

“It's not paranoia if they really are out to get you”: Navigating risk to journalists when connected devices are everywhere

Anjuli R. K. Shere*, Jason R. C. Nurse**, Andrew Martin***

* Department of Computer Science, University of Oxford, Oxford, United Kingdom

@AnjuliRKShere

ORCID: 0000-0002-1338-4256

** School of Computing, University of Kent, Kent, United Kingdom

@JasonNurse

ORCID: 0000-0003-4118-1680

*** Department of Computer Science, University of Oxford, Oxford, United Kingdom

@APMAPMAPM

ORCID: 0000-0002-8236-980X

CONTACT Anjuli R. K. Shere [anjuli.shere\[at\]cs.ox.ac.uk](mailto:anjuli.shere[at]cs.ox.ac.uk)

Track: Journalism Research and Education Section (JRE)

Topic Areas: Media freedom and safety of journalists #JRE

ExOrdo submission ID number: 2300

“It's not paranoia if they really are out to get you”: Navigating risk to journalists when connected devices are everywhere

Abstract

The consumer Internet of Things (IoT) is a fast-growing area of technology, increasingly embedded in the public and private spheres, including both in and on bodies. There are various security concerns and academic investigations into potential risks of this expansion, but none yet specifically addressing the implications to journalists and the democratic pillar of press freedom. Not only are risks to this community not yet assessed, but IoT threats generally are not communicated without technical jargon, making them inaccessible to non-experts. Given the importance of a free press, mapping IoT devices and, crucially, communicating associated risk in ways understandable and actionable to journalists themselves, is key.

Journalists and the press are particularly at-risk from IoT devices that may feature in the environments with which they must regularly interact because of the fundamental imperative of source confidentiality. Previous research demonstrated that members of the press are largely unaware of the ways in which the IoT can threaten their work and wellbeing. The networked capabilities of IoT devices increases the ease with which well-resourced threat actors can target journalists who routinely handle confidential information and are already at risk around the world from a variety of non-IoT threats. This paper therefore presents a novel categorisation of both ambient and wearable consumer IoT devices according to the environments in which journalists are most likely to interact with them. It draws on related academic work classifying devices for technical audiences to create a system that is accessible to journalists and their sources. Its goal is to make members of the media aware of the prevalence of these technologies and which of the devices' capabilities may increase their individual risk. Useful risk assessments cannot be undertaken without an accurate understanding of where threats may be encountered. By systematically outlining risks in numerous environments, this taxonomy can be easily incorporated into existing security training materials and risk assessments for journalists.

This paper presents a novel taxonomy to codify and organise IoT 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. This paper enables journalists and readers to not only visualise and conceptualise how IoT devices in different environments may create risks, its user-focused language and organisation also empower journalists to begin to use this taxonomy for awareness, mitigation, and protective purposes.

Keywords:

Internet of Things; IoT; Cyber security; Taxonomy; Emerging technology; Consumer devices

Introduction

Recent years have seen a global increase in the number and kinds of threats against the press [1]. Journalists are aware that many of these threats stem from technological considerations, including

data collected by personal devices and either stored with inadequate security or made accessible to state agencies [2–5]. However, previous work has demonstrated that journalists do not know how to mitigate threats to their work and wellbeing from the consumer Internet of Things (IoT), i.e. novel internet-connected devices [6], and that existing journalism security training is insufficient [7].

The consumer IoT includes technologies from autonomous vehicles [8] to children’s toys [9], 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 [10]. However, the omnipresence of IoT devices means that journalists may continually, unknowingly, interact with them [11, 12], thereby degrading existing security and privacy measures and presenting more opportunities and vectors for attacks [13, 14].

The prevalence of consumer IoT devices has increased the amount of personal data collated, transferred and stored, as well as potentially exposed [15, 16]. This, combined with the Snowden cache’s disclosure that states engage in mass surveillance and are therefore capable of de-anonymising source communications, may contribute to a “chilling effect” on sources [17], which prevents leaks to the press and causes self-censorship by writers [18]. 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 also freely available to consumers. 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.

Regarding who may look to exploit the IoT against journalists and what these adversaries may be aiming to achieve, there are different possibilities that likely depend on the subjects of a journalist’s work. This study assumed well-resourced threat actors, particularly nation-states, which are well-documented adversaries of journalists’ and news organisations’ cyber security [19–22]. Additionally, there are “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) [23]. Further, the motivation for primarily discussing state attackers is that there is no higher authority in the global arena than the state, which has 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 paper because states dictate what qualifies as a public or private space.

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. 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 paper, including the novel taxonomy presented, 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 against these actors. Further, 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 motivation 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.

Methods

Having a tool to categorise components of the IoT allows identification of both assets and vulnerabilities, as recommended by the National Institute of Standards and Technology [24]. Our methodology therefore aimed to answer the research question that underpins the creation of this taxonomy of consumer and smart city IoT device categories: *How can existing IoT devices be assigned clear and memorable categories both to make individual journalists' mitigation strategies easier, and also to facilitate the creation of news organisations' security policies that are effective long-term?*

Taxonomies classify components of systems, regardless of their complexity, in a way that facilitates easy navigation and sharing by stakeholders (e.g. academia, governments and the private sector). They are composed of categories of items that are not necessarily similar but are instead linked by their relationship to each other [25]. 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 study.

In their systematic mapping study, Alkhabbas *et al.* reviewed existing IoT taxonomies to find the different ways in which the IoT has been characterised [26]. One of the dimensions that Alkhabbas *et al.* specified to define IoT “Things” is “physical locations where they are installed”, examples that were given were “buildings, human bodies, and cities”, which does not feature the same level of granularity as our taxonomy and is therefore less specific than lay-users may require. Similarly, while Mountrouidou *et al.*'s taxonomic validation taxonomy avoids devices falling into multiple categories, its target user group is clearly not people with a non-technical background, as it relies on, for example, practitioners being able to tell whether a device has one or more communications channels [27]. This is consistent in other IoT taxonomies such as by Dorsemayne *et al.* [28]. Weinberg *et al.*'s taxonomy provides a similar classification system to our IoT device taxonomy, with the following categories: “wearables”, “health care”, “building and home automation”, “smart manufacturing”, “smart cities” and “automotive” [15]. Additionally, when discussing IoT threat models, Weinberg *et al.* emphasise the effects of privacy threats to users, which are particularly germane to journalists, who must consider not only the maintenance of their own privacy but the protection of their confidential sources.

Our taxonomy organises consumer IoT devices by the environments in which they may be present. It is intended to demonstrate that a significant meta-level development for journalists and their sources is that IoT devices with a variety of sensors and analytical capabilities (many of which can gather and parse bystander data) exist in almost every environment.

Tables 1-4 include three columns, each with an additional layer of detail: 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 taxonomy 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 Sturges *et al.* [29]. 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.

Four categories emerged from thematic literature analysis: (1) *private homes*, (2) *public spaces*, (3) *workplace*, and (4) *wearable*. They were further refined through secondary source analysis of existing IoT taxonomies and news articles to curate subcategories related to IoT functionalities.

Broad categories were chosen to allow 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 the *indoor public areas* and *private homes* or *workplace* categories, if working from a hotel room or college bedroom. Further, the *wearable* category should always be viewed in addition to location-specific environments.

To create a Venn diagram, as many details of devices as possible were collected, to reach a critical mass of material. 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.

Results

We define *private homes* to include not just a journalist’s own residence, but also 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 broadly similar daily patterns of life. The inclusion criteria for the *private homes* category are that the devices are primarily 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 necessarily be included there.

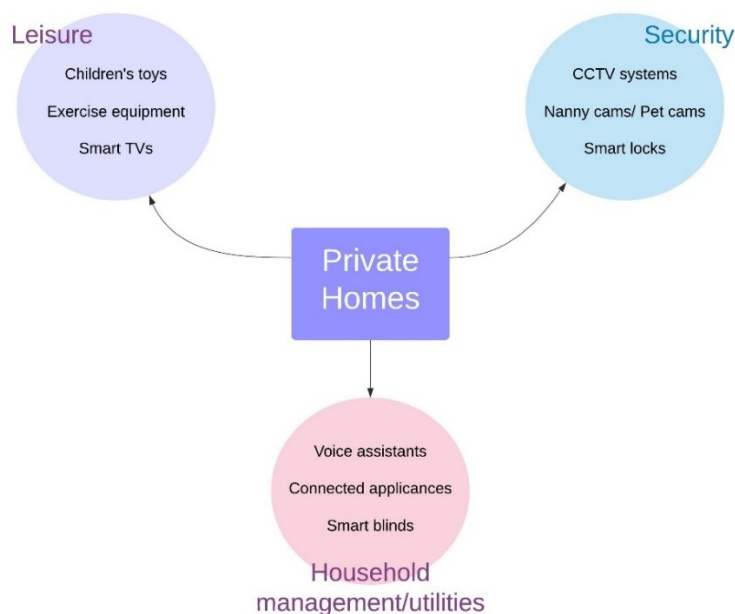


Figure 1. Private homes category

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 also includes transient areas, such as *transport*, where one might encounter both fixed sensors and those hosted on other people (and animals) who are also passing through, on public transport (underground lines, trains, etc.), semi-public transport (ride-sharing services, commercial airplanes, 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 also 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 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 necessarily be included there.

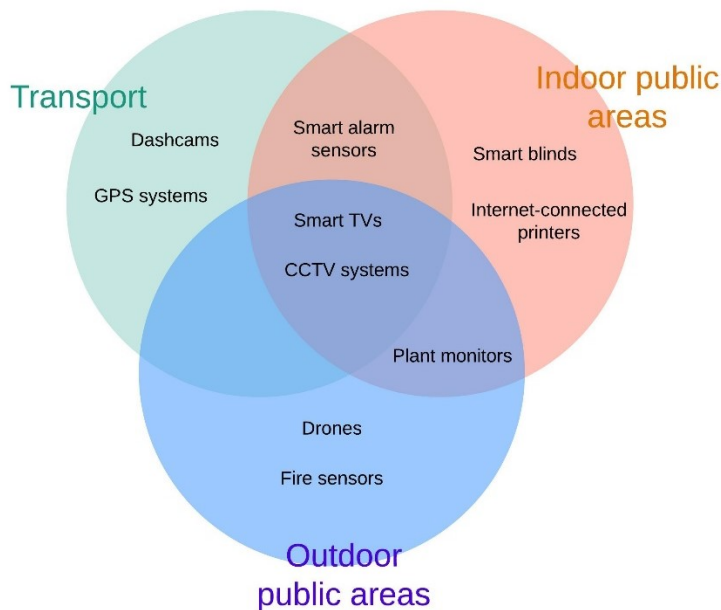


Figure 2. *Public spaces* category

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 the more infrastructurally embedded devices like smart whiteboards.

The inclusion criteria for the *workplace* category are that the devices are primarily 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 necessarily be included there.

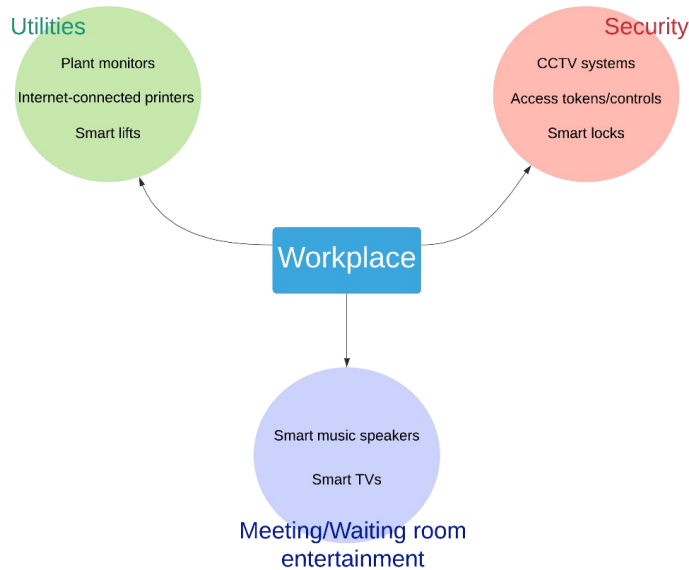


Figure 3. Workplace category

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 additionally 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.

The first three categories – *private homes*, *public spaces* and *workplace* – include overlapping device types. These overlaps are important features of this taxonomy as they demonstrate the increasingly networked and homogenised nature of previously diverse environments [16], as well as the massive volumes of data collected, parsed, transmitted and stored by IoT networks in these environments. As much of the IoT is dynamic, due to its portability and also models of shared ownership, this taxonomy is an organisational mechanism for journalist security training. It is not meant to imply that devices exist only in each specified environment.

Figure 4 is a Venn diagram taxonomy showing the main categories of environments in which journalists may encounter the IoT, to highlight overlaps [30]. Figures 1, 2 and 3 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 4, *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, according to the principles outlined above. A full list of device types within each category is included in the Appendices (Tables 1-4).

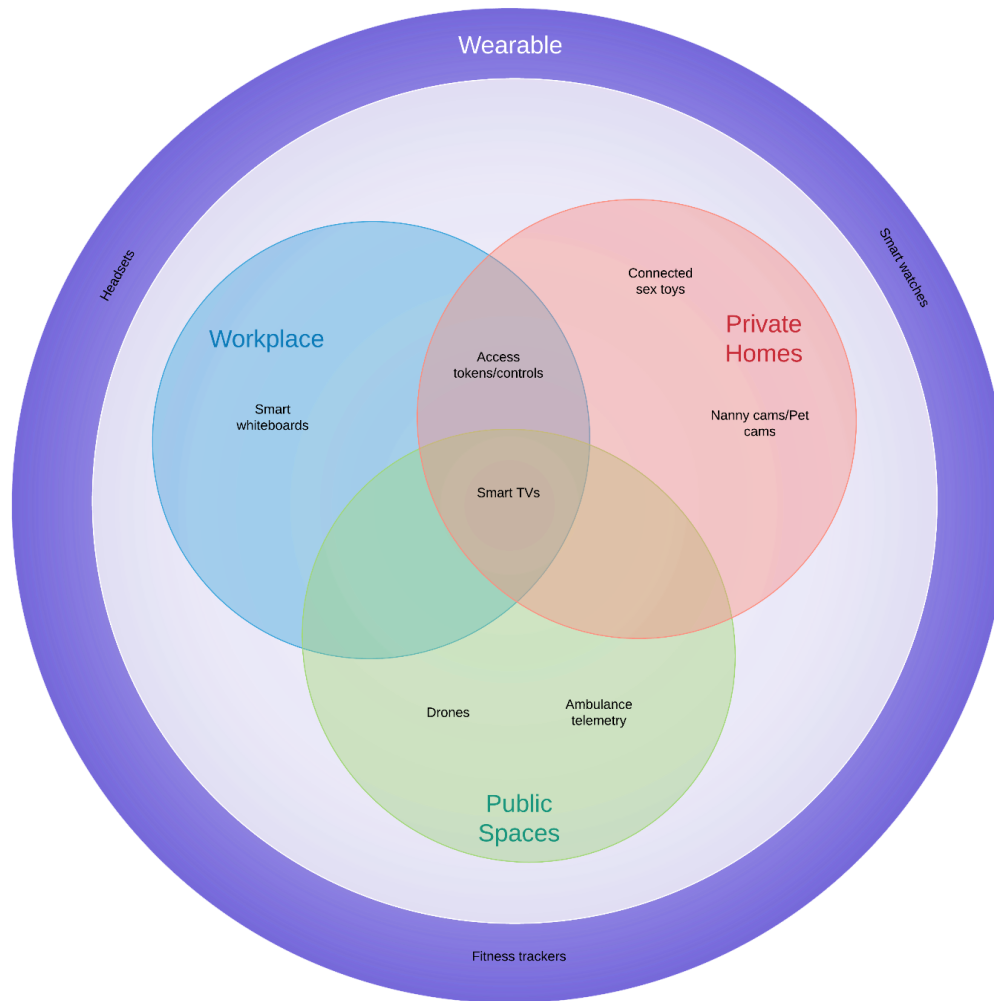


Figure 1. IoT device taxonomy by environment

Discussion

The main takeaway of this taxonomy 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. This taxonomy is operationally media-centric to fit into existing organisational security training mechanisms, as co-opting existing taxonomies that are intended for use by a different audience would be less intuitive and potentially counterproductive [25, 31].

Overall, smart televisions feature in all static (i.e. non-wearable) core categories. This is particularly significant because their additional IoT-relevant features are designed to be unobtrusive. Further, there is ample evidence that some smart televisions track on-screen user activities [32], some of these devices incorporate microphones [33], and many of them have poor security and non-existent encryption [16, 34, 35]. It therefore seems probable that journalists would also not recognise or consider that screens mounted in public places would also have these capabilities.

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. 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), 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.

Challenging areas within the *workplace* category emerged more prominently during the COVID-19 pandemic lockdowns, as individuals were required to execute a variety of their normal functions within one space, often shared with other inhabitants, like working, studying and caring for children and elderly parents, and so needed the equipment for each of these functions to be kept in the same space. Especially as many of these changes took place quite quickly, the likelihood that otherwise expected cybersecurity protocols and security considerations were less rigorously applied remains a concern.

Another challenge relating to public versus private distinctions relates to accommodation that cannot be controlled by the journalist who resides there, such as hotels. While hotel rooms are ostensibly culturally private, we consider them to fall under the *indoor public areas* subcategory because of the lack of individual environmental control. Still, cross-referencing with the *private homes* category may also be necessary to fully capture the likely IoT landscape within hotels, including hotel rooms.

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 [36]. 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 [37]. 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.

The goal is for this taxonomy 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 taxonomy, 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. However, given that there is a lack of knowledge of the IoT among journalists [6], 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; to achieve this, it shows how a variety of IoT devices overlap in scope and location, with facets designed based on perceptions of user needs.

Conclusion

This taxonomy of IoT devices is categorised according to environments in which journalists are likely to encounter IoT devices during their everyday lives. Each of the four categories – private homes, public spaces, workplace, and wearable – includes further subcategories organised according to device purpose, to allow users to engage with their content in more depth. CCTV systems, smart lighting and smart TVs may appear in various environments and could have capabilities that make ambient data collection both more likely and more accurate. It is probable that journalists interact intentionally with printers – which are increasingly likely to be internet-connected – and unintentionally with smart televisions – which seem to be the single most prevalent kind of IoT device.

Although taxonomies 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 [15, 26–28]. 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 [6]. Increasing the accessibility of the taxonomy to non-technical journalists is likely to 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 [38]. 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.

This taxonomy creates categories that are directly relevant to the free press, which is the devices are not filtered by technical aspects (e.g. method of communication), but rather by location and broad functionality, to give 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. This taxonomy highlights that the IoT has the potential to pose an intentional or ambient threat to journalists’ privacy, sources’ confidentiality and therefore the security of both.

Paper word count (inc. abstract): 3895

Acknowledgements

We are grateful to all participants of this research project for their time and contribution, to the Journalism Safety Research Network for inviting us to be part of their paper panel, to the reviewers for their feedback, and to Dr. Melcher and Dr. Debarros for their careful reading of this work.

Disclosure statement

This work was supported by the Engineering and Physical Sciences Research Council under Grant EP/P00881X/1.

References

1. 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).

2. Tsui, L.: The importance of digital security to securing press freedom. *Journalism*. 20, 80–82 (2019). <https://doi.org/10.1177/1464884918809276>.
3. Wu, S., Jr, E.C.T., Salmon, C.T.: When Journalism and Automation Intersect: Assessing the Influence of the Technological Field on Contemporary Newsrooms. *Journalism Practice*. 13, 1238–1254 (2019). <https://doi.org/10.1080/17512786.2019.1585198>.
4. Jamil, S.: Artificial Intelligence and Journalistic Practice: The Crossroads of Obstacles and Opportunities for the Pakistani Journalists. *Journalism Practice*. 0, 1–23 (2020). <https://doi.org/10.1080/17512786.2020.1788412>.
5. 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).
6. 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>.
7. Oliver, J.: Journalism schools still behind on cybersecurity training, new survey finds, <https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php>, last accessed 2020/11/15.
8. Bryans, J.W.: The Internet of Automotive Things: vulnerabilities, risks and policy implications. *Journal of Cyber Policy*. 2, 185–194 (2017). <https://doi.org/10.1080/23738871.2017.1360926>.
9. Keymolen, E., Hof, S.V. der: Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. *Journal of Cyber Policy*. 4, 143–159 (2019). <https://doi.org/10.1080/23738871.2019.1586970>.
10. Mills, J., Pellanda, E., Pase, A.: New Interactions. *Journalism Practice*. 11, 980–999 (2017). <https://doi.org/10.1080/17512786.2016.1224679>.
11. Maple, C.: Security and privacy in the internet of things. *Journal of Cyber Policy*. 2, 155–184 (2017). <https://doi.org/10.1080/23738871.2017.1366536>.
12. Constance, E.: The Internet of Things: preparing for the revolution. *Journal of Cyber Policy*. 2, 152–154 (2017). <https://doi.org/10.1080/23738871.2017.1361890>.
13. Nurse, J.R.C., Creese, S., De Roure, D.: Security Risk Assessment in Internet of Things Systems. *IT Professional*. 19, 20–26 (2017). <https://doi.org/10.1109/MITP.2017.3680959>.
14. Mohamad Noor, M. binti, Hassan, W.H.: Current research on Internet of Things (IoT) security: A survey. *Computer Networks*. 148, 283–294 (2019). <https://doi.org/10.1016/j.comnet.2018.11.025>.
15. 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>.
16. Smith, S.: The Internet of Risky Things: Trusting the Devices That Surround Us. O'Reilly Media, Inc., Sebastopol, CA, USA (2017).
17. Lashmar, P.: No More Sources? *Journalism Practice*. 11, 665–688 (2017). <https://doi.org/10.1080/17512786.2016.1179587>.
18. PEN American Center: Chilling effects: NSA surveillance drives U.S. writers to self-censor. PEN American Center and The FDR Group, New York, NY, USA (2013).
19. 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).
20. Huntley, S., Marquis-Boire, M.: Tomorrow's news is today's intel: Journalists as targets and compromise vectors. Black Hat Asia 2014. , Singapore (2014).
21. Wagstaff, J.: Journalists, media under attack from hackers: Google researchers, <https://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328>, (2014).
22. 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.
23. 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).

24. Keller, N.: Identify: NIST Cybersecurity Framework, <https://www.nist.gov/cyberframework/identify>, last accessed 2020/09/11.
25. Lambe, P.: Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness. Chandos Publishing (Oxford) Limited, Oxford (2007).
26. 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>.
27. Mountroudou, 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>.
28. Dorsemayne, 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>.
29. Sturgess, J., Nurse, J.R.C., 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. p. 37 (8 pp.)-37 (8 pp.). Institution of Engineering and Technology, London, UK (2018). <https://doi.org/10.1049/cp.2018.0037>.
30. Barstow, B.A., Vice, J., Bowman, S., Mehta, T., Kringen, S., Axelson, P., Padalabalanarayanan, S.: Examining perceptions of existing and newly created accessibility symbols. *Disability and Health Journal*. 12, 180–186 (2019). <https://doi.org/10.1016/j.dhjo.2018.11.012>.
31. Firesmith, D.G.: Security Use Cases. *Journal of Object Technology*. 2, 53–64 (2003).
32. Lawler, R.: Vizio IPO plan shows how its TVs track what you’re watching, <https://www.engadget.com/2015-07-24-vizio-ipo-inscape-acr.html>, last accessed 2020/10/26.
33. Constantin, L.: Smart TVs raise privacy concerns, <https://www.computerworld.com/article/2881715/smart-tvs-raise-privacy-concerns.html>, last accessed 2020/10/26.
34. Goodin, D.: Man-in-the-middle attack on Vizio TVs coughs up owners’ viewing habits, <https://arstechnica.com/information-technology/2015/11/man-in-the-middle-attack-on-vizio-tvs-coughs-up-owners-viewing-habits/>, last accessed 2020/10/26.
35. Constantin, L.: Samsung smart TVs don’t encrypt the voice data they collect, <https://www.computerworld.com/article/2885775/samsung-smart-tvs-dont-encrypt-the-voice-data-they-collect.html>, last accessed 2020/10/26.
36. Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., Tanczer, L.: ‘Internet of Things’: How Abuse is Getting Smarter. Social Science Research Network, Rochester, NY (2019). <https://doi.org/10.2139/ssrn.3350615>.
37. RadioFreeEurope/RadioLiberty: Marie Colvin’s Death Raises Concerns About Use Of Satellite Phones, https://www.rferl.org/a/marie_colvin_death_concerns_about_safe_use_satelite_phones/24495230.html, last accessed 2020/11/19.
38. 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>.

Appendices

Tables

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
	Remote-controlled lighting systems	Environment Sensor
	Internet-connected printers	Manual Activation
	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)	Microphone/ Camera/ Environment Sensor/ Consumption Sensor/ Timed Activation/ Manual Activation/ Weather Display/ Integrated Web Browser/ Integrated Television/ User Account
	Smart electricity meter	Consumption Sensor
	Smart gas meter	Consumption Sensor
	Smart lifts (in accessible housing)	Manual Activation/ Presence Sensor
	Plant monitors	Environment Sensor
	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	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 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

Table 1 - Private homes category

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
	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, car parks, skate parks, 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 monitors	Environment Sensor
	Pipeline leak detection	Environment Sensor

	Traffic control	Camera/ Presence Sensor/ Environment Sensor/ Timed Activation
	Fire sensors	Environment Sensor
	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
	Remote-controlled lighting systems	Environment Sensor
	Smart TVs	Microphone/ Camera/ Manual Activation/ Integrated Web Browser/ Integrated Television/ Weather Display/ User Account
	Internet-connected printers	Manual Activation
	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 monitors	Environment Sensor
	Smart electricity meter	Consumption Sensor

Table 2 - Public spaces category

Workplace (e.g. office/ school)		
Purpose	Item	Capability
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
	Remote-controlled lighting systems	Environment Sensor
	Remote-access HVAC systems (e.g. thermostats)	Environment Sensor
	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 gas meter	Consumption Sensor
	Smart lifts	Manual Activation/ Presence Sensor
	Connected appliances, White Goods (e.g. washing machines, fridges, cookers)	Microphone/ Camera/ Environment Sensor/ Consumption Sensor/ Timed Activation/ Manual Activation/ Weather Display/ Integrated Web Browser/ Integrated Television/ User Account
	Plant monitors	Environment Sensor
	Smart electricity meter	Consumption Sensor
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 3 - Workplace category

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
Security	Keychain finders with GPS beacons	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 4 - Wearable category