Responsibility and Privacy: Caring for a Dependent in a Digital Age

Martin J Kraemer
Dept. of Computer Science
University of Oxford
martin.kraemer@cs.ox.ac.uk

William Seymour
Dept. of Computer Science
University of Oxford
william.seymour@cs.ox.ac.uk

Ivan Flechais
Dept. of Computer Science
University of Oxford
ivan.flechais@cs.ox.ac.uk

Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations (CHI '20 Workshop), April 26, 2020, Honolulu, HI, USA.

Abstract
Taking care of technology for a dependant can be a daunting task. Often poorly resourced and lacking the formal training and codes of practise available to professionals, those giving informal digital care need to be understood and empowered by the HCI community. These problems are particularly challenging when people who share access to devices must negotiate issues of privacy and security, or when those giving care must do so remotely. For example, situations where one user is given responsibility for devices in the home can further exacerbate existing power asymmetries. Using insights from our past and current work on technology adoption in smart homes, we illustrate the reality of informal digital care and highlight how this reality increases the complexity of researching privacy and requires a human-centered approach.

Author Keywords
Communal technology use, smart home, multi-user

CCS Concepts
•Security and privacy → Social aspects of security and privacy; •Human-centered computing → Ethnographic studies; *Empirical studies in collaborative and social computing;*

Martin Kraemer

Martin is a PhD student working on empowering communal privacy practices in the home.

William Seymour

William is a PhD student at the University of Oxford researching ethics of smart home devices.

Ivan Flechais

Ivan is an associate professor at the University of Oxford. His research explores usable design, particularly in the area of IoT, smart, and home digital security and privacy.

Introduction

Are we doing what is right, or are we doing what is convenient? In any discussion of care, whether for young, disabled, or elderly populations, the concept of *duty of care* frames the training, processes, and practices that are put in place to ensure that ethical and legal principles are adhered to by care providers to achieve a high standard of care while protecting the dignity of the dependent population. This is commonplace in caring professions, however informal carers—individuals who take on a caring role without being employed to do so—are not regulated, or subject to codes of practice.

When it comes to IT and digital technology, despite a variety of professional services that can offer support to help individuals with their IT needs, a great amount of IT work and support is performed informally by parents, friends, and relatives informally—we argue these can be thought of as *informal digital carers*. These are trusted, well-meaning, socially connected individuals who undertake support activities, offer advice, and help to enable others in achieving their digital goals.

We argue that the caring perspective helps to uncover particular challenges for informal IT work. In particular we note that *informal digital carers* are not trained, have few resources, and do not have a code of practice to help them achieve a good standard of work while protecting the dignity of the people whom they support. This is particularly relevant in a discussion of privacy, as typical digital care practices involve installing, configuring, managing, and even acting on behalf of others. This involves a clear trust and power relationship between the carer and the dependent, however this relationship is seldom considered in the design of consumer digital systems and services.

Indeed, very few consumer products and services are designed with models of caring in mind, no codes of practice have been published to guide carers (and dependents), most security and privacy tools are intended for individuals to protect themselves, and training and education is likewise aimed at helping individuals protect themselves. There is one notable exception to this educational aspect: the advice given around helping to protect children online. Whilst this is helpful, it is only one example of an informal digital caring relationship, and many other examples exist (e.g. caring for elderly or ailing relatives, friends, or local communities).

In this paper, we propose that *informal digital care* is a useful analytic perspective to help uncover ways of empowering vulnerable populations by targeting their carers. We explore this to unpack the principles of duty of care in this space, and offer insights to help informal digital carers.

Context

Informal Support

Digital care and informal support are embedded in established social contexts (relationships, hierarchies, and moral orders). Researchers found that helpers for home computer support are rather chosen by social criteria, such as trust, over practical considerations such as skill or ability [12], and that such advice giving and receiving relationships are accompanied by expectations of ‘continuity of care’ [11].

Such informal support relationships potentially amplify existing power imbalances and relationships in different ways. Researchers have pointed out that access to informal support can be constrained by socio-economic status in that finding advice can require people to leave social circles, e.g. family or education [13]. Particularly with regards to privacy and security, this can pose difficult challenges. Emami-

Naeini et al. point out differences in perceiving guidance of friends and experts [3]. Experts might be more knowledgeable but questionable as to their motives. However, if friends' advice is in line with expert advice, this difference diminishes. As a consequence, trust can be easily lost if recommendations turn out to be unsuitable. Nthala and Flechais find people suffer from outcome bias in arranging for their security protection measures—judging that they are doing the right things to protect themselves because they believe that they have not experienced any problems [11].

Caring in Smart Homes

Because of its social and technical complexity, the smart home represents a particularly challenging environment for advice givers. Current research shows how shared ownership of devices can lead to difficulties in managing relationships: cohabitants share access to resource and devices in the home, yet they have different preferences, abilities, interests, and aptitudes [7]. This can often result in discomfort, as one person accumulates increased levels of control over devices in the home e.g. [5].

Within healthy/functioning social relationships, people share access to and sometimes even ownership of devices. This might be driven by the nature of devices, either being inherently shared or personal, but even personal devices can be shared with friends or cohabitants [4, 8, 7, 17]. However, the continued access to and control of smart home devices can stress caring relationships [2, 15] and cause friction when relationships break down [10]. By extension of the home and informal support contexts, informal digital carers who might not even be living with the people they are supporting face the challenge of navigating this context.

Generational Divides

Elderly people are somewhat more likely to be benefiting from informal digital care [6, 16], sometimes as a result of lacking the confidence to engage fully with contemporary technology [6]. Relatedly, studies on how young children understand privacy show that while they might have more *confidence* with technology, they nonetheless lack the skills required to accurately assess privacy risks beyond the interpersonal [18]. Privacy and security have been identified as issues and concerns not only for the appropriation of devices by elderly people but also in situations of care. While many smart home devices are designed for home care (ambient assisted living) [1, 9, 19], Hornung et al. identify a lack of practice-based work to inform design for security and privacy in home care settings and provide insights on issues of personal data management [6]. For younger dependants, the prevalence of parental control apps is undermined by the fact that children are rarely consulted during the design of support tools and regulations [18].

Informal Digital Care

This is the challenging context in which informal digital care is situated. Digital carers may discharge their responsibilities towards their dependants' digital privacy to the best of their ability, but however knowledgeable, skilled, and experienced they might be with such matters, they also face the challenge of having to navigate the murky waters highlighted above. Not only do these situations represent a power imbalance, as inhabitants struggle to organise and negotiate use of technology in the home between them, but the complexity of the task and nature of the social relationship require high levels of vigilance and circumspection: practice-focused research to facilitate the work of digital carers is needed. The privacy dimensions of care from a carer's perspective have not received much attention. As a result, there is a lack of research trying to understand the privacy work of informal digital carers for their dependants and shedding light onto how it could be supported.

Our Research

In the course of our research, we have frequently encountered examples of parents looking out for their children online, or children looking after their (usually elderly) parents' IT needs, and have seen how unique challenges arise for those providing digital care for others. Both our work and others' has highlighted how caring for technology follows established social and familial relationships, e.g. recently [4, 7, 11]. As a consequence, those chosen to help might do so less by their own choice and more order to follow social obligations.

We also find that 'caring for technology' can be bothersome, both in the eyes of those needing help as well as those providing advice to others. This means that finding the time and space to care for technology can be difficult, and we find this amplified by expectations of 'continuity of care' that are common in such relationships [11, 8]. An ultimate consequence of this is that conversations about technology in the home, especially related to privacy and security, do not take place as frequently as they probably should. Keeping up with ever-changing requirements (and associated devices and systems) in the home can be challenging: in the hierarchy of everyday life goals and demands, issues of privacy and security that appear important in isolation are quickly postponed in lieu of the more immediate challenges of daily life.

We have, however, made some advances in attempting to understand and address these issues. Our paper at CHI this year [14] explores the design space for privacy-empowering tools in the connected home that combine legible visualisations with education and actionable controls. The six week deployment of our technology probe showed how this approach can help address knowledge asymmetries by educating household members about how and why their devices might share data. The common understanding generated by the probe also helped to prompt household conversations around online security and privacy.

We are also in the process of conducting a longitudinal study to disentangle privacy practices in smart homes. This ethnographic study combines home visits with interventions and participant diaries to capture communal and individual perspectives on the use of internet-connected devices in the home [7]. Families choose from a selection of security cameras, voice assistants, and other devices. We are particularly interested in how families organise their daily life around these smart devices. For example, tensions arise from increased levels of responsibility and discomfort with the levels of access assigned to a single person, or Google forcing owners of their devices into data fuelled services. But cameras are also used as enabling devices, for a family father being frequently abroad but wishing to stay in touch or even to 'help out' by keeping the house safe, and for parents to be reassured of their children returning home from school safely. The situations we encountered in our studies appear benign, and they seem to work well with designers' intentions and visions for the device to be used. However, it is also easy to imagine that such situation can take turns for the worse, and that the design of devices provides inadequate affordances to manage such situations.

At the Workshop

We intend to bring our own research experience and the idea of an analytic perspective of informal digital care to the workshop table; and we are very eager to learn about and discuss other perspectives on privacy that might allow us to tailor our own privacy research to better understand and help carers and their dependents.

Acknowledgements
Martin and William are funded through EPSRC grant number P00881X/1. This work is part of a larger initiative into Informing the Future of Data Protection by Design and by Default in Smart Homes at the University of Oxford, funded by the UK Information Commissioner's Office.

REFERENCES

[1] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place* 50, May 2017 (2018), 112–118. DOI:http://dx.doi.org/10.1016/j.healthplace.2018.01.006

[2] Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and teens' perspectives on privacy in a technology-filled world. In *Proc. SOUPS*.

[3] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios. *Proc. ACM Hum.-Comput. Interact.* 2 (2018). DOI: http://dx.doi.org/10.1145/3274317

[4] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 2 (2019), 1–21. DOI: http://dx.doi.org/10.1145/3328915

[5] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM. DOI: http://dx.doi.org/10.1145/3290605.3300498

[6] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. 2017. Navigating Relationships and Boundaries: Concerns around ICT-Uptake for Elderly People. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 7057–7069. DOI: http://dx.doi.org/10.1145/3025453.3025859

[7] Martin J Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home: Uncovering Household Group Efficacy. In *Proceedings of the Halfway to the Future Symposium 2019*. ACM. DOI: http://dx.doi.org/10.1145/3363384.3363389

[8] Martin J Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. 2020. Further exploring communal technology use in smart homes: social expectations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM.

[9] Linda Little and Pam Briggs. 2009. Pervasive Healthcare: The Elderly Perspective. In *Proceedings of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments (PETRA '09)*. Association for Computing Machinery, New York, NY, USA, Article Article 71, 5 pages. DOI: http://dx.doi.org/10.1145/1579114.1579185

[10] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2189–2201.

[11] Norbert Nthala and Ivan Flechais. 2018. Informal Support Networks: an investigation into Home Data Security Practices. *Fourteenth Symposium on Usable Privacy and Security (SOUPS)* (2018), 63–82. https://www.usenix.org/conference/soups2018/presentation/nthala

[12] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E Grinter, and W Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 739–748. DOI: http://dx.doi.org/10.1145/1518701.1518816

[13] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. *Proceedings of the 2017 SIGCHI Conference on Human Factors in Computing Systems* (2017), 931–936. DOI: http://dx.doi.org/10.1145/3025453.3025673

[14] W Seymour, MJ Kraemer, R Binns, and M Van Kleek. 2020. Informing the design of privacy-empowering tools for the connected home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery. DOI: http://dx.doi.org/10.1145/3313831.3376264

[15] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 129–139. DOI: http://dx.doi.org/10.1145/2632048.2632107

[16] John Vines, Mark Blythe, Stephen Lindsay, Paul Dunphy, Andrew Monk, and Patrick Olivier. 2012. Questionable Concepts: Critique as Resource for Designing with Eighty Somethings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. Association for Computing Machinery, New York, NY, USA, 1169–1178. DOI: http://dx.doi.org/10.1145/2207676.2208567

[17] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart. 3, November (2019).

[18] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 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 (CHI '19)*. ACM, New York, NY, USA, Article Paper 106, 13 pages. DOI: http://dx.doi.org/10.1145/3290605.3300336

[19] Martina Ziefle, Simon Himmel, and Wiktoria Wilkowska. 2011. When Your Living Space Knows What You Do: Acceptance of Medical Home Monitoring by Different Technologies. In *Proceedings of the 7th Conference on Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society: Information Quality in e-Health (USAB'11)*. Springer-Verlag, Berlin, Heidelberg, 607–624. DOI: http://dx.doi.org/10.1007/978-3-642-25364-5_43