: Strategic and Organizational Impacts*. New York, NY: Springer Berlin Heidelberg. Available at: http://index-of.co.uk/Big-Data-Technologies/Big%20Data%20and%20Analytics%20-%20bb.pdf.

Morlino L, Dressel B and Pelizzo R (2011) The Quality of democracy in Asia-Pacific: issues and findings. *International Political Science Review* 32(5). SAGE Publications Ltd: 491–511. DOI: 10.1177/0192512111418334.

Morris S (2019) Facial recognition tech prevents crime, police tell UK privacy case. *The Guardian*, 22 May. Available at: https://www.theguardian.com/technology/2019/may/22/facial-recognition-prevents-crime-police-tell-uk-privacy-case (accessed 28 May 2019).

Morrow B (2012) BYOD security challenges: control and protect your most sensitive data. *Network Security* 2012(12): 5–8. DOI: 10.1016/S1353-4858(12)70111-3.

Motta RC, de Oliveira KM and Travassos GH (2018) On challenges in engineering IoT software systems. In: *Proceedings of the XXXII Brazilian Symposium on Software Engineering*, Sao Carlos, Brazil, 17 September 2018, pp. 42–51. SBES '18. Association for Computing Machinery. DOI: 10.1145/3266237.3266263.

Mountrouidou X, Billings B and Mejia-Ricart L (2019) Not just another Internet of Things taxonomy: A method for validation of taxonomies. *Internet of Things* 6: 100049. DOI: 10.1016/j.iot.2019.03.003.

Mozilla Foundation (2021) *Privacy Not Included: A Buyer's Guide for Connected Products. Available at: https://foundation.mozilla.org/en/privacynotincluded/ (accessed 7 June 2021).

Mulligan C (2015) Personal Property Servitudes on the Internet of Things. *Georgia Law Review* 50(4): 1121–1168.

Murray-Rust D, O'Hara K and Oswald M (2015) Privacy by obfuscation: Possibilities and constraints. *The Economics of Surveillance: A Web Science Workshop on Critical Exploration of Data Practices, Consumer Rights and the Future of Digital Economies*: 6.

Mythen G (2010) Reframing risk? Citizen journalism and the transformation of news. *Journal of Risk Research* 13(1). Routledge: 45–58. DOI: 10.1080/13669870903136159.

Nakashima R (2018) AP Exclusive: Google tracks your movements, like it or not. *AP NEWS*, 13 August. Available at: https://apnews.com/828aefab64d4411bac257a07c1af0ecb (accessed 9 September 2019).

Nascimento DR, Ciano MP, Gumz J, et al. (2022) The acceptance process of smart homes by users: a statistical meta-analysis. *Behaviour & Information Technology* 0(0). Taylor & Francis: 1–18. DOI: 10.1080/0144929X.2022.2146534.

Nassi B, Bitton R, Masuoka R, et al. (2021) SoK: Security and Privacy in the Age of Commercial Drones. In: *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 73–90. IEEE Computer Society. DOI: 10.1109/SP40001.2021.00005.

National Cyber Security Centre (NCSC) (2016) BYOD: Executive Summary. Available at: https://www.ncsc.gov.uk/guidance/byod-executive-summary (accessed 17 February 2020).

National Cyber Security Centre (NCSC) (2018) End user device (EUD) security guidance. Available at: https://www.ncsc.gov.uk/collection/end-user-device-security (accessed 17 February 2020).

National Cyber Security Centre (NCSC) (2020) NCSC advice on the use of equipment from high risk vendors in UK telecoms networks. Available at: https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks (accessed 24 February 2020).

National Cyber Security Centre (NCSC) (2022) NCSC Scanning information. Available at: https://www.ncsc.gov.uk/information/ncsc-scanning-information (accessed 15 November 2022).

National Institute of Standards and Technology (2004) *Standards for security categorization of federal information and information systems*. NIST FIPS 199, February. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.FIPS.199.

National Institute of Standards and Technology (2006) *Minimum security requirements for federal information and information systems*. NIST FIPS 200, March. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.FIPS.200.

National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018, 16 April. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.04162018.

National Institute of Standards and Technology (2020) *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. 16 January. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf (accessed 28 January 2020).

National Institute of Standards and Technology (NIST) (2021a) countermeasures - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/countermeasures (accessed 13 October 2021).

National Institute of Standards and Technology (NIST) (2021b) information security - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/information_security (accessed 11 November 2021).

National Institute of Standards and Technology (NIST) (2021c) mitigate - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/mitigate (accessed 13 October 2021).

National Institute of Standards and Technology (NIST) (2021d) privacy - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/privacy (accessed 11 November 2021).

National Institute of Standards and Technology (NIST) (2021e) protection - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/protection (accessed 13 October 2021).

National Institute of Standards and Technology (NIST) (2022a) Internet of Things (IoT) - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/internet_of_things_IoT (accessed 11 May 2022).

National Institute of Standards and Technology (NIST) (2022b) security - Glossary | CSRC. Available at: https://csrc.nist.gov/glossary/term/security (accessed 28 April 2022).

National Security Agency (2020) *Limiting Location Data Exposure*. National Security Agency | Cybersecurity Information U/OO/155603-20 | PP-20-0535, August. USA: National Security Agency. Available at: https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF (accessed 11 September 2020).

Nawir M, Amir A, Yaakob N, et al. (2016) Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, August 2016, pp. 321–326. IEEE. DOI: 10.1109/ICED.2016.7804660.

NCC Group (2021) UK government announces plans for new IoT security law. In: *NCC Newsroom*. Available at: https://newsroom.nccgroup.com/news/uk-government-announces-plans-for-new-iot-security-law-425797 (accessed 23 April 2021).

Neate R and correspondent RNW (2022) Senior media figures call for law to stop oligarchs silencing UK journalists. *The Guardian*, 29 November. Available at: https://www.theguardian.com/news/2022/nov/29/slapps-senior-media-figures-call-for-law-stop-oligarchs-silencing-uk-journalists (accessed 21 December 2022).

New York Academy of Medicine (1999) What is Grey Literature? | Grey Literature Database. Available at: https://greylit.org/about (accessed 21 March 2020).

New York Desk (2021) America grapples with regulating surveillance technology. *The Economist*, 9 March. Available at: https://www.economist.com/united-states/2021/03/09/america-grapples-with-regulating-surveillance-technology (accessed 23 March 2021).

Newman LH (2016) What We Know About Friday's Massive East Coast Internet Outage. *Wired*, 21 October. Available at: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ (accessed 9 September 2019).

Newton C (2020) 'Instagram can hurt us': Mark Zuckerberg emails outline plan to neutralize competitors. Available at: https://www.theverge.com/2020/7/29/21345723/facebook-instagram-documents-emails-mark-zuckerberg-kevin-systrom-hearing (accessed 3 August 2020).

Nisbett MJ, Lee D, Hesmondhalgh D, et al. (2015) *Culture, Economy and Politics: The Case of New Labour*. Palgrave Macmillan. Available at: https://kclpure.kcl.ac.uk/portal/en/publications/culture-economy-and-politics-the-case-of-new-labour(c6305a5f-921f-49c1-868a-ead3f83a079b).html (accessed 9 September 2019).

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. 1 edition. Stanford, Calif: Stanford University Press.

NIST Joint Task Force Transformation Initiative (2012) *Guide for conducting risk assessments*. 0 ed. NIST SP 800-30r1. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-30r1.

NIST Joint Task Force Transformation Initiative (2015) *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication (SP) 800-53 Rev. 4, 22 January. Gaithersburg, MD: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-53r4.

Noble SU (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

Noguera J and Morcillo L (2012) *The Future of Non-Metropolitan Regions in the European Union: A Member-State Comparative Report*. European Development Opportunities for Rural Areas (EDORA). Spain: Universitat de València.

Noorlander MP (2020) *Background paper on the implementation of CM/rec(2016)4 on the safety of journalists and other media actors, for the Conference of Ministers responsible for Media and Information Society (Nicosia, Cyprus, May 2020)*. May. Council of Europe, Avenue de l'Europe F-67075 Strasbourg Cedex, France: Council of Europe. Available at: https://rm.coe.int/background-paper-safety-of-journalists-and-other-media-actorsfinal/168094b396 (accessed 11 September 2020).

Norman TL (2010) Physical security risk and countermeasures: Effectiveness metrics. *CSO Online*, 22 February. Available at: https://www.csoonline.com/article/2124831/physical-security-risk-and-countermeasures-effectiveness-metrics.html (accessed 13 October 2021).

Northern Ireland Desk (2020) Loughinisland: Journalists search warrants wrongly obtained. *BBC News*, 10 July. Available at: https://www.bbc.com/news/uk-northern-ireland-53367027 (accessed 31 December 2020).

Noto La Diega G (2016) Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom. *Journal of Law & Economic Regulation* 9(1): 69–93.

Nott L (2019) Across Global Elections, Social Media Spreads Political Propaganda and Disinformation | Freedom Forum Institute. Available at: https://www.freedomforuminstitute.org/2019/05/23/across-

global-elections-social-media-spreads-political-propaganda-and-disinformation/ (accessed 28 May 2019).

Noura M, Atiquzzaman M and Gaedke M (2019) Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Networks and Applications* 24(3): 796–809. DOI: 10.1007/s11036-018-1089-9.

Nthala N (2019) *Home data security decisions*. http://purl.org/dc/dcmitype/Text. University of Oxford, Oxford, United Kingdom. Available at: https://ora.ox.ac.uk/objects/uuid:72401f07-d923-4448-af20-f99ecb677e3a (accessed 9 August 2022).

Nurse J, Erola A, Agrafiotis I, et al. (2015) Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things. In: *Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT)*, Vienna, Austria, 21 September 2015. DOI: 10.1109/SIOT.2015.10.

Nurse J, Williams M and Creese S (2016) The Perfect Storm: The Privacy Paradox and the Internet-of-Things. In: *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, 31 September 2016. IEEE. DOI: 10.1109/ARES.2016.25.

Nurse JRC, Atamli A and Martin A (2016) Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home. In: *HAS 2016: Human Aspects of Information Security, Privacy, and Trust* (ed. T Tryfonas), Cham, 2016, pp. 255–267. Lecture Notes in Computer Science. Springer International Publishing. DOI: 10.1007/978-3-319-39381-0_23.

Nurse JRC, Creese S and De Roure D (2017) Security Risk Assessment in Internet of Things Systems. *IT Professional* 19(5): 20–26. DOI: 10.1109/MITP.2017.3680959.

Nurse JRC, Radanliev P, Creese S, et al. (2018) If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems. In: *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK, 2018, p. 1 (9 pp.)-1 (9 pp.). Institution of Engineering and Technology. DOI: 10.1049/cp.2018.0001.

NVivo (2021) Using NVivo. Available at: https://help-nv.qsrinternational.com/12/mac/v12.1.98-d3ea61/Content/concepts-strategies/using-nvivo-for-qualitative-research.htm?_ga=2.208752986.975483198.1583162118-1098817361.1582235989 (accessed 10 February 2021).

OECD (2020) Country profiles: regional facts and figures - OECD. Available at: https://www.oecd.org/regional/regional-policy/country-profiles.htm (accessed 31 December 2020).

Okoli C (2015) A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems* 37(1). DOI: 10.17705/1CAIS.03743.

Oliver J (2018) Journalism schools still behind on cybersecurity training, new survey finds. Available at: https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php (accessed 15 November 2020).

O'Neil C (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. First edition. New York: Crown.

Online Trust Alliance (2018) *OTA IoT Trust Framework*. 22 May. USA: Internet Society. Available at: https://www.internetsociety.org/iot/trust-framework/ (accessed 7 June 2021).

Onosé C (2020) Designing for Consumer Trust in a Data-Powered World. *IEEE Consumer Electronics Magazine* 9(2): 89–93. DOI: 10.1109/MCE.2019.2954561.

Opentopia (2019) Live Streaming Web Cam Views from Around the World. Available at: http://www.opentopia.com/ (accessed 9 September 2019).

Orlik A and Veldkamp L (2014) Understanding Uncertainty Shocks and the Role of Black Swans. Working Paper Series 20445, Working Paper. National Bureau of Economic Research. DOI: 10.3386/w20445.

O'Shea L (2019) *Future Histories: What Ada Lovelace, Tom Paine, and the Paris Commune Can Teach Us about Digital Technology*. London ; New York: Verso.

OWASP (2016) Top 10 2014-I4 Lack of Transport Encryption - OWASP. Available at: https://wiki.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption (accessed 27 February 2020).

Owens K, Gunawan J, Choffnes D, et al. (2022) Exploring Deceptive Design Patterns in Voice Interfaces. In: *2022 European Symposium on Usable Security*, Karlsruhe Germany, 29 September 2022, pp. 64–78. ACM. DOI: 10.1145/3549015.3554213.

Pallone F, McMorris Rodgers C and Wicker R (2022) *American Data Privacy and Protection Act*. H.R. 8152. Available at: https://www.commerce.senate.gov/services/files/6CB3B500-3DB4-4FCC-BB15-9E6A52738B6C (accessed 15 November 2022).

Palmer D (2020) Rogue IoT devices are putting your network at risk from hackers | ZDNet. Available at: https://www.zdnet.com/google-amp/article/rogue-iot-devices-are-putting-your-network-at-risk-from-hackers/ (accessed 11 September 2020).

Park S, Won DD, Lee BJ, et al. (2020) A mountable toilet system for personalized health monitoring via the analysis of excreta. *Nature Biomedical Engineering* 4(6). 6. Nature Publishing Group: 624–635. DOI: 10.1038/s41551-020-0534-9.

Parker A and Tritter J (2006) Focus group method and methodology: current practice and recent debate. *International Journal of Research & Method in Education* 29(1). Routledge: 23–37. DOI: 10.1080/01406720500537304.

Parker B (2020) EXCLUSIVE: The cyber attack the UN tried to keep under wraps. Available at: https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack (accessed 2 March 2020).

Parliament of Australia (2011) *Cybercrime Legislation Amendment Bill 2011*. Bills Digest no. 31 2011–12. Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1112a/12bd031#_Toc301448354 (accessed 31 December 2020).

Parliament of Australia (2012) *Cybercrime Legislation Amendment Act 2012*. No. 120, 2012-C2012A00120. Attorney-General's Department. Available at: https://www.legislation.gov.au/Details/C2012A00120/Html/Text, http://www.legislation.gov.au/Details/C2012A00120 (accessed 31 December 2020).

Parliament of the United Kingdom (1998) *Data Protection Act 1998: Chapter 29*. London: The Stationery Office.

Parliament of the United Kingdom (2000) *Regulation of Investigatory Powers Act 2000: Part III: Power to require disclosure: Section 50: Effect of notice imposing disclosure requirement.* 2000 c. 23. Statute Law Database. Available at: https://www.legislation.gov.uk/ukpga/2000/23/section/50 (accessed 31 December 2020).

Parliament of the United Kingdom (2016) *Investigatory Powers Act 2016: Part 5: Equipment interference*. 2016 c. 25. Queen's Printer of Acts of Parliament. Available at: https://www.legislation.gov.uk/ukpga/2016/25/part/5/enacted (accessed 31 December 2020).

Parliament of the United Kingdom (2018) *Data Protection Act 2018: Chapter 12*. London: The Stationery Office. Available at: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (accessed 28 May 2019).

Parra Rodriguez JD, Schreckling D and Posegga J (2016) Addressing Data-Centric Security Requirements for IoT-Based Systems. In: *2016 International Workshop on Secure Internet of Things (SIoT)*, September 2016, pp. 1–10. DOI: 10.1109/SIoT.2016.007.

Patel C and Doshi N (2019) Security Challenges in IoT Cyber World. In: Hassanien AE, Elhoseny M, Ahmed SH, et al. (eds) *Security in Smart Cities: Models, Applications, and Challenges*. Lecture Notes in Intelligent Transportation and Infrastructure. Cham: Springer International Publishing, pp. 171–191. DOI: 10.1007/978-3-030-01560-2_8.

Patel P (2022) *National Security Bill - Parliamentary Bills - UK Parliament*. Bill 165 2022-23. Available at: https://bills.parliament.uk/bills/3154 (accessed 15 November 2022).

Paterson C (2003) Prospects for a democratic information Society: The news agency stranglehold on global political discourse. In: *Presented to the EMTEL: New Media, Technology and Everyday Life in Europe Conference*, London, UK, 23 April 2003. London School of Economics and Political Science. Available at: https://www.lse.ac.uk/media@lse/research/EMTEL/Conference/papers/Paterson.pdf.

Paul K (2019) Teen claims to tweet from her smart fridge – but did she really? *The Guardian*, 13 August. Available at: https://www.theguardian.com/technology/2019/aug/13/teen-smart-fridge-twitter-grounded (accessed 9 September 2019).

Pavur J and Knerr C (2019) GDPArrrrr: Using Privacy Laws to Steal Identities. In: *Blackhat USA 2019 Whitepaper*, Las Vegas, 2019, p. 10. Blackhat USA. Available at: https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf.

Pearson M and Galvin C (2019) The Australian Parliament and press freedom in an international context. *Pacific Journalism Review* 13(2). Pacific Media Centre. DOI: 10.24135/pjr.v13i2.910.

Pegg D, Lewis P, Safi M, et al. (2021) FT editor among 180 journalists identified by clients of spyware firm. *The Guardian*, 20 July. Available at: https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware (accessed 12 April 2022).

PEN American Center (2013) *Chilling effects: NSA surveillance drives U.S. writers to self-censor*. 12 November. New York, NY, USA: PEN American Center and The FDR Group. Available at: https://pen.org//sites/default/files/Chilling%20Effects_PEN%20American.pdf (accessed 27 February 2020).

Perera C, Ranjan R, Wang L, et al. (2015) Big Data Privacy in the Internet of Things Era. *IT Professional* 17(3): 32–39. DOI: 10.1109/MITP.2015.34.

Perez A, Zeadally S, Garcia L, et al. (2018) FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things. *Electronics* 7: 379. DOI: 10.3390/electronics7120379.

Perez AJ, Zeadally S and Griffith S (2017) Bystanders' Privacy. *IT Professional* 19(3): 61–65. DOI: 10.1109/MITP.2017.42.

Perkin G (1965) News. In: Revill L and Roderick C (eds) *The Journalist's Craft: A Guide to Modern Practice*. 1st ed. Sydney, Australia: Angus and Robertson.

Perlroth N (2013) Washington Post Joins List of News Media Hacked by the Chinese. *The New York Times*, 1 February. Available at: https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html (accessed 15 February 2020).

Pesé MD, Pu X and Shin KG (2020) SPy: Car Steering Reveals Your Trip Route! *Proceedings on Privacy Enhancing Technologies* 2020(2). Sciendo: 155–174. DOI: 10.2478/popets-2020-0022.

Pettey C (2015) The Internet of Things and the Enterprise. Available at: //www.gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise/ (accessed 22 January 2020).

Pfefferkorn R (2020) There's Now an Even Worse Anti-Encryption Bill Than EARN IT. That Doesn't Make the EARN IT Bill OK. In: *Center for Internet and Society at Stanford Law School*. Available at: /blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok (accessed 31 December 2020).

Phillips G (2020) How the free press worldwide is under threat. *The Guardian*, 28 May. Available at: https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat (accessed 11 September 2020).

Phillips W (2018) *The Oxygen of Amplification*. Report, 22 May. USA: Data & Society Research Institute. Available at: https://apo.org.au/node/172901 (accessed 1 December 2022).

Pickard V (2020) Restructuring Democratic Infrastructures: A Policy Approach to the Journalism Crisis. *Digital Journalism* 8(6). Routledge: 704–719. DOI: 10.1080/21670811.2020.1733433.

Pierce J, Fox S, Merrill N, et al. (2018) Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proceedings of the ACM on Human-Computer Interaction* 2(CSCW): 139:1-139:24. DOI: 10.1145/3274408.

Politics Desk (2020a) ABC journalist Dan Oakes will not be prosecuted over Afghan Files leak. *ABC News*, 15 October. Available at: https://www.abc.net.au/news/2020-10-15/dan-oakes-afghan-files-prosecution-decision/12771304 (accessed 31 December 2020).

Politics Desk (2020b) UK government plans to hold daily White House-style televised press briefings. *BBC News*, 3 July. Available at: https://www.bbc.com/news/uk-politics-53275395 (accessed 1 January 2021).

Politou E, Alepis E and Patsakis C (2018) Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* 4(1). DOI: 10.1093/cybsec/tyy001.

Popescul D (2018) Smart TVs: What Do They Know (and Tell) about Us? In: *IACSS 2018 - IACLPM 2018 Joint Conference Proceedings*, Czechia, 27 July 2018. The International Institute for Academic Development. Available at: https://www.academia.edu/37850674/Smart_TVs_What_Do_They_Know_and_Tell_about_Us (accessed 6 December 2022).

Porambage P, Ylianttila M, Schmitt C, et al. (2016) The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing* 3(2): 36–45. DOI: 10.1109/MCC.2016.28.

Poremba S (2018) Data Privacy Must Evolve Beyond Confidentiality. In: *Security Intelligence*. Available at: https://securityintelligence.com/data-privacy-must-evolve-beyond-confidentiality/ (accessed 14 April 2020).

Posetti J (2017) *Protecting Journalism Sources in the Digital Age*. UNESCO SERIES ON INTERNET FREEDOM. UNESCO. Available at: https://webarchive.unesco.org/20220403135611/http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/protecting_journalism_sources_in_digital_age.pdf (accessed 20 May 2022).

Poulsen K (2019) India Bullies Twitter Into Banning Accounts of American, British Students Thousands of Miles Away. *The Daily Beast*, 18 June. Available at: https://www.thedailybeast.com/india-bullies-twitter-into-banning-accounts-of-american-british-students-using-censorship-law-15 (accessed 3 March 2020).

Powell A (2019) Chapter 7: The Mediations of Data. In: Hesmondhalgh D and Curran J (eds) *Media and Society*. 6th ed. London: Bloomsbury Publishing Inc., pp. 121–139. Available at: https://www.academia.edu/39303546/Media_and_Society_6th_edition (accessed 9 September 2019).

PRISMA (2015) Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Checklist. Available at: http://prisma-statement.org/PRISMAStatement/Checklist.aspx (accessed 11 February 2021).

Privacy International (2016a) Investigatory Powers Tribunal: LEGAL PROCEEDINGS - Privacy International and Others v. United Kingdom. Available at: http://privacyinternational.org/legal-case-files/1686/b-investigatory-powers-tribunal (accessed 31 December 2020).

Privacy International (2016b) Why the Internet of Things Begs for a Paradigm Shift in Internet Security. Available at: http://www.privacyinternational.org/blog/862/why-internet-things-begs-paradigm-shift-internet-security (accessed 9 September 2019).

Privacy International (2018) Invisible Manipulation: 10 ways our data is being used against us. Available at: http://privacyinternational.org/feature/1064/invisible-manipulation-10-ways-our-data-being-used-against-us (accessed 28 May 2019).

Privacy International (2019a) Case Study: Connected Cars and the Future of Car Travel in the Digital Age. Available at: http://privacyinternational.org/case-studies/769/case-study-connected-cars-and-future-car-travel-digital-age (accessed 9 September 2019).

Privacy International (2019b) Welcome to 5G: Privacy and security in a hyperconnected world (or not?). Available at: http://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not (accessed 9 September 2019).

Pu V (Lin) (2019) Taiwan Can Profit from the US-China Tech War. Available at: https://thediplomat.com/2019/10/taiwan-can-profit-from-the-us-china-tech-war/ (accessed 31 December 2020).

Pugh R and Shaw N (2021) Warning over doorbell cameras after £100k court case. Available at: https://www.manchestereveningnews.co.uk/news/uk-news/brits-video-doorbells-installed-incorrectly-21861280 (accessed 9 November 2021).

Quirk RE (2017) Are Your Company's Consumer Electronics Exempt from FCC Marketing Regulations? [Future Directions]. *IEEE Consumer Electronics Magazine* 6(2): 22–26. DOI: 10.1109/MCE.2016.2640578.

Rader E, Wash R and Brooks B (2012) Stories as informal lessons about security. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, Washington, D.C., 2012, p. 1. ACM Press. DOI: 10.1145/2335356.2335364.

RadioFreeEurope/RadioLiberty (2012) Marie Colvin's Death Raises Concerns About Use Of Satellite Phones. Available at: https://www.rferl.org/a/marie_colvin_death_concerns_about_safe_use_satelite_phones/24495230.html (accessed 19 November 2020).

Rahaman T (2022) Smart Things are Getting Smarter: An Introduction to the Internet of Behavior. *Medical Reference Services Quarterly* 41(1). Routledge: 110–116. DOI: 10.1080/02763869.2022.2021046.

Rakuszitzky M (2019) Third Suspect in Skripal Poisoning Identified as Denis Sergeev, High-Ranking GRU Officer. Available at: https://www.bellingcat.com/news/uk-and-europe/2019/02/14/third-suspect-in-skripal-poisoning-identified-as-denis-sergeev-high-ranking-gru-officer/ (accessed 3 March 2020).

Rasmussen LB (2005) The narrative aspect of scenario building - How story telling may give people a memory of the future. *AI & SOCIETY* 19(3): 229–249. DOI: 10.1007/s00146-005-0337-2.

Rauta V (2020) Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. *Cambridge Review of International Affairs* 33(6). Routledge: 868–887. DOI: 10.1080/09557571.2019.1656600.

Rawnsley GD and Rawnsley M-Y (2018) *Critical Security, Democratisation and Television in Taiwan*. 2nd ed. UK: Taylor and Francis. Available at: https://www.google.co.uk/books/edition/Critical_Security_Democratisation_and_Te/7vhKDwAAQBAJ?hl=en&gbpv=0.

Rayner G (2023) China can use people's fridges and laptops to spy on them, UK warned. *The Telegraph*, 23 January. Available at: https://www.telegraph.co.uk/news/2023/01/23/china-could-spy-millions-britons-household-objects-like-fridges/ (accessed 7 February 2023).

Reeder RW, Ion I and Consolvo S (2017) 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security Privacy* 15(5): 55–64. DOI: 10.1109/MSP.2017.3681050.

Regime TV Channels hacked, showing MEK leader Massoud Rajavi's portray; January 27, 2022 (2022) YouTube. Available at: https://www.youtube.com/watch?v=AANEo9v_g-Q (accessed 5 December 2022).

Reichert C (2015) Data retention a barrier for IoT. Available at: https://www.zdnet.com/article/data-retention-a-barrier-for-iot/ (accessed 26 February 2020).

Ren J, Dubois DJ, Choffnes D, et al. (2019) Information exposure from consumer IoT devices: a multidimensional, network-informed measurement approach. In: *ACM Internet Measurement Conference (IMC)*, 1 October 2019. ASSOC COMPUTING MACHINERY. DOI: 10.1145/3355369.3355577.

Rendall M (2022) Nuclear war as a predictable surprise. *Global Policy* 0(0): 1–10. DOI: 10.1111/1758-5899.13142.

Reporters without borders (2018) *Worldwide round-up of journalists killed, detained, held hostage, or missing in 2018*. 12 January. Available at: https://rsf.org/sites/default/files/worldwilde_round-up.pdf (accessed 9 September 2019).

Reporters Without Borders (2019) 2019 World Press Freedom Index | Reporters Without Borders. Available at: https://rsf.org/en/ranking (accessed 13 January 2020).

Reporters without borders (2019a) Only nine percent of humankind lives in a country where press freedom is good. Available at: https://rsf.org/en/news/only-nine-percent-humankind-lives-country-where-press-freedom-good (accessed 9 September 2019).

Reporters without borders (2019b) *Worldwide round-up of journalists killed, detained, held hostage, or missing in 2019*. 1 December. Reporters without borders. Available at: https://rsf.org/sites/default/files/rsf_2019_en.pdf (accessed 20 December 2019).

Reporters Without Borders (2020a) 2020 World Press Freedom Index: "Entering a decisive decade for journalism, exacerbated by coronavirus" | RSF. Available at: https://rsf.org/en/2020-world-press-freedom-index-entering-decisive-decade-journalism-exacerbated-coronavirus (accessed 11 September 2020).

Reporters Without Borders (2020b) RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders. Available at: https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators (accessed 11 September 2020).
Reporters Without Borders (2020c) Taiwan: Media independence on hold | Reporters without borders. Available at: https://rsf.org/en/taiwan (accessed 14 March 2020).
Reporters Without Borders (2021) 2021 World Press Freedom Index: Journalism, the vaccine against disinformation, blocked in more than 130 countries. Available at: https://rsf.org/en/2021-world-press-freedom-index-journalism-vaccine-against-disinformation-blocked-more-130-countries (accessed 12 April 2022).
Reporters Without Borders (RSF) (2017a) #SPOILERSFORFREEDOM: Exiled journalists warn democracies about decline in media freedom. Available at: https://rsf.org/en/news/spoilersforfreedom-exiled-journalists-warn-democracies-about-decline-media-freedom (accessed 1 January 2021).
Reporters Without Borders (RSF) (2017b) Taiwan: ministers cannot choose the questions they are asked | Reporters without borders. Available at: https://rsf.org/en/news/taiwan-ministers-cannot-choose-questions-they-are-asked (accessed 31 December 2020).
Reporters Without Borders (RSF) (2019) RSF Report: 'China's Pursuit of a New World Media Order' | Reporters without borders. Available at: https://rsf.org/en/reports/rsf-report-chinas-pursuit-new-world-media-order (accessed 9 November 2021).
Reporters Without Borders (RSF) (2020) #Tracker_19: Live updates of Covid-19 impacts of press freedom. Available at: https://rsf.org/en/tracker19-Coronavirus-Covid19 (accessed 1 January 2021).
Reporters Without Borders (RSF) (2022) *2022 Round-Up: Journalists detained, killed, held hostage and missing*. 1 December. Paris, France: Reporters Without borders. Available at: https://rsf.org/sites/default/files/medias/file/2022/12/RSF_Bilan2022_EN.pdf (accessed 14 December 2022).
Reynolds N (2020) *Performing Information Manoeuvre Through Persistent Engagement*. RUSI Occasional Paper, June. London, UK: Royal United Services Institute for Defence and Security Studies (RUSI). Available at: https://rusi.org/sites/default/files/20200611_reynolds_final_web.pdf.
Riaz S (2008) Government Influence on Print Media Content in Pakistan: Pakistani Journalists' Perspective. *Global Media Journal* 1(1). Pakistan Edition. Available at: https://www.aiou.edu.pk/sab/gmj/artical5.asp (accessed 7 February 2020).
Richard B, Sivo SA, Orlowski M, et al. (2021) Qualitative Research via Focus Groups: Will Going Online Affect the Diversity of Your Findings? *Cornell Hospitality Quarterly* 62(1). SAGE Publications Inc: 32–45. DOI: 10.1177/1938965520967769.
Richey M (2019) US-led Alliances and Contemporary International Security Disorder: Comparative Responses of the Transatlantic and Asia-Pacific Alliance Systems. *Journal of Asian Security and International Affairs* 6(3). SAGE Publications India: 275–298. DOI: 10.1177/2347797019886690.
Rid T (2013) *Cyber War Will Not Take Place*. London: C Hurst & Co Publishers Ltd.
Ridgeway Information (2019) Ridgeway Information: Open Source Intelligence. Available at: https://www.ridgeway-information.com/open-source-intelligence (accessed 21 April 2020).
Rizvi S, Kurtz A, Pfeffer J, et al. (2018) Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And*

Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), August 2018, pp. 163–168. DOI: 10.1109/TrustCom/BigDataSE.2018.00034.

Roberts G (2020) Australians filmed through hacked private security cameras, live streamed on Russian-based website. *ABC News*, 23 June. Available at: https://www.abc.net.au/news/2020-06-24/security-cameras-hacked-streamed-on-russian-website/12380606 (accessed 31 December 2020).

Roderick C and Revill L (eds) (1965) *The Journalist's Craft: A Guide to Modern Practice*. Sydney: Angus and Robertson.

Rogers K (2018) Let's Talk About Mark Zuckerberg's Claim that Facebook 'Doesn't Sell Data'. In: *Vice*. Available at: https://www.vice.com/en_us/article/8xkdz4/does-facebook-sell-data (accessed 3 March 2020).

Roman R, Zhou J and Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* 57(10). Towards a Science of Cyber Security: 2266–2279. DOI: 10.1016/j.comnet.2012.12.018.

Romanek N (2020) Cyberwar is Hell. *FeedMagazine.tv* Who Goes There? The Cybersecurity Special(25): 25–28.

Roosendaal A and Wright J (2017) Will data protection eventually kill privacy? In: *TILTing perspectives 2017: regulating a connected world*, Tilburg University, the Netherlands, 17 May 2017, p. 12. Tilburg University.

Ropeik D (2006) Best Practices Response. *Journal of Applied Communication Research* 34(3). Routledge: 253–256. DOI: 10.1080/00909880600771601.

Rory Peck Trust (2022) Digital Risk Assessment. Available at: https://rorypecktrust.org/freelance-resources/digital-security/ (accessed 9 June 2022).

Rose QC D, Jaffey QC B, Cleaver T, et al. (2016) *THE QUEEN on the application of PRIVACY INTERNATIONAL and INVESTIGATORY POWERS TRIBUNAL and (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS (2) GOVERNMENT COMMUNICATION HEADQUARTERS: STATEMENT OF FACTS AND GROUNDS*. 9 May. London, UK: In the High Court of Justice, Queen's Bench Division, Administrative Court. Available at: https://privacyinternational.org/sites/default/files/2018-04/2016.05.09%20PI%20Grounds.pdf (accessed 31 December 2020).

Rostami A, Vigren M, Raza S, et al. (2022) Being Hacked: Understanding Victims' Experiences of {IoT} Hacking. In: *Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA, USA, 8 August 2022, pp. 613–631. USENIX Association. Available at: https://www.usenix.org/conference/soups2022/presentation/rostami (accessed 19 September 2022).

Rouf I, Miller R, Mustafa H, et al. (2010) Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. In: *Proceedings of the 20th USENIX Security Symposium*, San Francisco, CA, 14 August 2010, pp. 323–338. USENIX Association.

Rowland D, Kohl U and Charlesworth A (2016) *Information Technology Law*. 5 edition. Abingdon, Oxon ; New York, NY: Routledge.

Royal Society of Edinburgh (2017) *Royal Society of Edinburgh: Advice Paper*. No. 17-21, September. Edinburgh, Scotland: Royal Society of Edinburgh. Available at: https://www.rse.org.uk/wp-content/uploads/2017/09/AP17_21.pdf (accessed 3 August 2020).

Royal United Services Institute for Defence and Security Studies (RUSI) (2015) *A Democratic Licence to Operate: Report of the Independent Surveillance Review*. Whitehall Report 2-15, July. London, UK: Royal United Services Institute for Defence and Security Studies (RUSI). Available at:

https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf (accessed 3 March 2020).
Rueckert P (2021) Pegasus: The new global weapon for silencing journalists. *Forbidden Stories*, 18 July. Available at: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ (accessed 12 April 2022).
Rule of Law staff (2019) Implied Freedom of Political Communication - Case Note and New Resource. In: *Rule of Law Education Centre*. Available at: https://www.ruleoflaw.org.au/implied-freedom-of-political-communication-case-note-and-new-resource/ (accessed 31 December 2020).
Russell A, Kunelius R, Heikkilä H, et al. (eds) (2017) *Journalism and the NSA Revelations: Privacy, Security and the Press*. 1 edition. UK: I.B. Tauris Ltd in association with the Reuters Institute for the Study of Journalism, University of Oxford.
Rustad ML (2019) How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices. *Suffolk University Law Review* 52(2): 227–272.
Sadler D (2017) Security ratings for IoT devices? In: *InnovationAus*. Available at: https://www.innovationaus.com/security-ratings-for-iot-devices/ (accessed 31 December 2020).
Sadowski J (2019) When data is capital: Datafication, accumulation, and extraction. *Big Data & Society* 6(1). SAGE Publications Ltd: 2053951718820549. DOI: 10.1177/2053951718820549.
Sagiroglu S and Sinanc D (2013) Big data: A review. In: *2013 International Conference on Collaboration Technologies and Systems (CTS)*, San Diego, CA, USA, 20 May 2013, pp. 42–47. IEEE. DOI: 10.1109/CTS.2013.6567202.
Saidi SJ, Mandalari AM, Kolcun R, et al. (2020) *A haystack full of needles: scalable detection of IoT devices in the wild*. Working Paper, 22 September. arXiv. Available at: http://spiral.imperial.ac.uk/handle/10044/1/82881 (accessed 3 June 2021).
Sajfert J and Quintel T (2017) Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. *Edward Elgar Publishing*: 22.
Saltzman DL (2014) *Examining the Feasibility of the Nisonger Outcome Assessment Tool*. PhD thesis. The Ohio State University, Ohio, USA. Available at: https://etd.ohiolink.edu/apexprod/rws_olink/r/1501/10?clear=10&p10_accession_num=osu1397221453 (accessed 19 January 2022).
Sanchez I, Satta R, Nai Fovino I, et al. (2014) Privacy leakages in Smart Home Wireless Technologies. In: *Proceedings - International Carnahan Conference on Security Technology*, 1 October 2014. DOI: 10.1109/CCST.2014.6986977.
SANS Institute (2009) Practical Risk Analysis and Threat Modeling Spreadsheet. In: *SANS Cyber Defense*. Available at: https://www.sans.org/blog/practical-risk-analysis-and-threat-modeling-spreadsheet/ (accessed 13 October 2021).
Santhosh L, Rojas JC and Lyons PG (2021) Zooming into Focus Groups: Strategies for Qualitative Research in the Era of Social Distancing. *ATS Scholar* 2(2). American Thoracic Society - ATS Scholar: 176–184. DOI: 10.34197/ats-scholar.2020-0127PS.
Savolainen R (2021) Assessing the credibility of COVID-19 vaccine mis/disinformation in online discussion. *Journal of Information Science*. SAGE Publications Ltd: 01655515211040653. DOI: 10.1177/01655515211040653.

Schwedel S and Palus H (2019) A Ranking of the Weirdest Appliances That You Can Technically Tweet From. Available at: https://slate.com/technology/2019/08/twitter-electronics-ranked-list-which-is-best.html (accessed 11 September 2020).

Schwitz JG (2011) Risk-Based Cybersecurity Policy. *American Intelligence Journal* 29(1). National Military Intelligence Association: 115–125.

Scottish Legal News (2021) English High Court rules GCHQ general warrants require sufficient specificity. *Scottish Legal News*, 11 January. Available at: https://www.scottishlegal.com/article/english-high-court-rules-gchq-general-warrants-require-sufficient-specificity (accessed 1 March 2021).

Scott-Railton J, Marczak B, Razzak BA, et al. (2017) *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*. Citizen Lab Research Report No. 93, 19 June. The Citizen Lab: University of Toronto. Available at: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (accessed 12 April 2022).

Scroxton A (2015) Inside Taiwan: The engine room of the internet of things. Available at: https://www.computerweekly.com/feature/Inside-Taiwan-The-engine-room-of-the-internet-of-things (accessed 31 December 2020).

Secretary of State for Digital, Culture, Media & Sport and Secretary of State for the Home Department (2020) *Online Harms White Paper: Full Government Response to the consultation*. December. London, UK: HM Government. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf (accessed 31 December 2020).

Secretary of State for the Home Department and Secretary of State for Northern Ireland (1998) *Legislation Against Terrorism: A consultation paper*. December. London: The Stationery Office Limited: The Stationery Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265689/4178.pdf (accessed 31 December 2020).

SecureDrop (2021) SecureDrop: Share and accept documents securely. Available at: https://securedrop.org/ (accessed 31 December 2020).

SecureDrop (2022) About SecureDrop. Available at: https://securedrop.org/faq/about-securedrop/ (accessed 13 September 2022).

Seidman I (2006) Interpreting The Material. In: *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. Third. New York: Teachers College Press, Columbia University, pp. 128–131.

Seliem M, Elgazzar K and Khalil K (2018) Towards Privacy Preserving IoT Environments: A Survey. *Wireless Communications and Mobile Computing* (Article ID 1032761): 15. DOI: https://doi.org/10.1155/2018/1032761.

Semple N, Pearce RG and Knake RN (2015) A Taxonomy of Lawyer Regulation: How Contrasting Theories of Regulation Explain the Divergent Regulatory Regimes in Australia, England and Wales, and North America. *Legal Ethics* 16(2). Routledge: 258–283.

Sen AAA, Eassa FA, Jambi K, et al. (2018) Preserving privacy in internet of things: a survey. *International Journal of Information Technology* 10(2): 189–200. DOI: 10.1007/s41870-018-0113-4.

Sengul C (2016) Privacy in the Internet of Things: Regulation vs Innovation. In: *IEEE Internet of Things Newsletter*. Available at: https://iot.ieee.org/newsletter/september-2016/privacy-in-the-internet-of-things-regulation-vs-innovation.html (accessed 25 February 2020).

Seymour W (2019) Privacy Therapy with Aretha: What If Your Firewall Could Talk? In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow, Scotland Uk, 2 May 2019, pp. 1–6. CHI EA '19. Association for Computing Machinery. DOI: 10.1145/3290607.3308449.

Seymour W and Van Kleek M (2019) The Internet of Kant: Respect as a Lens for IoT Design. In: *CHI'19 Workshops: Standing on the Shoulders of Giants: Exploring the Intersection of Philosophy and HCI*, Glasgow UK, 2019. Association for Computing Machinery.

Seymour W, Krämer M, Binns R, et al. (2020) Informing the design of privacy-empowering tools for the connected home. In: *CHI 2020 Papers on Human Factors in Computing Systems*, Honolulu, Hawai'i, USA, 25 April 2020. Association for Computing Machinery. Available at: https://ora.ox.ac.uk/objects/uuid:4f4f2de7-830b-4c81-a4cd-3ba56549d867 (accessed 31 January 2020).

Seymour W, Zhan X, Cote M, et al. (2022) A Systematic Review of Ethical Concerns with Voice Assistants. arXiv:2211.04193. London, UK: arXiv. Available at: http://arxiv.org/abs/2211.04193 (accessed 6 December 2022).

Shaban H (2018) An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says - The Washington Post. *The Washington Post*, 24 May. Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/ (accessed 13 September 2020).

Shead S (2020) Government plans new laws for smart gadgets. *BBC News*, 27 January. Available at: https://www.bbc.com/news/technology-51271717 (accessed 4 March 2020).

Sheehan M (2022) *Biden's Unprecedented Semiconductor Bet*. 27 October. Washington DC: Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2022/10/27/biden-s-unprecedented-semiconductor-bet-pub-88270 (accessed 27 October 2022).

Sheikhmiri M and Issa T (2020) Awareness Factors, Opportunities and Challenges of Iot Application in Australia. In: Issa T, Issa Theodora, Issa TB, et al. (eds) *Sustainability Awareness and Green Information Technologies*. Green Energy and Technology. Cham: Springer International Publishing, pp. 271–320. DOI: 10.1007/978-3-030-47975-6_12.

Shere A (2020) Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis. *The New Collection* 14: 3–21.

Shere A (2021) How the Internet of Things poses a threat to journalists. In: *The Journalist's Resource*. Available at: https://journalistsresource.org/home/how-the-internet-of-things-poses-a-threat-to-journalists/ (accessed 5 May 2022).

Shere A, Nurse J and Martin A (2022) "It's not paranoia if they really are out to get you": navigating risk to journalists when connected devices are everywhere. In: *Presented at IAMCR 2022*, Beijing, China, 11 July 2022. The International Association for Media and Communication Research (IAMCR). Available at: https://ora.ox.ac.uk/objects/uuid:f2c3134b-a6bc-4071-b207-ec7f7cedb118 (accessed 27 September 2022).

Shere ARK (2020) Now you [don't] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy* 5(3). Routledge: 429–448. DOI: 10.1080/23738871.2020.1832129.

Shere ARK (2021) Legal tiptoeing: the Integrated Review, Data-Sharing, and the EU. In: *Wavell Room*. Available at: https://wavellroom.com/2021/06/22/legal-tiptoeing-the-integrated-review-data-sharing-and-the-eu/ (accessed 27 September 2022).

Shere ARK (2022) 6 ways the Internet of Things poses security threats to journalists. In: *The Journalist's Resource*. Available at: https://journalistsresource.org/media/6-ways-the-internet-of-things-poses-security-threats-to-journalists/ (accessed 6 December 2022).

Shere ARK and Ashdown N (2020) Growth of privately held data increases risk of espionage. *Jane's Intelligence Review*. Available at: https://www.janes.com/images/assets/638/94638/Growth_of_privately_held_data_increases_risk_of_espionage.pdf.

Shere ARK and Melcher M (2020) Investigating the Information Commissioner's Office: Is It Fit for Purpose? *RUSI Newsbrief*, 13 November. Whitehall, London, UK. Available at: https://www.rusi.org/publication/investigating-information-commissioner%E2%80%99s-office-it-fit-purpose (accessed 27 September 2022).

Shere ARK and Nurse JRC (2020) Police surveillance of Black Lives Matter shows the danger technology poses to democracy. *The Conversation*, 24 July. Available at: http://theconversation.com/police-surveillance-of-black-lives-matter-shows-the-danger-technology-poses-to-democracy-142194 (accessed 29 March 2022).

Shere Anjuli R K, Nurse JRC and Flechais I (2020) "Security should be there by default": Investigating how journalists perceive and respond to risks from the Internet of Things. In: *The 5th European Workshop on Usable Security*, Genova, Italy, 7 September 2020, p. 12. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Shere.pdf.

Shere Anjuli R. K., Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.

Shere ARK, Nurse JRC and Martin AP (2023) Threats to journalists from the consumer Internet of Things. In: *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Springer Nature. Wales, UK: Springer, p. 230. Available at: https://link.springer.com/book/9789811964138.

Shere ARK (2023) Threats To Press Freedom In The COVID-19 Era. In: Shorenstein Center. Available at: https://shorensteincenter.org/commentary/threats-press-freedom-covid-19-era/ (accessed 19 June 2023).

Shodan (2019) The search engine for the Internet of Things. Available at: https://www.shodan.io/ (accessed 9 September 2019).

Shoemaker PJ and Reese SD (1996) *Mediating the Message: Theories of Influences on Mass Media Content*. 2nd ed. White Plains, N.Y: Longman.

Shu C (2019) Changes to Facebook Graph Search leaves online investigators in a lurch | TechCrunch. Available at: https://techcrunch.com/2019/06/10/changes-to-facebook-graph-search-leaves-online-investigators-in-a-lurch/ (accessed 3 March 2020).

Sicari S, Rizzardi A, Grieco LA, et al. (2015) Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* 76: 146–164. DOI: 10.1016/j.comnet.2014.11.008.

Sicker DC (2019) The Breadth of Policy and Regulatory Issues Facing IoT. *IEEE Internet of Things Magazine* 2(1): 4–5. DOI: 10.1109/MIOT.2019.8835416.

Silverio-Fernández M, Renukappa S and Suresh S (2018) What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering* 6(1): 3. DOI: 10.1186/s40327-018-0063-8.

Simmon ED, Kim K, Subrahmanian E, et al. (2013) *A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems*. NIST Interagency/Internal Report (NISTIR)-7951, NIST Interagency/Internal Report (NISTIR), 26 August. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/publications/vision-cyber-physical-cloud-computing-smart-networked-systems (accessed 11 February 2020).

Sinha GA (2014) *With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law and American Democracy*. New York, N.Y.: Human Rights Watch.

Sirur S, Nurse JRC and Webb H (2018) Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In: *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security - MPS '18*, Toronto, Canada, 2018, pp. 88–95. ACM Press. DOI: 10.1145/3267357.3267368.

Slupska J and Tanczer LM (2021) Chapter 39: Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In: Bailey J, Flynn A, and Henry N (eds) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Studies In Digital Crime, Technology and Social Harms. London, UK: Emerald Publishing Limited, pp. 663–688. DOI: 10.1108/978-1-83982-848-520211049.

Smalley S (2022) White House to unveil ambitious cybersecurity labeling effort modeled after Energy Star. *CyberScoop*, 11 October. Available at: https://www.cyberscoop.com/white-house-to-unveil-internet-of-things-labeling/ (accessed 12 October 2022).

Smets A and Lievens B (2018) Human Sensemaking in the Smart City: A Research Approach Merging Big and Thick Data. *Ethnographic Praxis in Industry Conference Proceedings* 2018(1): 179–194. DOI: 10.1111/1559-8918.2018.01203.

Smith S (2017) *The Internet of Risky Things: Trusting the Devices That Surround Us*. 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.

Smyth F, Lowenthal T and O'Brien D (2012) *Journalist Security Guide: Covering the news in a dangerous and changing world*. Committee to Protect Journalists (CPJ). Available at: https://cpj.org/security/guide.pdf (accessed 15 January 2020).

Söderström O, Paasche T and Klauser F (2014) Smart cities as corporate storytelling. *City* 18(3): 307–320. DOI: 10.1080/13604813.2014.906716.

Solon O and Farivar C (2019) Thousands of leaked Facebook documents show Mark Zuckerberg as 'master of leverage' in plan to trade user data. *NBC News*, 19 April. Available at:

https://www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706 (accessed 3 March 2020).
Solove DJ (2008) *Understanding Privacy*. Cambridge, Mass: Harvard University Press.
Solove DJ (2011) *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, UNITED STATES: Yale University Press.
Solove DJ and Hartzog W (2022) *Breached!: Why Data Security Law Fails and How to Improve It*. Oxford, New York: Oxford University Press.
Staff of Senator Ed Markey (2015) *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*. February. Massachusetts, USA: Office of the United States Senator for Massachusetts. Available at: https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (accessed 26 October 2020).
Statista (2020) *SMART HOME REPORT 2019: Statista Digital Market Outlook - Market Report*. January. Statista. Available at: https://www.statista.com/outlook/279/100/smart-home/worldwide (accessed 23 January 2020).
Stauss D, Bowman B and Rogers M (2019) Two New State IoT Laws Go into Effect on January 1. Available at: https://www.bytebacklaw.com/2019/10/two-new-state-iot-laws-go-into-effect-on-january-1/ (accessed 31 December 2020).
Stevens A, Beurskens A, Köke A, et al. (2013) The use of patient-specific measurement instruments in the process of goal-setting: a systematic review of available instruments and their feasibility. *Clinical Rehabilitation* 27(11): 1005–1019. DOI: 10.1177/0269215513490178.
Stotzky IP (2001) The Role of a Free Press and Freedom of Expression in Developing Democracies. *University of Miami Law Review* 56: 255.
Strava (2018) Strava Terms of Service. Available at: https://www.strava.com/legal/terms (accessed 11 September 2020).
Stray J (2014) Security for Journalists, Part Two: Threat Modeling. Available at: https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/ (accessed 11 September 2020).
Strömbäck J (2005) In Search of a Standard: four models of democracy and their normative implications for journalism. *Journalism Studies* 6(3): 331–345. DOI: 10.1080/14616700500131950.
Sturgess J, Nurse JRC and Zhao J (2018) A capability-oriented approach to assessing privacy risk in smart home ecosystems. In: *2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK, 2018, p. 37 (8 pp.)-37 (8 pp.). Institution of Engineering and Technology. DOI: 10.1049/cp.2018.0037.
Sullivan J and Lee C-Y (eds) (2018) *A New Era in Democratic Taiwan: Trajectories and Turning Points in Politics and Cross-Strait Relations*. 1st ed. New York : Routledge, [2018] | Series: Routledge research on Taiwan series: Routledge. DOI: 10.4324/9781315161648.
Sulzberger AG (2019) Opinion | The Growing Threat to Journalism Around the World. *The New York Times*, 23 September. Available at: https://www.nytimes.com/2019/09/23/opinion/press-freedom-arthur-sulzberger.html (accessed 25 September 2019).
Susskind J (2018) *Future Politics: Living Together in a World Transformed by Tech*. Oxford, United Kingdom ; New York, NY: Oxford University Press.

Swinford S (2013) Leveson could have 'chilling effect' on journalism, Information Commissioner warns. *The Telegraph*, 7 January. Available at: https://www.telegraph.co.uk/news/uknews/leveson-inquiry/9786404/Leveson-could-have-chilling-effect-on-journalism-Information-Commissioner-warns.html (accessed 9 September 2019).

Syal R and Agencies (2021) UK launches action plan to prevent harassment and abuse of journalists. *The Guardian*, 9 March. Available at: http://www.theguardian.com/media/2021/mar/09/uk-launches-action-plan-prevent-harassment-abuse-journalists (accessed 9 March 2021).

Szathmari G (2017) Threats | Threat Modeling | Privacy for Journalists. Available at: https://privacyforjournalists.org.au/threat-modeling-for-journalists (accessed 11 September 2020).

Tabassum M, Kosiński T and Lipford HR (2019) 'I don't own the data': end user perceptions of smart home device data practices and risks. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, USA, 12 August 2019, pp. 435–450. SOUPS'19. USENIX Association.

Tanczer L (2020) *Gender and the Internet of Things ('IoT'): Futureproofing Online Harms legislation*. Tech Abuse, February. London, UK: UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP). Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/ucl_g-iot_online_harms_tech_abuse_one_pager_-_feb2020.pdf (accessed 31 December 2020).

Tanczer L, Brass I, Elsden M, et al. (2019) The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In: *Rewired: Cybersecurity Governance*. Hoboken, NJ: Social Science Research Network, pp. 37–56. Available at: https://papers.ssrn.com/abstract=3385548 (accessed 22 April 2021).

Tanczer LM, Steenmans I, Elsden M, et al. (2018) Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? In: *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK, 2018, p. 33 (9 pp.)-33 (9 pp.). Institution of Engineering and Technology. DOI: 10.1049/cp.2018.0033.

Tatam M, Shanmugam B, Azam S, et al. (2021) A review of threat modelling approaches for APT-style attacks. *Heliyon* 7(1): e05969. DOI: 10.1016/j.heliyon.2021.e05969.

Taylor J (2019) Australia's anti-encryption laws being used to bypass journalist protections, expert says. *The Guardian*, 8 July. Available at: https://www.theguardian.com/australia-news/2019/jul/08/australias-anti-encryption-laws-being-used-to-bypass-journalist-protections-expert-says (accessed 9 September 2019).

Taylor J (2020) Melbourne professor quits after health department pressures her over data breach. Available at: http://www.theguardian.com/australia-news/2020/mar/08/melbourne-professor-quits-after-health-department-pressures-her-over-data-breach (accessed 31 December 2020).

Templeton B (2020) Tesla In Taiwan Crashes Directly Into Overturned Truck, Ignores Pedestrian, With Autopilot On. Available at: https://www.forbes.com/sites/bradtempleton/2020/06/02/tesla-in-taiwan-crashes-directly-into-overturned-truck-ignores-pedestrian-with-autopilot-on/ (accessed 31 December 2020).

The Australian Privacy Foundation (2011) *The Cybercrime Bill is Excessive and Unbalanced*. 7 September. The Australian Privacy Foundation. Available at: https://www.privacy.org.au/Papers/Cybercrime-PS-110904.html (accessed 31 December 2020).

The British Office Taipei (2021) Taiwan and the UK - GOV.UK. Available at: https://www.gov.uk/world/taiwan/news (accessed 2 March 2021).

The Economist: Daily Chart (2019) Britain is rejecting an ever greater share of freedom-of-information requests - Daily chart. *The Economist*, 5 January. Available at: https://www.economist.com/graphic-

detail/2019/05/01/britain-is-rejecting-an-ever-greater-share-of-freedom-of-information-requests (accessed 9 September 2019).

The Economist: Daily Chart (2021) A record number of journalists are in prison. *The Economist*, 14 December. Available at: https://www.economist.com/graphic-detail/2021/12/14/a-record-number-of-journalists-are-in-prison (accessed 12 April 2022).

The Electronic Privacy Information Center (EPIC) (2002) *Privacy & Human Rights 2002: An International Survey of Privacy Rights & Developments*. Washington DC: ELECTRONIC PRIVACY INFORMATION. Available at: https://www.powells.com/book/privacy-human-rights-2002-an-international-survey-of-privacy-rights-developments-9781893044166?partnerid=24075 (accessed 14 March 2020).

The European Parliament and The Council of the European Union (1995) *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. *281*. 31995L0046. Available at: http://data.europa.eu/eli/dir/1995/46/oj/eng (accessed 21 April 2020).

The European Parliament and The Council of the European Union (2016) *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. *119*. 32016L0680. Available at: http://data.europa.eu/eli/dir/2016/680/oj/eng (accessed 21 April 2020).

the Finnish Lifelong Learning Foundation (KVS), Birzeit University Media Development Center (MDC), and the Finnish Ministry for Foreign Affairs (2021) The journalistic work process. In: *Media Guide*. Available at: https://mediaguide.fi/mediaguide/the-journalistic-work-process/ (accessed 10 June 2021).

The National Archives (2013) UK Public General Acts: Defamation Act 2013. Available at: https://www.legislation.gov.uk/ukpga/2013/26/enacted?view=interweave (accessed 9 February 2020).

The Nobel Prize (2021) The Nobel Peace Prize 2021. Available at: https://www.nobelprize.org/prizes/peace/2021/press-release/ (accessed 12 April 2022).

The True Story of Using Fiction to Enhance Risk Intelligence (2021) The Association of International Risk Intelligence Professionals (AIRIP). Available at: https://www.youtube.com/watch?v=qP_i94eP2Ho (accessed 18 January 2023).

The White House (2022) FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity. The White House. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/ (accessed 12 October 2022).

Thipursian ED, Thogarcheti S, Fahad AA, et al. (2014) Case Study – News of the World Phone Hacking Scandal (NoTW). Available at: https://resources.infosecinstitute.com/topic/case-study-news-world-phone-hacking-scandal-notw/ (accessed 31 December 2020).

Thompson L (2020) Why Taiwan Has Become The 'Geographical Pivot Of History' In The Pacific Age. Available at: https://www.forbes.com/sites/lorenthompson/2020/09/29/why-taiwan-has-become-the-geographical-pivot-of-history-in-the-pacific-age/ (accessed 31 December 2020).

Thomson JJ (1975) The Right to Privacy. *Philosophy & Public Affairs* 4(4): 295–314.

Thomson Reuters and Clarivate Analytics (2020) Web of Science [v.5.34] - Web of Science Core Collection Basic Search. Available at:

https://apps.webofknowledge.com/WOS_GeneralSearch_input.do?product=WOS&search_mode=GeneralSearch&SID=C3pUmUGBBQzCxmoaLcM&preferencesSaved= (accessed 14 April 2020).
Thorsen E (2019) Surveillance of Journalists/Encryption Issues. In: *The International Encyclopedia of Journalism Studies*. New York, NY, USA: John Wiley & Sons, Inc, pp. 1–7. DOI: 10.1002/9781118841570.iejs0272.
Tian S, Liu L and Christian CY (2004) Course-specific Corpora in the Classroom: A News Media English Class in Taiwan. *The Journal of Asia TEFL* 1(1): 267–290.
Timm T (2016) The government just admitted it will use smart home devices for spying | Trevor Timm. *The Guardian*, 9 February. Available at: https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government (accessed 9 September 2019).
Titcomb J, Murphy M, Cook J, et al. (2018) Facebook security breach exposed 50 million accounts to attackers. *The Telegraph*, 28 September. Available at: https://www.telegraph.co.uk/technology/2018/09/28/facebook-security-flaw-exposed-50-million-accounts-hackers/ (accessed 2 March 2020).
Torr P (2005) Demystifying the threat modeling process. *IEEE Security Privacy* 3(5): 66–70. DOI: 10.1109/MSP.2005.119.
Townend J and Danbury R (2017) *Protecting Sources and Whistleblowers in a Digital Age*. 22 February. London, UK: Information Law and Policy Centre, Institute of Advanced Legal Studies. Available at: https://infolawcentre.blogs.sas.ac.uk/source-protection-report-2017/ (accessed 31 December 2020).
Tracy M (2020) News Media Outlets Have Been Ravaged by the Pandemic. *The New York Times*, 10 April. Available at: https://www.nytimes.com/2020/04/10/business/media/news-media-coronavirus-jobs.html (accessed 1 January 2021).
Treise D, Baralt C, Birnbrauer K, et al. (2016) Establishing the need for health communication research: best practices model for building transdisciplinary collaborations. *Journal of Applied Communication Research* 44(2). Routledge: 194–198. DOI: 10.1080/00909882.2016.1155729.
Trend Micro (2018) NIST Cybersecurity Framework Series Part 2: Protect. Available at: https://blog.trendmicro.com/nist-cybersecurity-framework-series-part-2-protect/ (accessed 23 January 2020).
Troncoso C (2021) *Privacy & Online Rights Knowledge Area*. The Cyber Security Body Of Knowledge Version 1.0.2. Lausanne: Ecole Polytechnique Federale de Lausanne. Available at: https://www.cybok.org/media/downloads/Privacy_Online_Rights_v1.0.2.pdf (accessed 27 April 2022).
Tse C and Browning J (2020) Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls. *Bloomberg.com*, 20 March. Available at: https://www.bloomberg.com/news/articles/2020-03-20/locked-down-lawyers-warned-alexa-is-hearing-confidential-calls (accessed 31 December 2020).
TSMC (2020) About TSMC - Taiwan Semiconductor Manufacturing Company Limited. Available at: https://www.tsmc.com/english/aboutTSMC (accessed 31 December 2020).
Tsui L (2019) The importance of digital security to securing press freedom. *Journalism* 20(1). SAGE Publications: 80–82. DOI: 10.1177/1464884918809276.
Tsui L and Lee F (2019) How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. *Journalism* 00(0). SAGE Journals: 1–23. DOI: 10.1177/1464884919849418.

Tunggal AT (2021) What are the CIS Controls for Effective Cyber Defense? In: *UpGuard*. Available at: https://www.upguard.com/blog/cis-controls (accessed 13 October 2021).

Turner S, Nurse J and Li S (2021) When Googling It Doesn't Work: The Challenge of Finding Security Advice for Smart Home Devices. In: *15th International Symposium on Human Aspects of Information Security & Assurance (HAISA)* (eds S Furnell and N Clarke), Cham, 2021, pp. 115–126. IFIP Advances in Information and Communication Technology. Springer International Publishing. DOI: 10.1007/978-3-030-81111-2_10.

Turner Sarah, Galindo J, Turner Simon, et al. (2019) The Present & Future of Data Portability in IoT. PowerPoint. London, UK. Available at: https://www.ncl.ac.uk/media/wwwnclacuk/newcastleuniversitylawschool/files/news/Turner,%20Galindo,%20Turner,%20Lis%20and%20Tanczer.pdf (accessed 1 January 2021).

Turner Sarah, Galindo Quintero J, Turner Simon, et al. (2020) The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*. SAGE Publications: 1461444820934033. DOI: 10.1177/1461444820934033.

Turow J (2021) Journalism and the Voice Intelligence Industry. *Digital Journalism* 9(7). Routledge: 1000–1006. DOI: 10.1080/21670811.2020.1829979.

Tusikov N (2019) Precarious Ownership of the Internet of Things in the Age of Data. In: Haggart B, Henne K, and Tusikov N (eds) *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*. International Political Economy Series. Cham: Springer International Publishing, pp. 121–148. DOI: 10.1007/978-3-030-14540-8_6.

Tuttas CA (2015) Lessons Learned Using Web Conference Technology for Online Focus Group Interviews. *Qualitative Health Research* 25(1). SAGE Publications Inc: 122–133. DOI: 10.1177/1049732314549602.

Uchendu B, Nurse JRC, Bada M, et al. (2021) Developing a cyber security culture: Current practices and future needs. *Computers & Security* 109: 102387. DOI: 10.1016/j.cose.2021.102387.

UCL STEaPP (2018) *Tech Abuse: How Internet-connected Devices Can Affect Victims of Gender-based Domestic and Sexual Violence and Abuse*. July. London: UCL. Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/gender-iot-tech-abuse.pdf (accessed 9 September 2019).

UK Foreign and Commonwealth Office (2020) *Policy paper: Statement by the Media Freedom Coalition on its first meeting*. 25 February. London, UK: UK Foreign and Commonwealth Office. Available at: https://www.gov.uk/government/publications/media-freedom-coalition-january-2020-meeting-statement/statement-by-the-media-freedom-coalition-on-its-first-meeting (accessed 5 March 2020).

UK Government Office for Science (2014) *The Internet of Things: making the most of the Second Digital Revolution - A report by the UK Government Chief Scientific Adviser*. Research and analysis: Internet of things: Blackett review GS/14/1230, 18 December. London, UK: Government Office for Science. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

UK Health Security Agency (2020) Guidance: Focus group study: qualitative studies. Available at: https://www.gov.uk/guidance/focus-group-study-qualitative-studies (accessed 12 January 2022).

UK Home Office (2016) *Equipment Interference: Draft Code of Practice*. London, UK: UK Home Office. Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/557861/IP_Bill_-_Draft_EI_code_of_practice.pdf (accessed 31 December 2020).

Understanding Future Technology: How do you solve a problem like cyber security for consumer devices (2021) CYBERUK 2021 ONLINE. CYBERUK 2021 ONLINE. Available at: https://www.youtube.com/watch?v=UU0BNhAhSis (accessed 13 May 2021).

UNESCO (2018) Trends in media pluralism - UNESCO Digital Library. In: *World Trends in Freedom of Expression and Media Development: Global Report 2017/2018*. Paris: UNESCO, pp. 66–100. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000261370 (accessed 1 January 2021).

UNESCO and Reporters without borders (2015) *SAFETY GUIDE FOR JOURNALISTS: A handbook for reporters in high-risk environments*. Reporters without borders. Available at: https://rsf.org/sites/default/files/guide_journaliste_rsf_2015_en_0.pdf (accessed 9 September 2019).

United States Department of State (2021) U.S. Relations With Taiwan. Available at: https://www.state.gov/u-s-relations-with-taiwan/ (accessed 2 March 2021).

United States District Court for the District of Massachusetts (2018) *Civil Action Case 1:17-cv-11730-DJC (United States District Court for the District of Massachusetts, January 26, 2018)*. Available at: https://www.eff.org/files/2018/01/26/alasaad_v._nielsen_opposition_to_motion_to_dismiss.pdf (accessed 9 September 2019).

United States Office of Personnel Management (2016) *Status of Telework in the Federal Government: Report to Congress: Fiscal Years 2014 – 2015*. November. Washington, D.C.: United States Office of Personnel Management. Available at: https://www.telework.gov/reports-studies/reports-to-congress/2016-report-to-congress.pdf (accessed 27 February 2020).

Urquhart L, Lodge T and Crabtree A (2019) Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology* 27(1). Oxford Academic: 1–27. DOI: 10.1093/ijlit/eay015.

US Department of Homeland Security (2016) *Strategic Principles for Securing the Internet of Things (IoT)*. 15 November. Washington DC: US Department of Homeland Security. Available at: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf (accessed 7 June 2021).

US Department of Homeland Security (2019) CISA Internet of Things Tip Sheet. Available at: https://www.cisa.gov/sites/default/files/publications/Internet-of-Things-Tip-Sheet-122019-508.pdf (accessed 7 June 2021).

Uzunov AV and Fernandez EB (2014) An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces* 36(4). Security in Information Systems: Advances and new Challenges.: 734–747. DOI: 10.1016/j.csi.2013.12.008.

Vailshery LS (2022) *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (in billions)*. 22 November. Statista. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed 3 December 2022).

van der Linden D, Edwards M, Hadar I, et al. (2020) Pets without PETs: on pet owners' under-estimation of privacy concerns in pet wearables. *Proceedings on Privacy Enhancing Technologies 2020* 2020(1): 143–164. DOI: 10.2478/popets-2020-0009.

van Zoonen W, Sivunen A and Rice RE (2020) Boundary communication: how smartphone use after hours is associated with work-life conflict and organizational identification. *Journal of Applied Communication Research* 48(3). Routledge: 372–392. DOI: 10.1080/00909882.2020.1755050.

Varieties of Democracy (V-Dem) (2019) *V-DEM ANNUAL DEMOCRACY REPORT 2019: Democracy Facing Global Challenges*. V-DEM ANNUAL DEMOCRACY REPORT, May. V-Dem Institute at the University of Gothenburg, Sweden: Varieties of Democracy (V-Dem) Institute at the University of Gothenburg. Available at: https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf (accessed 11 January 2020).

Varmarken J, Le H, Shuba A, et al. (2020) The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking. *Proceedings on Privacy Enhancing Technologies* 2020(2). Sciendo: 129–154. DOI: 10.2478/popets-2020-0021.

Veale M, Binns RDP and Ausloos J (2018) When data protection by design and data subject rights clash. *International Data Privacy Law* 8(2). Oxford University Press: 105–123.

Vetrivel S, van Harten V, Gañán CH, et al. (2023) Examining Consumer Reviews to Understand Security and Privacy Issues in the Market of Smart Home Devices. In: *Proceedings of the 32nd USENIX Security Symposium*, Anaheim, CA, USA, 9 August 2023, p. 18. USENIX Association. Available at: https://www.usenix.org/system/files/sec23summer_454-vetrivel-prepub.pdf.

Vicari J (2019a) Venturing into a New World of Journalism. Available at: https://medium.com/journalism-of-things/journalism-of-things-65aa481b2dda (accessed 11 January 2020).

Vicari J (2019b) When things are staring at people. Available at: https://medium.com/journalism-of-things/when-things-are-staring-at-people-59f448945089 (accessed 11 January 2020).

Vigliarolo B (2017) NIST Cybersecurity Framework: A cheat sheet for professionals. Available at: https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/ (accessed 23 January 2020).

Voorhoof D and Cannie H (2010) Freedom of Expression and Information in a Democratic Society. *International Communication Gazette* 72(4–5). SAGE Publications Ltd: 407–423. DOI: 10.1177/1748048510362711.

Wachter S (2018) The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation and Technology* 10(2). Routledge: 266–294. DOI: 10.1080/17579961.2018.1527479.

Wachter S (2019) Data protection in the age of big data. *Nature Electronics* 2(1). 1. Nature Publishing Group: 6–7. DOI: 10.1038/s41928-018-0193-y.

Wagner J (2017) China's Cybersecurity Law: What You Need to Know. Available at: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ (accessed 31 December 2020).

Wagner J and Benecke A (2016) National Legislation within the Framework of the GDPR. *European Data Protection Law Review* 2(3): 353–361. DOI: 10.21552/EDPL/2016/3/10.

Wagstaff J (2014) Journalists, media under attack from hackers: Google researchers. *Reuters*, 28 March. Available at: https://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328 (accessed 15 February 2020).

Wahl-Jorgensen K, Hintz A, Dencik L, et al. (2017) Introduction: Journalism, citizenship and surveillance. *Digital Journalism* 5(3). Routledge: 256–261. DOI: 10.1080/21670811.2016.1266134.

Wakefield J (2020) Ring doorbells to send live video to Mississippi police. *BBC News*, 5 November. Available at: https://www.bbc.com/news/technology-54809228 (accessed 7 November 2020).

Walker M, Shockey K, Neiman A, et al. (2018) Awakening Global Governments: An International Survey of Internet of Things Regulation. In: *TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018*, Rochester, NY, 16 March 2018. Social Science Research Network. Available at: https://papers.ssrn.com/abstract=3142105 (accessed 25 February 2020).

Wang AB (2018) Nest cam security breach: A hacker took over a baby monitor and broadcast threats, Houston parents say - The Washington Post. *The Washington Post*, 20 December. Available at: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/ (accessed 6 December 2022).

Watkins EA (2017) *Workers' Sensemaking for Information Security: a Research Agenda for the Future of Work*. ACM. Available at: https://drive.google.com/file/d/1llLwRsXCSqnPxuRueHk2M1cYD2x4U1BZ/edit? (accessed 9 September 2019).

Watkins EA, Al-Ameen MN, Roesner F, et al. (2017) Creative and Set in Their Ways: Challenges of Security Sensemaking in Newsrooms. In: *Proceedings of Free and Open Communications on the Internet (FOCI) 2017 Workshop, USENiX*, Vancouver, BC, Canada, August 2017, p. 11. USENIX Association. Available at: https://www.usenix.org/conference/foci17/workshop-program/presentation/watkins.

Watts M and Ebbutt D (1987) More than the Sum of the Parts: research methods in group interviewing. *British Educational Research Journal* 13(1): 25–34. DOI: 10.1080/0141192870130103.

Weber RH (2009) Internet of things – Need for a new legal environment? *Computer Law & Security Review* 25(6): 522–527. DOI: 10.1016/j.clsr.2009.09.002.

Weber V (2020) *Strategic Update: Making Sense of Technological Spheres of Influence*. LSE IDEAS, April. London, UK: London School of Economics. Available at: http://eprints.lse.ac.uk/107791/1/LSE_IDEAS_Technological_Spheres_of_Influence_April_2020.pdf (accessed 1 January 2021).

Weinberg BD, Milne GR, Andonova YG, et al. (2015) Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons* 58(6). SPECIAL ISSUE: THE MAGIC OF SECRETS: 615–624. DOI: 10.1016/j.bushor.2015.06.005.

Welch D and Taylor K (2018) Chinese video surveillance network used by the Australian Government - ABC News. *ABC News*, 12 September. Available at: https://www.abc.net.au/news/2018-09-12/chinese-video-surveillance-network-used-by-australian-government/10212600 (accessed 31 December 2020).

Wells AR (2020) *Between Five Eyes: 50 Years of Intelligence Sharing*. United Kingdom: Casemate.

Wells D and Gibson H (2017) OSINT from a UK perspective: Considerations from the law enforcement and military domains.: 32.

WESNET Australia (Women's Services Network, Australian Government) (2020) Smart toys & location tracking: privacy & safety concerns with children & pets. In: *TechSafety*. Available at: https://techsafety.org.au/resources/resources-women/toys/ (accessed 6 December 2022).

Westlund O and Krumsvik AH (2014) Perceptions of Intra-Organizational Collaboration and Media Workers' Interests in Media Innovations. *The Journal of Media Innovations* 1(2). 2: 52–74. DOI: 10.5617/jmi.v1i2.858.

White H (2005) The limits to optimism: Australia and the rise of China. *Australian Journal of International Affairs* 59(4). Routledge: 469–480. DOI: 10.1080/10357710500367273.

Whitman JQ (2004) The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal* 113: 71.

Wiener JB (2016) The Tragedy of the Uncommons: On the Politics of Apocalypse. *Global Policy* 7(S1). John Wiley & Sons, Ltd: 67–80. DOI: 10.1111/1758-5899.12319.

Williams M, Nurse J and Creese S (2017) 'Privacy is the Boring Bit': User Perceptions and Behaviour in the Internet-of-Things. In: *15th International Conference on Privacy, Security and Trust (PST)*, 28 August 2017. DOI: 10.1109/PST.2017.00029.

Williams M, Nurse JRC and Creese S (2019) Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior* 99: 38–54. DOI: 10.1016/j.chb.2019.04.026.

Willnat L, Weaver DH and Wilhoit GC (2019) The American Journalist in the Digital Age. *Journalism Studies* 20(3). Routledge: 423–441. DOI: 10.1080/1461670X.2017.1387071.

Wintterlin F (2020) Trust in distant sources: An analytical model capturing antecedents of risk and trustworthiness as perceived by journalists. *Journalism* 21(1). SAGE Publications: 130–145. DOI: 10.1177/1464884917716000.

Wirch DA (2019) Default Password Lookup Utility. Available at: https://fortypoundhead.com/ (accessed 9 September 2019).

Witschge T, Anderson CW, Domingo D, et al. (2016) *The SAGE Handbook of Digital Journalism*. SAGE.

Wood P (2019) Total Data Domination: 5G, IoT, AI Surveillance And The Smart City. Available at: https://www.technocracy.news/total-data-domination-5g-iot-ai-surveillance-and-the-smart-city/ (accessed 11 September 2020).

Woodhams S (2021) Spyware: An Unregulated and Escalating Threat to Independent Media. *Center for International Media Assistance*, 25 August. Available at: https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/ (accessed 12 April 2022).

Woodhouse A (2015) Taiwan launches hackathon to help make itself an impregnable fortress against cyber criminals from China as attacks proliferate. Available at: https://www.scmp.com/tech/apps-gaming/article/1861116/taiwan-launches-hackathon-help-make-itself-impregnable-fortress (accessed 31 December 2020).

World Economic Forum (2019) Breathing new life into a rules-based system – a global strategy. Available at: https://www.weforum.org/agenda/2019/11/breathing-new-life-into-a-rules-based-system-a-global-strategy/ (accessed 7 February 2020).

World Health Organisation (2009) WHO | Violence and Injury Prevention: Country profiles. World Health Organization. Available at: https://www.who.int/violence_injury_prevention/road_safety_status/country_profiles/en/ (accessed 31 December 2020).

Worthington E, Blumer C and Investigations ABC (2019) What do the AFP raids mean for journalists and their sources? *ABC News*, 6 June. Available at: https://www.abc.net.au/news/2019-06-06/abc-raids-what-they-tell-us-about-press-freedom/11187364 (accessed 9 September 2019).

Wright L (2017) Economic Espionage and Business Intelligence. In: Wright L (ed.) *People, Risk, and Security: How to Prevent Your Greatest Asset from Becoming Your Greatest Liability*. London: Palgrave Macmillan UK, pp. 91–105. DOI: 10.1057/978-1-349-95093-5_7.

Written Procedure for the adoption of the Council's position at first reading and the statement of the Council's reasons on the Draft Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) CM2213/16. Brussels, Belgium: Council of the European Union. Available at: https://web.archive.org/web/20171201053947/http://www.europarl.europa.eu/cmsdata/99614/Procedure_ecrite_GDPR_EN.docx (accessed 19 April 2020).

Wu D (2020a) Apple Chipmaker TSMC Raises Outlook in Sign of Tech's Resilience. Available at: https://www.bloomberg.com/news/articles/2020-07-16/tsmc-s-profit-beats-as-virus-drives-demand-for-datacenter-chips (accessed 31 December 2020).

Wu D (2020b) Taiwan Accuses Chinese Hackers of Targeting Its Citizens' Data. Available at: https://www.bloomberg.com/news/articles/2020-08-19/chinese-hackers-target-taiwan-data-through-government-systems (accessed 31 December 2020).

Wu S, Jr ECT and Salmon CT (2019) When Journalism and Automation Intersect: Assessing the Influence of the Technological Field on Contemporary Newsrooms. *Journalism Practice* 13(10). Routledge: 1238–1254. DOI: 10.1080/17512786.2019.1585198.

Wu SM, Chen T, Wu YJ, et al. (2018) Smart Cities in Taiwan: A Perspective on Big Data Applications. *Sustainability* 10(1). 1. Multidisciplinary Digital Publishing Institute: 106. DOI: 10.3390/su10010106.

Xia Q, Hong F, Feng Y, et al. (2018) MotionHacker: Motion sensor based eavesdropping on handwriting via smartwatch. In: *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2018, pp. 468–473. DOI: 10.1109/INFCOMW.2018.8406879.

Xiong W and Lagerström R (2019) Threat modeling – A systematic literature review. *Computers & Security* 84: 53–69. DOI: 10.1016/j.cose.2019.03.010.

Xu W, Zhou H, Cheng N, et al. (2018) Internet of vehicles in big data era. *IEEE/CAA Journal of Automatica Sinica* 5(1): 19–35. DOI: 10.1109/JAS.2017.7510736.

Yang Y, Wu L, Yin G, et al. (2017) A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal* 4(5): 1250–1258. DOI: 10.1109/JIOT.2017.2694844.

Yar M and Steinmetz KF (2019) *Cybercrime and Society*. Third edition. Thousand Oaks, CA: SAGE Publications Ltd.

Yin J (2008) Beyond the Four Theories of the Press: A New Model for the Asian & the World Press. *Journalism & Communication Monographs* 10(1). SAGE Publications Inc: 3–62. DOI: 10.1177/152263790801000101.

Yin RK (2009) *Case Study Research: Design and Methods*. Fourth. Applied Social Research Methods Series. California, USA: SAGE Publications, Inc.

Young J (1981) Beyond the consensual paradigm: A critique of left functionalism in media theory. In: Cohen S and Young J (eds) *The Manufacture Of News: Deviance, Social Problems and the Mass Media*. 2nd Revised edition. London: Constable, pp. 393–421.

Young J and Cohen S (1981) *The Manufacture Of News: Deviance, Social Problems and the Mass Media*. 2nd Revised edition. London: Constable.

Zanella A, Bui N, Castellani A, et al. (2014) Internet of Things for Smart Cities. *IEEE Internet of Things Journal* 1(1): 22–32. DOI: 10.1109/JIOT.2014.2306328.

Zeng X, Jain S, Nguyen A, et al. (2019) New perspectives on citizen journalism. *Global Media and China* 4(1): 3–12. DOI: 10.1177/2059436419836459.

Zhang N, Mi X, Feng X, et al. (2019) Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. In: *2019 IEEE Symposium on Security and Privacy (SP)*, Stockholm, Sweden, May 2019, pp. 1381–1396. IEEE. DOI: 10.1109/SP.2019.00016.

Zhang S (2019) Mobile Experience in War and Conflict Reporting. In: Xu X (ed.) *Impacts of Mobile Use and Experience on Contemporary Society*. Singapore: IGI-Global, pp. 226–241. DOI: 10.4018/978-1-5225-7885-7.ch014.

Zhang W, Abdulghani AM, Imran MA, et al. (2020) Internet of Things (IoT) enabled Smart Home Safety Barrier System. In: *Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things*, New York, NY, USA, 24 April 2020, pp. 82–88. CNIOT2020. Association for Computing Machinery. DOI: 10.1145/3398329.3398341.

Zhao B (2020) Unraveling Home Protection in the IoT Age: *Science and Technology Law Review* 21(1). 1: 43–80. DOI: 10.7916/stlr.v21i1.5763.

Zhao J, Wang G, Dally C, et al. (2019) `I make up a silly name': Understanding Children's Perception of Privacy Risks Online. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow, Scotland Uk, 2 May 2019, pp. 1–13. CHI '19. Association for Computing Machinery. DOI: 10.1145/3290605.3300336.

Zheng S, Apthorpe N, Chetty M, et al. (2018) User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2(CSCW): 1–20. DOI: 10.1145/3274469.

Ziegeldorf JH, Morchon OG and Wehrle K (2014) Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks* 7(12): 2728–2742. DOI: 10.1002/sec.795.

Zifcak S (2020) Why Bernard Collaery's case is one of the gravest threats to freedom of expression. Available at: http://theconversation.com/why-bernard-collaerys-case-is-one-of-the-gravest-threats-to-freedom-of-expression-122463 (accessed 11 September 2020).

Zorz Z (2020) Government-backed cyber attackers increasingly targeting journalists. In: *Help Net Security*. Available at: https://www.helpnetsecurity.com/2020/03/27/cyber-attackers-targeting-journalists/ (accessed 11 September 2020).

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books Ltd.

Zwaanswijk M and van Dulmen S (2014) Advantages of asynchronous online focus groups and face-to-face focus groups as perceived by child, adolescent and adult participants: a survey study. *BMC Research Notes* 7(1): 756. DOI: 10.1186/1756-0500-7-756.

孫興瑄 (2020) Taiwan people have little trust in local media: media watch group. In: *The China Post, Taiwan*. Available at: https://chinapost.nownews.com/20200114-931507 (accessed 31 December 2020).