Approaches and Technologies to Support Home Users' Engagement with Cyber Security

Sarah Turner
School of Computing
University of Kent
Giles Lane, Canterbury
Kent, CT2 7NZ
slt41@kent.ac.uk

"Approaches and Technologies to Support Home Users' Engagement with Cyber Security" analyses the way in which UK families engage with cyber security when using home Internet of Things (IoT) devices. By determining the prevalence of devices in the home, how different family members use those devices, and what knowledge of cyber security those individuals have, it aims to expose specific needs in the improvement of device design, marketing or support; more targeted governmental policy, or regulation, where devices are used by both adults and children; and how best to address the need for further education, both for adults and children.

Internet of Things; Parents; Children; Privacy; Cyber security; Cyber awareness schemes; Multi-use.

1. INTRODUCTION

The Internet of Things is increasingly prevalent in everyday life, with estimates suggesting that consumer IoT spending reached $108 billion in 2019 (Kemper, 2019). The promise of the IoT in the home is alluring: optimised utilities usage, monitoring the home when absent, checking in on sick or elderly relatives. Yet, there are a range of issues to be resolved, including methods to achieve interoperability of devices within the house (Basaure et al., 2020), data security risks (Zeng et al., 2017) and the inability of devices to accommodate multiple users (Jang et al., 2017).

2. SECURITY, PRIVACY AND THE INTERNET OF THINGS

The privacy and security of all people within the home is of key importance when considering home IoT devices. Significant considerations have already been given to the implications of constant data collection, where IoT devices process data in the cloud (Apthorpe et al., 2018), and the patterns that can be extrapolated from it (Tolmie et al., 2016). The perceived convenience of such devices sees that individuals exhibit the privacy paradox: despite considering themselves privacy conscious, in practice, users exhibit risky behaviours, in particular sharing a significant amount of personal information where the perceived benefit of using such devices is worthwhile (Williams et al., 2016, 2017).

Keeping data that is intended to be private out of the public domain is fundamental, but the security issues arising from the adoption of IoT devices extend beyond this. When surveyed, experts considered there to be a high potential for crime, exploitation, risk to physical safety and a loss of personal control to emanate from IoT devices (Tanczer et al., 2018).

It is unsurprising that adherence to recommended cybersecurity hygiene measures (for example, those found in National Cyber Security Centre (2019)) is poor, when cost and features are may be more important than security at point of purchase (Emami-Naeini et al., 2019), and given individuals have incorrect mental models in relation to how devices work (Abdi et al., 2019). There are few formal legal or regulatory obligations in place around mandatory security requirements: the UK government has put forward a law mandating no default passwords, software update processes and details of vulnerability disclosure procedures (Department for Digital, Culture, Media and Sport, 2020). This follows a wider-ranging Code of Practice for Consumer IoT devices that was not widely taken on board by IoT producers, despite its uncontroversial requirements (Department for

Proceedings of BCS HCI 2020 Doctoral Consortium. Keele University, UK

Digital, Culture, Media and Sport, 2018). Unsurprisingly, details of cyber security measures are largely absent from home IoT device documentation, making it extremely hard for users to understand all the features of the devices they are buying, and how to ensure such devices are secure (Blythe et al., 2019). It is also unclear how well home IoT devices will adhere to the proposed Age Appropriate Design Code that is currently subject to Parliamentary approval (Information Commissioner's Office, n.d.).

3. DIGITAL TECHNOLOGIES AND FAMILIES

Research has started to consider the role of multiple users of IoT devices within the home: in particular, the design implications arising from the expectation of any household member being able to access the Internet upon devices designed for one individual (Geeng & Roesner, 2019; Matthews et al., 2016; Tabassum et al., 2020; Watson et al., 2020). In parallel, there has been consideration of how families negotiate digital technology use (Cranor et al., 2014; Moser et al., 2016; Ur et al., 2014; Wisniewski et al., 2017), including how cyber security is controlled (Garitaonandia et al., 2019; Muir & Joinson, 2020). Parents often manage digital technology use within the household through restricting access or facilitating discussion about how the technology works or what it is doing (Livingstone et al., 2017). This works in cases where technology is used to access content or where the device is not designed to be available in the background at all times. Neither aspect is necessarily true of IoT devices in the home. Furthermore, with device interfaces typically absent (Geeng & Roesner, 2019), app-based control introduces risks of inequality of use and access, whether intentional or otherwise – posing significant threats to vulnerable family members (Chatterjee et al., 2018; Markwick et al., 2019).

Limitations in devices (either through restricting software, or as a result of having been "designed for children") often leads to children using alternative technologies (designed for adults) or circumventing controls in other ways (Ghosh et al., 2018; McReynolds et al., 2017). There is a significant balancing act required in the designing of systems to recognize the value of collaborative technologies in a family setting, with the concerns that privacy is essential to facilitate maturation – and also, that children are much more likely to encounter a family member or a close friend as a threat than a stranger.

It has been shown that cyber awareness schemes targeted at adults tend to have low impact rates (Bada et al., 2015). This is particularly true of IoT devices. How best to explain the security and privacy risks of a device used by multiple household members remains elusive. Children also need to understand how to use IoT devices safely. It is important to note that children's ways of learning about privacy and other cybersecurity skills may require significantly different knowledge scaffolding and approaches than adults, using techniques such as storytelling or game-playing (Zhang-Kennedy et al., 2016; Zhao et al., 2019). There may also need to be a cultural shift: amongst groups sharing devices, discussions about the security and privacy preferences of individuals within these groups do not happen (Watson et al., 2020). It is even less likely such discussions will occur within families.

4. CURRENT WORK AND FUTURE PLANS

Little prior work appears to have been done to understand how the adoption of IoT devices in the home affect both adult and child family members, taking into account differences between individual interaction preferences and abilities, what data the device may collect and knowledge of how to use such devices in a secure manner. Our systematic literature review found that, when IoT devices were researched, privacy arising from the data being collected was considered in depth, whereas other cyber security issues were not. There was no clear understanding of which devices were most commonly used in a typical home, and although men are largely known to be the main purchasers and maintainers of devices (Geeng & Roesner, 2019; Strengers et al., 2019), when parents were being interviewed in relation to their child's or family's use of devices, mothers were disproportionately over-represented in the research. Many papers cited the recognition of a lack of understanding of how digital technologies work as a key concern for parents.

The following work strands arose from the literature review:

- Determining the prevalence of IoT devices used by families in the UK, and understanding how they are used by household members of all ages.
- Critically examining the cyber security issues present in IoT devices typically used by families, and the extent to which different family members pose different risks.
- Investigating what information needs to be provided for secure IoT use in the home, and how, to whom, and when is this information best presented.

Using the work strands as a guide, immediate future work will involve mixed methods approaches to determine, in particular, the ways in which different family members use the most common devices, what they understand about how the

devices work, and how cyber security knowledge is brought into, and used within, the family. The research will also aim to understand how well the most commonly used devices adhere to the proposed Age Appropriate Design Code and regulation on smart device cyber security.

It is hoped that the findings of such research may serve to underline specific needs in the improvement of device design, marketing or support; the need for more targeted governmental policy, or regulation, in the case of devices that can reasonably be expected to be used by both adults and children; and how best to address the need for further education, both for adults and children, in terms of the specific types of cyber security risks devices may pose within the household.

5. REFERENCES

Abdi, N., Ramokapane, K. M., & Such, J. M. (2019). More than smart speakers: Security and privacy perceptions of smart home personal assistants. *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, 451–466.

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(2), 59:1-59:23. https://doi.org/10.1145/3214262

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118–131.

Basaure, A., Vesselkov, A., & Töyli, J. (2020). Internet of things (IoT) platform competition: Consumer switching versus provider multihoming. *Technovation*, *90–91*, 102101. https://doi.org/10.1016/j.technovation.2019.102101

Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz005

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. *2018 IEEE Symposium on Security and Privacy (SP)*, 441–458. https://doi.org/10.1109/SP.2018.00061

Cranor, L. F., Durity, A. L., Marsh, A., & Ur, B. (2014). Parents' and teens' perspectives on privacy in a technology-filled world. *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, 19–35.

Department for Digital, Culture, Media and Sport. (2018). *Code of Practice for Consumer IoT Security*. 24.

Department for Digital, Culture, Media and Sport. (2020, July 16). *Proposals for regulating consumer smart product cyber security—Call for views*. GOV.UK.

Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3290605.3300764

Garitaonandia, C., Karrera, I., & Larranaga, N. (2019). Media convergence, risk and harm to children online. *Doxa Comunicacion*, *28*, 179–199. https://doi.org/10.31921/doxacom.n28a10

Geeng, C., & Roesner, F. (2019). Who's In Control? Interactions In Multi-User Smart Homes. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3290605.3300498

Ghosh, A. K., Badillo-Urquiola, K., Guha, S., LaViola Jr, J. J., & Wisniewski, P. J. (2018). Safety vs. Surveillance: What children have to say about mobile apps for parental control. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3173574.3173698

Information Commissioner's Office. (n.d.). *Age appropriate design: A code of practice for online services*. Retrieved 22 July 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

Jang, W., Chhabra, A., & Prasad, A. (2017). Enabling multi-user controls in smart home devices. *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, 49–54. https://doi.org/10.1145/3139937.3139941

Kemper, G. (2019). *IoT Technology and Smart Devices in the Home*.

Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation: Maximizing Opportunities and Minimizing Risks. *Journal of*

Communication, *67*(1), 82–105. https://doi.org/10.1111/jcom.12277

Markwick, K., Bickerdike, A., Wilson-Evered, E., & Zeleznikow, J. (2019). Technology and Family Violence in the Context of Post-Separated Parenting. *Australian and New Zealand Journal of Family Therapy*, *40*(1), 143–162. https://doi.org/10.1002/anzf.1350

Matthews, T., Liao, K., Turner, A., Berkovich, M., Reeder, R., & Consolvo, S. (2016). 'She'll just grab any device that's closer': A Study of Everyday Device & Account Sharing in Households. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5921–5932. https://doi.org/10.1145/2858036.2858051

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5197–5207. https://doi.org/10.1145/3025453.3025735

Moser, C., Schoenebeck, S. Y., & Reinecke, K. (2016). Technology at the Table: Attitudes about Mobile Phone Use at Mealtimes. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 1881–1892. https://doi.org/10.1145/2858036.2858357

Muir, K., & Joinson, A. (2020). An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home. *Frontiers in Psychology*, *11*, 424. https://doi.org/10.3389/fpsyg.2020.00424

National Cyber Security Centre. (2019). *Smart devices: Using them safely in your home*.

Strengers, Y., Kennedy, J., Arcari, P., Nicholls, L., & Gregg, M. (2019). Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3290605.3300875

Tabassum, M., Kropczynski, J., Wisniewski, P., & Lipford, H. R. (2020). Smart home beyond the home: A case for community-based access control. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3313831.3376255

Tanczer, L. M., Steenmans, I., Elsden, M., Blackstock, J., & Carr, M. (2018). Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 1–9. https://doi.org/10.1049/cp.2018.0033

Tolmie, P., Crabtree, A., Rodden, T., Colley, J., & Luger, E. (2016). "This has to be the cats": Personal Data Legibility in Networked Sensing Systems. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 491–502. https://doi.org/10.1145/2818048.2819992

Ur, B., Jung, J., & Schechter, S. (2014). Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance. *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 129–139. https://doi.org/10.1145/2632048.2632107

Watson, H., Moju-Igbene, E., Kumari, A., & Das, S. (2020). "We hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3313831.3376605

Williams, M., Nurse, J. R. C., & Creese, S. (2017). Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 181–18109. https://doi.org/10.1109/PST.2017.00029

Williams, M., Nurse, J. R. C., & Creese, S. (2016). The Perfect Storm: The Privacy Paradox and the Internet-of-Things. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 644–652. https://doi.org/10.1109/ARES.2016.25

Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17*, 523–540. https://doi.org/10.1145/2998181.2998236

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 65–80.

Zhang-Kennedy, L., Mekhail, C., Abdelaziz, Y., & Chiasson, S. (2016). From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. *Proceedings of the the 15th International Conference on Interaction Design and Children*, 388–399. https://doi.org/10.1145/2930674.2930716

Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M., & Shadbolt,

N. (2019). `I make up a silly name': Understanding Children's Perception of Privacy Risks Online. *Proceedings of the 2019 CHI Conference on* Human Factors in Computing Systems, 1–13. https://doi.org/10.1145/3290605.3300336