Written evidence submitted by Sarah Turner and Dr Jason Nurse

We are writing in our capacities as socio-technical researchers, in particular to provide evidence from the PhD research project we are undertaking to understand how families manage the cyber security of smart devices in the home. We are delighted to be given this opportunity to respond to this call for evidence, and will answer those questions that our research can provide some insight into. The entire 3.5 year project has engaged with in excess of 1100 families in the UK through survey work, 25 families directly through interviews, and it is expected another 30 families will take part in a final participatory design exercise. The below work highlights specific pieces of published and peer reviewed findings of the project to date. This set of questions is looking for a broad set of responses, and as such, none of the answers below should be considered a full response to the entirety of possible issues, concerns or outcomes that these questions hope to address; rather, these answers focus on our research into the ways in which families – parents, or legal guardians, and children in the UK – use, understand and manage their smart home devices.

> *Are there any groups in society who may particularly benefit from or be vulnerable to the increasing prevalence of smart technology, such as young or elderly people, people with disabilities and people likely to be digitally excluded?*

Our research has found that the purchase of smart devices for use in the home is often not widely discussed within the family prior to purchase, and certainly not between parents and children (Turner et al., 2022b). This leads to a **number of potential vulnerable people within the home at any one point**. Vulnerability must be considered broadly in this case, encompassing actual harm, but also potential for harm to be caused through the use of these devices. Harms, too, cover a broad spectrum – ranging from physical damage to person or property, to the much less tangible loss of personal data – or provision of personal data to services without an opportunity to consent. Part of the reason for the inclusion of the provision of personal data being considered a harm is simply that, given the relative infancy of the smart technology ecosystem, it is not always abundantly clear how securely this data is stored, how proportionate its collection is against the benefits the technology confers with its use and – vitally – what happens to this data in the longer-term: who can access it not just today, but in the future, and how the user retains long-term control over something so intimately linked to them.

Children are broadly made vulnerable by the introduction of these devices into the home. Our interviews with families in the UK on this topic found that both parents and children were quick to discuss aspects of online safety and security when asked about device security, suggesting **ineffective mental models of how the devices operate**, and what the potential threats linked to device use may be, as opposed to using the Internet through a computer or similar device. Parents rarely spoke to children about smart home device use – indeed, the more integral to the house the device,[1] the less likely the parent was to consider needing to discuss the device at all with their children, as they did not consider the connection to the Internet to be worth of comment or consideration (Turner et al., 2022b).

This is particularly problematic as **children do not receive meaningful education as part of the UK school curriculum** about how connected devices work or the way that data may be processed, meaning that they are – on the whole – receiving no explanation at all about how these devices work as they grow up to become consumers. Instead, they are introduced to them either without

[1] e.g. thermostats, security cameras and doorbells, washing machines, dishwashers.

explanation at all (in the case of the thermostats, white goods or security equipment), or as a frivolous thing (in the case of smart speakers or smart TVs, for instance). Younger children, in particular, have been shown to consider smart assistants as a friend, or person, without any sense of the data they are providing to it, how to control, or delete that data – and how to manage the fact that **they, typically, neither control nor own the device** they are talking to. Often, children reported not being able to be understood by voice activated devices. Without the legal ability to have a managing account for the devices or even access to the smartphone app that so often is the user interface for the device, **children are necessarily put in a position of vulnerability**.

As is discussed below, however, it is not just children that have the potential to be vulnerable in a smart home. **Depending upon the strength of the security measures on the device – and the ways in which those measures are configured and subsequently updated, the entire household could be at risk.** This is particularly problematic given the short life-span of many smart devices from a software point of view[2] – an issue that was entirely misunderstood by those interviewed in our research. Given the ramifications of using devices with unsupported software – losing functionality at one extreme, to losing data, or being targeted by – or hosting – malware at the other, which could lead to you being disconnected from the Internet by your provider (Turner et al., 2021a), **the average family is extremely vulnerable, simply by virtue of expecting more from the life-span of these products than they currently provide.**

Possibly unsurprisingly, it was not the case in our research that there was overt evidence of abuse of power by individuals in the house through the use of these devices. That is not at all to say that this does not happen (see, for example, Parkin et al., 2019 on technology-facilitated abuse), but **the power imbalance between parents and children can, again, make children in particular vulnerable through the loss of autonomy and privacy**. Older research has shown how, despite agreeing that children deserve privacy, parents will set up devices in ways that allow them to monitor their teenage children "just in case" (Ur et al., 2014); families interviewed in our research described a range of accounts set up so that parents could monitor or control the child's activities. In many cases, **this oversight is something expected by the children in a way that could hinder the risk taking and individual decision making required as part of growing up** (see, for instance Livingstone et al., 2019).

[2] For example, the backlash Sonos received when they announced the removal of support from several of their speaker range (as described in, for example, https://www.wired.com/story/older-sonos-speakers-will-stop-receiving-updates/)

What are the key short- and long-term risks and threats, and how can we ensure the devices, systems and networks of individuals, businesses and organisations are digitally-literate and cyber secure?

As hinted in the response to the previous question, there is a **fundamental lack of understanding in within the typical family home as to how the devices that they are using work, may take in and use their data, and how to keep those pieces of information – or other things – that they consider important secure.** This poses risks in the short-term, as well as in the longer-term, as without concern over the value of security, these devices will continue to be embedded in the smart home, and may continue to pose the same threats as they may do today.

Participants in our research pointed to the novelty of the devices, and the ease with which devices worked straight out of the box. **They typically were not asked to review security settings either at the point of setup or subsequently.** One of the largest vulnerabilities introduced by these devices is the lack of easily and obviously provided information as to how the devices work – or specifically, what the most appropriate means of using such devices securely would be – or even what "most securely" might mean in specific instances of device use (Turner et al., 2021a). This is problematic as **without robust, easy to follow guidance, parents are unable to model good security behaviour to their children**, or able to explain how to control the personal data provided in the use of such devices. As mentioned above, children are also not being educated in school about how these devices work, meaning that the average household devoid of any knowledge when it comes to security and privacy in relation to these devices. As such**, it is – in the current state – impossible to rely upon users of smart devices in the home to ensure that devices are set up in ways to ensure appropriate security.**

A key question that could mitigate many future risks is why so many devices are becoming connected to the Internet – what true value does it bring to the user experience, and what are the technical credentials of those people bringing these devices to market? In our research with families, **many participants explained that they did not see these devices as "serious" elements in their homes, with many underusing features, forgetting to use them entirely, or using them in place of items that performed the same function without an Internet connection** (for instance, many smart speakers, over time, ended up being used for nothing more than a radio). Other participants, as mentioned above, did not consider devices like thermostats or vacuum cleaners as being primarily connected to the Internet, and so ignored them once installed.

Those participants that had endeavoured to connect up more elements of a smart home together reported two main issues: the **difficulty of interoperability between ecosystems**, and **the expense of always buying new, branded devices.** Indeed, children routinely reported being told to take extremely good care of devices they had received, as they would not get replaced should they be broken. **All of these issues make anyone in the smart home vulnerable.** The combination of devices that do not provide seamless interoperability outside of their own ecosystem as well as the ability to buy second hand, or unlabelled, devices much more cheaply from the Internet creates the potential for security issues: **pieces of software, not intended to work together, may overlap or underlap in ways that create weakness.** Parents interviewed in our research discussed how they would use forums online to find ways to hack together devices that did not naturally talk to each other, with no consideration for the potential risks that that may cause. **No participants in the research knew whether the devices that they used still received software updates** – but, given the prevalence of second hand and well preserved older devices, it is almost certainly the case that many were not. This makes the entire household vulnerable.

The lack of interoperability of devices and data is a major risk for users of smart home devices today and in the future. **A lack of interoperability of both of these things makes long-term use of the smart home impossible.** Where devices integrate with important functional features of the house – for example the boiler, water system, heating or electrics – it is infeasible for the devices to be moved with the people living in the home. **Without the ability to port data safely, securely and completely in these circumstances, there is a significant risk that the technology will never be able to be truly integrated or useful.** There is also significant **risk to the user that all this data is being collected with no real long-term objective** for its collection. How does a user retain control over that data?

Do existing frameworks, like data protection legislation and the Public Security and Telecommunications Infrastructure Bill, adequately address concerns with smart technology, and if not, how could they be changed?

The Public Security and Telecommunications Infrastructure Bill is a welcome first step in legislating some of the issues arising from the situation of such easily available consumer technologies having such low bars to entry. In particular, **the importance of holding distributors to account is vital** when so much of the technology is bought online, typically with a focus upon price rather than the reputation of the manufacturer or the quality of the software or data management, for example (Turner et al., 2021a, 2021b).

That said, **incorporating the remaining steps in the DCMS Code of Practice for Consumer IoT Security[3] (DCMS Code) in any future legislation would add significantly to the safety of users,** if only by raising the bar to entry for potential producers in requiring the production of more secure and robust devices. **Our research suggests that users do not understand the devices they are using sufficiently to ensure their own safety, meaning that the most appropriate way to mitigate risk to users would be through additional robust regulatory and legislative measures.**

One area where the DCMS Code does not necessarily go far enough is in relation to software updates. Users do not understand that devices are often likely to become obsolete because of a lack of up to date software long before the device itself physically breaks and so will continue to use devices long after intended by the manufacturer with potential security issues, not only for the household, but also possibly more broadly.[4] There are also issues when device manufacturers go out of business, or take a financial decision not to support devices any longer. **Additional obligations should be put upon manufacturers to provide users with a more robust understanding of the supported life of a device – a supported life that should be commensurate with the expected life of the physical device** (which may, in the case of white goods, be in excess of ten years); or an alternative means of using the device safely without needing access to the Internet for an extended period of time (working in "dumb mode"). This typically does not happen at present, with devices more often than not giving the users error and fault messages should they not be given all the permissions needed, which may make device use hard when users do not want to provide certain pieces of data – or use the service without accessing the Internet (Turner et al., 2022a).

As mentioned above, **the widespread adoption of smart homes may require more robust requirements around mandatory data portability,** to ensure that users do not lose access to, or need to be concerned about the future use of, their data should they move home or need to change provider. Article 20 of the GDPR does not mandate portability (only requires it where it is technically feasible), relying, rather, on industry efforts to solve the technical issues. Adoption of standardisation efforts (such as ETSI's standard ETSI EN 303 645)[5] are obviously vital to create interoperability of data, but do not remain mandatory. It is telling, also, that the Big Tech-backed Data Transfer Project[6] does not focus on portability and interoperability between IoT devices, suggesting there may be a while to go before this becomes an industry issue worth considering, arguably at the expense of users, who cannot take their data with them between devices at present.

---

[3] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security#keep-software-updated

[4] For example, the proliferation of the Mirai botnet through insecure IoT devices.

[5] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[6] https://datatransferproject.dev/

References

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age: An evidence review.* https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. M. (2019). *Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse.* NSPW '19: Proceedings of the New Security Paradigms Workshop. 1–15. doi: 10.1145/3368860.3368861

Turner, S., Nurse, J., & Li, S. (2021a). When Googling It Doesn't Work: The Challenge of Finding Security Advice for Smart Home Devices. In S. Furnell & N. Clarke (Eds.), Human Aspects of Information Security and Assurance (Vol. 613, pp. 115–126). Springer International Publishing. doi: 10.1007/978-3-030-81111-2_10 https://kar.kent.ac.uk/88357/

Turner, S., Nurse, J. R. C., & Li, S. (2022a). "It Was Hard to Find the Words": Using an Autoethnographic Diary Study to Understand the Difficulties of Smart Home Cyber Security Practices. CHI Conference on Human Factors in Computing Systems Extended Abstracts. doi: 10.1145/3491101.3503577 https://kar.kent.ac.uk/92356/

Turner, S., Pattnaik, N., Nurse, J. R. C., & Li, S. (2022b). 'You Just Assume It Is In There, I Guess': UK Families' Application And Knowledge Of Smart Home Cyber Security. 25th ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW) (To appear). https://kar.kent.ac.uk/95346/

Turner, S., Quintero, J. G., Turner, S., Lis, J., & Tanczer, L. M. (2021b). The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. New Media & Society. 2021;23(10):2861-2881. doi: 10.1177/1461444820934033

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