

# “You Just Assume It Is In There, I Guess”: Understanding UK Families’ Application And Knowledge Of Smart Home Cyber Security

SARAH TURNER, NANDITA PATTNAIK, JASON R.C. NURSE, and SHUJUN LI, Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, UK

The Internet of Things (IoT) is increasingly present in many family homes, yet it is unclear precisely how well families understand the cyber security threats and risks of using such devices, and how possible it is for them to educate themselves on these topics. Using a survey of 553 parents and interviews with 25 families in the UK, we find that families do not consider home IoT devices to be significantly different in terms of threats than more traditional home computers, and believe the major risks to be largely mitigated through consumer protection regulation. As a result, parents focus on teaching being careful with devices to prolong device life use, exposing their families to additional security risks and modeling incorrect security behaviors to their children. This is a risk for the present and also one for the future, as children are not taught about the IoT, and appropriate cyber security management of such devices, at school. We go on to suggest that steps must be taken by manufacturers and governments or appropriate trusted institutions to improve the cyber security knowledge and behaviors of both adults and children in relation to the use of home IoT devices.

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

Additional Key Words and Phrases: Internet of Things, smart home, cyber security, families, parents, children, consumer protection

## 1 INTRODUCTION

A 2021 report into smart home product ownership in the UK found that 76% of respondents owned at least one such device [62]. Although the picture of ownership is a complex one, with only smart TVs, smart speakers and fitness devices being reported in this survey as having ownership levels higher than 20% of the respondent population, the increase of such devices in communal areas of the home cannot be denied. This means that all members of a household, whether adults or children, comfortable with technology or not, may be expected to live around Internet-connected devices.

Recently, research has focused upon the various usability and privacy issues of the multi-use of home IoT devices [4, 11, 24, 35, 72].<sup>1</sup> The privacy of all people living within a home is of key importance when considering home IoT devices, and keeping data that is intended to be private out of the public domain is fundamental. The security issues arising from the adoption of home IoT devices extend beyond this, however, and the relative novelty and heterogeneity of such devices, coupled with their global production, also mean that they have, to date, evaded meaningful regulation or legislation to mandate minimum security requirements. Blythe and Johnson [7] suggest that a lack of policy and technical intervention may facilitate a “crime harvest”, where crimes targeted at the individual (burglary, sex crimes) or a societal level (such as political

<sup>1</sup>“Home IoT devices” will be considered to be those explicitly defined in the Code of Practice for Consumer IoT Security published by the UK’s Department for Digital, Culture, Media and Sport (DCMS) [14].

subjugation) will become more common; Hodges [29] has shown that homes with smart technology at present are somewhat more likely to suffer crimes such as burglary.

Home IoT device threats are much more pervasive than those of home computers, in that they can allow for enormous data collection about the users, run essential elements of a home, be linked to credit card and other sensitive information, and be leveraged for cybercrime. In a multi-user setting, device owners should be considering a range of threat actors, from malicious adversaries [49], to misuse by the manufacturer [59], to those inside the house, who could use devices for control of others [39], or simply inadvertently making purchases or breaking a device. However, users' mental models of home IoT devices have been shown to be inaccurate [40], and this lack of understanding, coupled with a lack of interfaces, can make it harder to understand how the devices should be secured. Devices may not obviously provide users with means to implement appropriate security on the device, possibly requiring home network security to be increased for adequate protection. Home IoT devices that fail, or manufacturers that cease to exist, may cause fundamental parts of the home to stop working.

This paper extends out the work done on the privacy of multi-use devices by considering what it means for families to manage the cyber security aspects of such device use, and not solely the privacy concerns. It looks to understand how families in the UK consider and implement home IoT device cyber security, how they learn about and discuss it as a group with specific responsibilities around keeping each other safe and passing on knowledge. Using a survey of 553 individuals and interviews with 25 families,<sup>2</sup> we investigated the concerns that families in the UK have about managing the cyber security of home IoT devices, and how and when they educate themselves about cyber security issues. Prior research in this area has tended to use either smaller interview or focus groups [4, 60, 72], or a survey of individuals [10], or be based in the USA [2, 24]. By combining both a survey and interview of UK families, we are able to understand a wide range of parents' experiences of home IoT device use, along with their cyber security understanding for these devices. When combined with the qualitative detail of the interviews, we find that that families are well versed in controlling and discussing cyber security aspects that apply to being online, but do not have similar strategies in place to manage the different threats of home IoT use, assuming a certain level of protection simply from existing consumer protection regulation. Despite relying heavily on discussion as a means of facilitating a communal understanding of rules, neither parents nor children have sufficient prior knowledge or access to sufficient education or support to have meaningful conversations about home IoT device cyber security as a family unit, focusing instead on factors relating to cost saving and efficient use. We argue that this is a concern not only for the present day, but for the future as well, as children are not having appropriate behavior modeled to them by their parents, and make suggestions for the role of different stakeholders in managing this knowledge gap.

The rest of the paper reads as follows: an overview of related work is found in Section 2, methods of both survey and interviews are explained in Section 3. Survey findings, followed by interview findings, are in Section 4; these findings are discussed in Section 5. Limitations and further work are considered in Section 6, which are followed by concluding thoughts in Section 7.

## 2 RELATED WORK

### 2.1 Multi-use of IoT devices

Sun et al. [60] found, from interviewing 23 parents in the US and Canada, that parents' perception of the risk assessments to keep their children physically and digitally safe in the smart home typically

<sup>2</sup>Where a family group comprises of all the parents and/or legal guardians and school-aged children in a household (along with any other household members, although it is the parent/child interaction with devices that is of primary focus).

moved through three phases, encompassing purchasing decisions, re-evaluation as the children start to use the device, and further adjustments as the children grow. More specifically, Garg and Sengupta [23] explored how parents of different socio-economic groups and ethnicities had different concerns over their children’s use of smart speakers, ranging from managing the children’s use of the device, to behavioral and privacy considerations. Geeng and Roesner [24] found that home IoT devices often created tensions, requiring ongoing cooperation and negotiation between members of the home, particularly between parents and children. When interviewed, parents whose children used fitness trackers designed for children found that such trackers required significantly more parental interaction than expected because of the limited agency these devices provided to the children, despite device claims and parental hopes of increased child independence [47]. Apthorpe et al. [2] found, via a study involving 13 interviews and a survey of 508 individuals, that the lack of nuanced sharing solutions for home IoT devices meant that households were required to fall back to “social resolution techniques”, such as agreeing not use particular features, in order that ongoing use remains acceptable for all involved. Agreement and discussion from all participants about the goals and requirements of a device is a fundamental part of what Kraemer et al. [35] refer to as “group efficacy”, a key element of acceptable multi-user device management. However, power dynamics need to be recognized as a limiting factor in group efficacy: Bernd et al. [4] report that nannies working within a family context did not consider themselves to have enough power in the relationship with parents – their employers – to ask for smart surveillance systems to be switched off. Ehrenberg and Keinonen [17] similarly found that the use of smart technologies in the home can work to create hierarchies by affecting access to, use of and interactions within physical household spaces.

## **2.2 Parent-child communication around cyber security and privacy**

There is suggestion that communal decision making about how and when families should use Internet-connected devices (in particular, smartphones) can create higher levels of willing compliance [28, 34]. This is in keeping with the argument of Blum-Ross and Livingstone [6] that family life is, increasingly, a democratic one, that requires more complex rule-making around technology use than time or content restriction, and the recognition that children are beings with their own agency.

Shin [56] and Kumar et al. [37] found that parents will often put off discussing security with their children, erroneously considering it to be a future risk. Wisniewski et al. [70] showed that this lack of interaction between parents and teenage children in regards to how to manage Internet-related risks sets children up poorly to manage them, should they occur. Additionally, children tend not to raise instances where they have encountered risks to their parents, and feel that their parents disproportionately tell them what they cannot – rather than can – do online [5].

Nikken and de Haan [44] showed that parents do not understand enough to feel comfortable in what their children are doing, or how to manage it appropriately, or by themselves, often relying on external support, or older siblings. Cranor et al. [13] discussed how, for teenagers, parents struggle with the need to exhibit trust to foster maturation and independence – but consider that their children need far less privacy in the digital realm than real life. This finding is echoed by Ur et al. [65], where parents agreed that children should have privacy when interviewed, only to deny them this privacy when subsequently setting up a security camera, as they should have nothing to hide.

## **2.3 Cyber Security and Privacy Knowledge and Action**

In a study of 13 families, Muir and Joinson [42] found that families worried about a wide range of cyber security issues, but considered threats such as cyber bullying and stranger danger of more concern than financial or technical threats, in terms of the immediate danger to the family. When

interviewed by Tanczer et al. [61], academic and industry participants with expertise in the security of IoT devices 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.

It has long been understood that people form inaccurate security stances based upon inaccurate mental models of the digital technologies that they use [22, 67]. Huang et al. [31] showed that, in the case of smart speakers at least, incorrect mental models about how the devices use and present data to all users can cause individuals to make poorer decisions about privacy than they may believe they are. Seymour et al. [55] found that visualisations of home IoT data flows did not provoke change of device use or restriction of those flows, despite the information about data flows being interesting to review.

In conjunction with inaccurate understandings of the risks the devices may pose, the perceived convenience of IoT devices leads individuals to exhibit the privacy paradox: despite considering themselves privacy conscious, in practice, they will behave in a more risky manner, in particular sharing a significant amount of personal information with home IoT devices and further with online services, where the perceived benefit of using such devices is worthwhile [69]. Zheng et al. [74] found that individuals trust manufacturers to protect their privacy, but do not take steps to verify this. Furthermore, users may turn to the Internet for advice on cyber security issues relating to home IoT devices, but often struggle to find formal guidance when online [63]. In situations where accounts are shared, participants in [68] suggested that they avoided discussing issues of security and privacy, despite the potential risks to everyone using the account. This accords with the performative aspect of trust that people exhibit when sharing devices with people that they are close to [41]. This lack of consistent behavior may cause problems for the next generation: Kumar et al. [37] explored the mental models that children aged 5-11 had around privacy and security in relation to Internet use. While they found that the children were able to develop some strategies for control (such as providing false information), they relied heavily on their parents for support.

### 3 METHODS

We started our research with two main research questions: 1) how do families manage the cyber security related to their home IoT device use, and 2) how and when do families educate themselves about home IoT device security. In order to answer these questions, we undertook a survey and semi-structured interviews. For both, families had to be living in the UK, with at least one IoT device at home. Survey participants had to be a parent or legal guardian of at least one school-aged child (between 4-18); for the interview, the participants had to be a family (of at least one adult and one school-aged child). The survey was framed in order to gather a wider picture of what devices families in the UK have and what steps they take to keep those devices secure, based upon the view of a single adult family member. It additionally asked questions about the participants' experience of cyber security in the news, what their children learned at school, and what they discussed at home. The interviews followed the survey, to dig deeper into questions around the family experience of home IoT device cyber security, giving the opportunity for both parents and children to discuss. Interview participants were recruited independently, with the agreeing adult asked to take the survey prior to the family interview, or through an expression of interest after completing the survey. For a visual guide to the recruitment process, see Figure 1; this is further explained in the sections that follow below. Both pieces of research received approval from the University's relevant ethics committee in July 2020.

#### 3.1 Survey

*3.1.1 Survey Design.* The survey was designed to capture a broad range of information about the type of home IoT devices found in the homes of respondents, how and who bought, used and

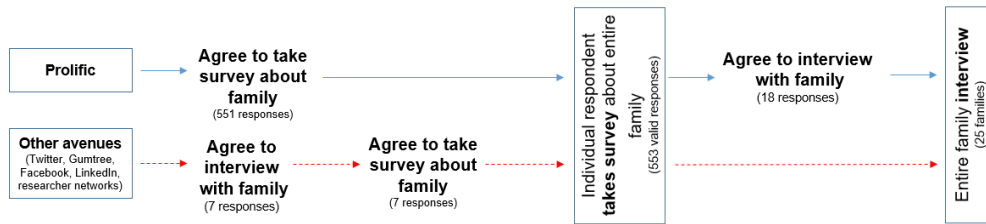


Fig. 1. Recruitment Process

managed them, as well as understanding the attention paid to cyber security in the home. Unlike the interviews, it was understood that only a single adult member of the family would be providing their interpretation of the family’s use of such devices, giving the opportunity to ask specific questions (such as “Does one person take ownership of managing the device?”) to understand the adult’s role in family technology use. Each question gave multiple options for response, including a free text field for adding in options not covered.

The survey asked participants to list all their home devices, based upon the list found in [14],<sup>3</sup> and then required the participants to answer a range of questions on the one or two devices they used most within the home. Participants were asked to focus on the most commonly used device(s) as a means of ensuring most, if not all, of the questions subsequently asked, would have been considered at some point during ownership of the particular device(s). Questions were asked about the devices that covered entire family use, from point of purchase onwards (e.g. “Was there discussion about buying the device amongst the household members (including children) before it was bought?”, “Does everyone in the household use the device in the same way?”, “Do you have to help the child(ren) in the house to use the device?”). These questions were asked to provide an understanding of how the participant perceived the role of home IoT device use in the home, and where children in particular fitted in the decision making and use of such devices.

The remainder of questions about the specific devices covered the understanding of cyber security and devices, broadly based on guidance provided by the UK’s National Cyber Security Centre (NCSC) [43]. These questions asked about the setup of the device (“When the device was set up, were there detailed instructions?”, and “Did setup involve changing the device’s password?”), the current use of the device (“Do you know how you would completely delete the information the device has collected?”, and “Do you know how long for, or until when, the software on the device is supported until?”) as well as more general questions around device misuse and breaking (“Has your current device ever broken?”, and “If the device broke tomorrow, what would be your major concerns?”) to assess cyber security risks against other risks that the users perceived.

The final part of the survey asked for details on the participants’ experience with cyber security issues more directly: “Who or where do you turn to for support with digital technology issues?”, followed by “Have you ever been a victim of a cybercrime of data breach?”. If they had, they were then asked if they incurred a loss as a result of this (with loss intentionally not being defined as purely financial). Finally, they were asked if they were aware of the manufacturers of devices in their home having reported a breach. In relation to cyber security and the family, they were then

<sup>3</sup>This list was used as it forms the basis of devices captured by a comprehensive code of practice for “consumer IoT devices”, set out by the UK government, and so provided a useful yardstick as to the devices available to consumers in the UK at the time. Participants were able to add in any devices they did not feel were covered in the list.

asked what aspects of cyber security they understood their children were taught at school, and what they discussed at home, based on the list of topics covered in the English curriculum [16].<sup>4</sup> These questions aimed to give a reflection of the awareness of the participant of their role as a potential victim of cybercrime, and educator about cyber security in the home.

**3.1.2 Survey participation.** The online survey was hosted on Jisc's Online Surveys tool,<sup>5</sup> using the participant recruitment platform Prolific.<sup>6</sup> In total, 558 adults responded to the survey during July and September 2020; 551 of these through Prolific, and 7 from the interview recruitment process. Two participants were excluded for responding solely about a laptop computer and smart phone, not a home IoT device, leaving 556 responses for further screening. There were two attention checks in the survey: four participants failed both attention checks (0.72%); one of these participants was also interviewed. The three participants who failed the attention checks and were not interviewed were excluded from further review. The decision was taken to retain the individual who was interviewed as it was possible to see the consistency in answers between the interview and survey. This left 553 valid responses for the final analysis. Survey participants recruited through Prolific were paid pro-rata for their time, using the UK's Living Wage Foundation calculated 2019/2020 rate of £9.30 per hour<sup>7</sup> (with the majority of participants taking around 15 minutes to complete it). Those survey participants recruited outside of Prolific (as part of the interview process) were paid £5 in Amazon gift vouchers for completing the survey.

**3.1.3 Demographic Information.** The participants of the survey had a mean age of 42.32 years (SD 7.51), with an age range of 24-66. 138 (24.82%) were male, 417 (75.00%) female, with one participant preferring not to answer this question. All participants lived in the UK at the time of taking the survey, with 473 living in England (85.07%), 41 in Scotland (7.37%), 21 in Wales (3.78%) and 18 in Northern Ireland (3.24%); although not intentionally sought, this proportion is broadly in line with the population breakdown across the countries in the UK as reported by the UK's Office of National Statistics for 2020 [46]. 81.69% of participants were employed either full- or part-time, or due to start a job within the next month, with 2.51% considering themselves to be unemployed, but job-seeking. The respondents were asked to detail out the age of their children. 17.36% of respondents (96) had a 0-5 year old child, 54.07% (299) had a child aged 6-10, 53.52% (296) had an 11-15 year old, and 19.89% (110) had a 16-17 year old.

## 3.2 Interview

**3.2.1 Interview Design.** The interview process was designed to build upon and flesh out the survey questions, by allowing the initial survey participants to expand upon their survey responses, and also to enable the entire family to add their views. The interview format was semi-structured, meaning that each individual could spend time focusing more on areas of concern (or awareness) for them; the full set of questions used in the interviews can be found in Appendix A.

The interview process was designed in such a way that the children would be asked questions by the interviewer first, where possible, without interruption from their parents; the parents were then asked to answer the questions after the children had spoken. This allowed for the parents

<sup>4</sup>Within the United Kingdom, each of the devolved nations have their own powers to build school curricula. The curricula within Wales, Scotland and Northern Ireland cover similar ground, focusing upon online safety and learning about the role of the Internet within society in particular; however, to avoid complexity, the English Department for Education curriculum has been used in this research as the basis upon which questions are asked as it is the oldest, and is referenced as a basis for at least some of the more recent devolved nations' curricula.

<sup>5</sup><https://www.onlinesurveys.ac.uk/>

<sup>6</sup><https://www.prolific.co/>

<sup>7</sup><https://www.livingwage.org.uk/what-real-living-wage>

to reflect on the children’s answers, as in most cases, the parents had remained within earshot as their children were interviewed. The questions for children were modified based on whether the child was either in primary school (4-11 years) or secondary or tertiary education (12-18 years) in two ways: the expected level of knowledge was taken into consideration, based upon the national curriculum for England laid out in [16], but also, the language used was modified by the interviewer based upon the age of the child. Questions focused on how each participant used the devices they chose to talk about: which device features did they like and dislike using, where they struggled to use the devices (and how they managed that). Participants were then asked, more specifically, about their understanding of what cyber security was. Children were asked to reflect on their understanding of what cyber security was, whether from school or elsewhere and what they considered the biggest risks of using the Internet, and home IoT devices were. Parents, additionally, were asked to share any situations of being a victim of a cyber crime or incident, any times where they felt that they needed to seek further information, and how they went about it.

*3.2.2 Interview Participation.* There were 25 interviews, taking place between July and September 2020; the longest interview was 1 hour 15 minutes, with the shortest being 20 minutes long. There were 33 adults interviewed in total, with 22 being female (66.67%), 11 male (33.34%). There were 38 children interviewed, aged from 4-16 (average age: 9.63 years, SD 3.59). Given ongoing COVID-19 social distancing restrictions at the time of interview, three video-conferencing systems were used: Microsoft Teams, Zoom and Google Meet, based on the participants’ preference. Where possible, all family members were asked to attend, in particular, to enable the interviewer (the first author of the paper) to ask questions of all family members and avoid the “driver” of device use answering all the questions on behalf of less knowledgeable family members, and to understand the interaction the family had when discussing the technology. This was not always possible, but for all interviews at least one adult and one child from the family participated. Participants were sourced through posts on social media and message board sites (Facebook, LinkedIn, Twitter, Gumtree), through expressing interest having completed the survey, and through the first author’s networks. Interview participants were remunerated with a £10 Amazon gift voucher if aged 18 or over, and a £5 Amazon gift voucher if under 18.

The participant details are in Table 1; throughout this paper, adults will be referred to through the following coding system: A (for adult), M or F (male or female), and their family’s Interview Reference number, e.g., the mother in interview 2 is referred to as “AF2”, the father in interview 3 as “AM3”. Children are referred to by C, their family’s Interview Reference number, then distinguished by their age, e.g., the two children in interview 14 are referred to as “C14, aged 13” and “C14, aged 16”.

*3.2.3 How the children participated.* The children interviewed had a wide range of ages, and so their participation and interaction in the interview process differed. All children reacted reasonably well to the use of video-conferencing and talking to the interviewer; in two circumstances, the children asked not to be interviewed on camera, which posed no problems, as they were comfortable to talk whilst off camera. In many cases, the opening questions, asking the children to describe the home IoT devices (more details on how this was handled by children of differing ages in the paragraphs below), followed by questions asking how they used them, were enough to allay any initial reticence to participate.

The youngest children (aged 4-5) did not sit by themselves to be interviewed: being interviewed in their own homes allowed them to wander around, and in certain circumstances, answer questions by doing – giving demonstrations of how they interacted with devices, rather than giving verbal explanations. Parents of children in this age group often re-framed questions posed by the interviewer, not only to focus the child upon answering the question but also to use more familiar

Table 1. Information of interview participants

Interview Reference	Number of adults	Number and ages of children
1	1	1 (15)
2	2	2 (12,15)
3	1	1 (5)
4	2	1 (4)
5	1	1 (10)
6	1	1 (6)
7	2	3 (7, 9, 11)
8	1	2 (5, 6)
9	2	2 (4, 8)
10	2	3 (7, 12, 13)
11	1	2 (7, 14)
12	1	1 (13)
13	1	1 (12)
14	2	2 (13, 16)
15	1	1 (7)
16	2	2 (7, 9)
17	1	1 (8)
18	1	1 (10)
19	1	1 (12)
20	2	2 (6, 9)
21	1	1 (9)
22	1	1 (8)
23	1	2 (14, 15)
24	1	1 (8)
25	1	1 (16)

terms (for example, “how do you use the device?” was typically modified by parents in ways such as “how do you use Alexa?”). Parents of children in this age group supplemented answers with additional descriptions of device use and their experience of their children’s level of understanding of how to use the devices. Children in this age group were able to think about, and talk through, how the devices they were familiar with might work – or make clear to the interviewer that they did not know.

Children roughly between 6-10 would participate with a parent on- or off-screen. This provided reassurance to the child that it was safe and appropriate to answer the questions posed by the interviewer (who was, of course, a stranger to them). In particular, children in this age group would not always give full answers to questions, so parents would prompt fuller explanations from their children when they recognized this was needed. Children of this age did not seem particularly inhibited by their parents’ presence, with at least one child quite happily discussing talking to strangers online, much to the shock of their parents, despite sitting right next to them. Children were able to think through how devices might work, apply concepts they had started to learn at school, and had some idea of risks that might come from the Internet, if not home IoT devices.

Children older than 10 or 11 were able to hold a conversation by themselves with the interviewer, with little to no interaction with the parents as they were interviewed. In the case of children in this age group, many commented that they had become used to talking this way as a result of COVID-19 lockdowns and home schooling in particular. Older children often also listened in to their parent(s)’ responses, which sometimes promoted broader discussions between the parent(s) and the child(ren) about the question being asked.

Interviews were carried out by the first author of the paper, audio recorded and transcribed. The transcripts from the interviews were subjected to inductive thematic analysis [8] by the first



two co-authors of the paper. Such thematic analysis allows relative freedom for researchers to distinguish, and then refine, themes as the data is reviewed, rather than starting from a point of pre-determined coding framework. This provides a flexibility that is important when trying to ascertain significant themes that may otherwise be overlooked. The authors undertaking the coding performed the process entirely independently, met to review similarities in the generated codes, and discussed differences. After the discussion, both coders refined their code books individually, and a subsequent analysis of similarity generated a Cohen’s *kappa* value of 0.63, indicating a substantial level of agreement. The agreed-upon codes, with description of primary sub-codes, can be found in Appendix B.

## 4 FINDINGS

### 4.1 Survey

Participants reported owning 2,326 devices in total: the top ten devices owned overall are reported in Table 2. There are three types of devices that appear to be much more prevalent than others: smart TVs, smart speakers/home assistants and streaming devices (such as Google Chromecast devices and Amazon Fire sticks), with 1,181 of these three devices being recorded.

Participants subsequently gave detailed information on 886 of these devices: the top eleven types of devices where participants gave detailed information reported in Table 3.

*4.1.1 Summary of findings.* This paragraph gives a high-level overview of the survey findings presented below. Devices that are usually more expensive or integral to the household (e.g., Smart TVs, refrigerators) were reported as being less new than other devices. Participants mostly bought devices after reading online customer reviews; despite over half responding that they received detailed instructions, the majority of participants could not provide significant details about cyber security requirements, either at set up or throughout device life. Participants’ primary concern about the device breaking was around the cost of replacement, not the implications for data security.

Participants reported, on the whole, neither helping the children in the household with the device, or having concerns about children using the devices. This was especially the case for older participants, or where there were older children in the family.

Participants overwhelmingly reported getting information for cyber security information online; the majority of participants were not aware of having been the victim of a data breach or cyber crime, or if the manufacturers of any of the devices in their home had ever reported a breach. Reported learning at school and that discussed at home focused more upon online safety than cyber security steps: despite men being more likely to say they managed devices in the home, they were less likely to show knowledge of the children’s school curriculum. Older participants seemed to be more likely to discuss cyber security strategies (rather than online safety) with their children.

*4.1.2 Quantitative Analysis.* As a result of the largely categorical nature of the variables in the survey, alongside descriptive statistics, the results were analyzed using chi-squared tests of independence to determine any associations between three of the main demographic variables and different survey variables. The demographic variables considered were: the age of the participants (based on the age ranges of 30 and below, 31-40, 41-50, 51 and above) and the age of the oldest child (based on the age ranges of 0-5, 6-10, 11-15, 16-18) and the gender of the participant responding to the survey (male, female).

For the purposes of the chi-squared tests of independence, one record, of the one participant that answered “prefer not to say” in relation to their gender, was excluded as an outlier so as not to unduly influence the results. The sample size (*N*) used for calculation is different depending upon whether the question responded to was about a specific device, or about the participant and their

family in general. For questions relating to the device, the sample size is the responses provided ( $N = 884$ ); for questions relating to the participant and their family, the sample size is the number of participants ( $N = 552$ ). The alpha value used throughout is  $< 0.05$ .

We had the following hypotheses:

**The null hypothesis:** There is no correlation between the particular demographic groups and how parents behave, in relation to their children and their use of IoT devices, portrayed through the survey question's variables.

**The alternative hypothesis:** There is a correlation between the specific demographic variables and the compared survey variables.

Those results that were statistically significant, and where, therefore, we could reject the null hypothesis, are detailed below.

#### 4.1.3 Responses about devices.

**Age of devices.** Although there was a relatively even spread in the age of devices (0-6m: 18.40%, 6-12m: 24.94%, 1-2 years: 27.43%, 2+ years: 29.23%), it was notable that 139 of the Smart TVs (40.17% of the 346 smart TVs considered in the detailed questions) were recorded as being over 2 years old. Although with much smaller reported numbers, 100% of connected refrigerators/freezers (3 reported) and 55.56% of connected washing machines and tumble dryers were bought two years ago or earlier (5 of 9 reported). These larger devices, which cost more and are considered to be a standard fixture of a family home, are not only less new than many of the other devices in the survey, but were reported to be bought in spite of the smart/connected features frequently. 2 of the 3 refrigerator/freezers were not bought for the smart features, along with 4 of the connected washing machine/tumble dryers, and 66 (19.08%) of the smart TVs.

Table 2. Top ten reported device types

Device type	Number owned	Percentage of all devices
Smart TV	437	18.57%
Smart speaker + home assistant	414	17.55%
Device connecting smartphone to TV (e.g., Chromecast)	330	14.02%
Smart meter	134	5.69%
Smart printer	130	5.52%
Connected children's toy	107	4.55%
Smart lighting	96	4.08%
Connected smoke detector	89	3.78%
Connected thermostat	84	3.57%
Connected doorbell	82	3.48%

**How devices were researched prior to purchase.** Respondents gave some insights into how they found reviews for the devices they were answering for. Participants either did not, or did not remember, researching 226 (25.51%) of the devices. Across the remaining devices, 572 (64.56%) devices were bought after reading "customer reviews on the Internet"; this option far outweighed more typically trustworthy means of ascertaining reviews, with only 116 devices (54 of which were smart TVs) being bought after the participant read a review from a consumer protection body such as Which?, the UK consumer protection body.<sup>8</sup> Much more important seems to have been the cost of devices relative to alternative products (this being a consideration for 316 of the devices), as well

<sup>8</sup><https://www.which.co.uk/>

Table 3. Top eleven devices: detailed participant response

Device type	Number in depth questions answered about	Percentage
Smart TV	346	39.05%
Smart speaker + home assistant	207	23.36%
Device to connect smartphone to TV (e.g., Chromecast, Fire Stick)	106	11.96%
Connected doorbell	39	4.40%
Connected children’s toy	33	3.72%
Smart meter	29	3.27%
Connected thermostat	18	2.03%
Smart printer	18	2.03%
Smart camera	16	1.81%
Connected smoke detector	13	1.47%
Smart lighting	13	1.47%

as what the device looked like (a consideration for 226 of the devices), and whether the device was compatible with other devices in the home already (200 devices).

**Who managed the devices?** Devices reported on in the survey were typically managed by one individual, whether adult or child (633 devices; 71.44%). The decision for one person to manage these devices was reported as being intentional in 59.87% of the cases (for 379 of those 633 devices). There was a relatively equal split between whether people intentionally decided how their device would be managed, with participants either confirming that there was no active decision making process for management (or that they could not remember this decision being made) for 428 of the devices (49.42%). Despite this, there were only 6 reported devices where the status quo had caused issues, ranging from disagreement over device use, to forgetting passwords (0.68%). There was a statistically significant relationship between gender and reported management of the device<sup>9</sup> ( $\chi^2(4, N = 884) = 57.21, p < .001$ ), with the data showing that men were more likely to say they had sole ownership of managing the device (62.8% for men against 39.3% for women).

**Security at the point of device setup.** The survey asked participants if they had received “detailed instructions” about how to set up their device. They responded that 536 of the 886 devices (60.50%) did have, with physically printed instructions included with 365 of the devices; 151 devices had prompts to visit a website, the remainder had a combination of both options. In one case, the instructions were also given by the retailer. The phrase “detailed instructions” was left deliberately vague for participants to interpret as they found appropriate. The survey showed that across all participants an overwhelming majority of users did not know when their devices were supported until – this was not known for 843 (95.15%). Having “detailed instructions” made little difference to this figure: of the 536 with such instructions, participants reported not knowing the supported life of 505 (94.22%) of them.

The majority of users did not remember set up involving a password change: 495 devices (55.87%) did not require a password change, and respondents did not remember for 196 of them (22.12%). Other activities that are linked to the security and privacy of the device are also poorly understood by users: respondents did not know how to delete personal data from 685 devices (77.31%). There was a statistically significant relationship between gender and whether the participant knew how to delete personal data from the device or not ( $\chi^2(1, N = 884) = 7.97, p < .005$ ); men were more likely

<sup>9</sup>With the options for management of the device being managed by: “me” (the participant), “another adult”, “a child”, “no one person in the household” or “a landlord”.

to report understanding how to delete data from the device (29.6% for men; 20.4% of women). When asked to give their concerns, should the device break tomorrow, participants were overwhelmingly concerned about replacing the device (67.16% of all devices), not over whether the data they had provided would become inaccessible to them (12.87% of all devices), or subsequently deletable (0.23%, just 2, devices).

**4.1.4 Family Use.** Respondents were asked about the type of help that they provided their children to use for each device they answered questions about. For 687 of the devices (77.54%), respondents suggested that they felt no need to give help to their children. When they did give help, parents reported explaining how to interact with the device the most (93 devices, 10.50%); in the case of 83 devices (9.37%), respondents suggested that they managed their children’s usage to avoid physical damage, or damage to the service the device provided. Respondents felt that they had no concerns about their children using the devices for 572 (64.56%) of those devices surveyed, and indeed, children were reported as using 682 of the devices (76.98%) by themselves, with very few reported issues.

**Older participants provide less help and have fewer concerns.** The age of participants was shown to be statistically significant in terms of both helping children with devices<sup>10</sup> ( $\chi^2(12, N = 884) = 67.18, p < .001$ ), and being concerned that children in the home may damage the device<sup>11</sup> ( $\chi^2(6, N = 884) = 31.21, p < .001$ ). In particular, the amount of help given to children seems to decrease as the age of the parent increases, and the same is true of the concern around breaking the device. For further detail, see Table 4.

Table 4. Age ranges of adult participants and interactions with their child(ren) (percentage based on all responses to the question by age range)

Age range of participant	Children do not get help with devices	Percentage	I am not concerned about children breaking the device	Percentage	Children learn about cyber security topics that could be applied to devices at school	Percentage	I talk to children about cyber security topics that could be applied to devices at home	Percentage
30 and under	28	52.8%	26	49.1%	5	20.8%	14	58.3%
31-40	264	75.0%	199	58.5%	68	30.2%	125	55.6%
41-50	302	79.3%	256	67.2%	113	47.1%	165	68.8%
51 and over	92	92.0%	82	82.0%	42	65.6%	49	76.6%

**The presence of older children makes for less help or concern for all children.** Similarly, the age of the oldest child in the family seems to make a difference to how the participant reported the help they provided or concerns they had for all of their children. When chi-square tests of association were applied to the eldest child a participant reported as having, there were statistically significant outcomes as to the generally reported levels of help given to children ( $\chi^2(12, N = 884) = 65.37, p < .001$ ), and concerns about breaking or damaging devices ( $\chi^2(6, N = 884) = 36.36, p < .010$ ), as well as whether the participant believed their children were competent with the device or not ( $\chi^2(3, N = 884) = 16.77, p < .001$ ). Survey participants with children in the oldest age range (16-17) were less likely, based upon the responses in the survey, to report giving help to any children in the family, or having any concerns about the children damaging the device. Interestingly, only when the oldest child was 5 or under was there a clear difference in the likelihood that the participants considered the children competent with the device. See Table 5 for more detail.

#### 4.1.5 Cyber Security in the Home.

<sup>10</sup>With the options for “who helps the children in the home” being “all/most of the adults in the home”, “another adult in the home”, “no one in the home”, “just me in the home”, or “I don’t know” (where ‘me’ and ‘I’ refer to the participant).

<sup>11</sup>With the options being “I have concerns”, “I do not have concerns”, or “the children do not use this device”.

Table 5. Age of oldest child and perceived ability (percentage based on all responses to the question by age range of oldest child)

Age of oldest child	Not concerned about breaking device	Percentage	No help given with device	Percentage	Is competent with the device	Percentage
Between 0-5	19	36.5%	22	55.8%	28	53.8%
5-10	157	56.7%	183	66.1%	217	78.3%
11-15	251	66.8%	313	83.2%	297	79.0%
16-17	136	75.1%	161	89.0%	140	77.3%

**Where do users get support?** There was a wide spread of answers to the multiple response question “Who or where do you turn to for support with digital technology use”. 406 respondents (73.29% of the total number of respondents) said that they would turn to the Internet for support, with 217 respondents (39.17%) saying that they would also turn to other adults within the household. 64 respondents (11.55%) suggested that they needed no support, with similar numbers turning to friends (73, 13.18%), family outside the household (65, 11.73%) or children within the home (72, 13.00%). Very few respondents said that they made use of paid support (6, 1.08%).

**Cyber crime and its effects.** The vast majority of participants had not, or did not believe that they had been, the victim of a cyber crime at any point (457, 82.50%). Of those that responded that they had, 26 reported having suffered a financial loss as a result. 65 said they had not, with 6 saying that they were not sure. 503 respondents (90.79%) said that they were unaware of manufacturers of devices that they owned ever having reported a security breach.

**How is cyber security discussed at school and home?** The survey also looked at the parents’ understanding of what children learned at school about cyber security and Internet safety. The most common themes were “cyber bullying” (411, 74.19%), “stranger danger” (396 respondents, 71.48%) and “harmful online content” (390, 70.40%). More traditional cyber security themes were much less frequently recorded, e.g., “use of strong unique passwords” by 194 (35.02%) and “malware” by 107 respondents (19.31%). 87 respondents (15.70%) said that they were unaware of what their children had learned at school. There was a statistical significance between the age of the participant and the knowledge of those types of themes associated with home IoT device use<sup>12</sup> ( $\chi^2(6, N = 552) = 35.99, p < .001$ ) (see Table 4), and also the gender of participant and the knowledge of these themes ( $\chi^2(2, N = 552) = 12.27, p < .002$ ). The data shows that the older a parent is, the more likely they would be to report such themes; women (44.6%) were more likely than men (31.7%) to do so, too.

Finally, the survey reviewed discussions held at home by families about cyber security, and the Internet. 481 respondents (86.82%) reported having discussed the importance of not talking to strangers online. Other topics were far less uniformly discussed. 245 (44.22%) had discussed “what data might identify or reveal about you”, and 212 (38.27%) had discussed the use of strong and unique passwords. 27.98% of respondents (155) had had discussions about how to minimize the risks of becoming a victim of malware. There was a statistical significance between the age of participant and the likelihood to discuss topics such as passwords and malware, instead of topics more closely linked to safeguarding, such as stranger danger<sup>13</sup> ( $\chi^2(6, N = 552) = 17.73, p < .007$ ).

<sup>12</sup>With the participant responses being gathered into topics that were home IoT device related (strong password use, data management practices, malware, cyber crime, personally identifiable data), those that are not home IoT device related (stranger danger, harmful online content, cyber bullying) and “I don’t know”.

<sup>13</sup>As with the school test described in the previous paragraph, the participant responses being gathered into topics that were home IoT device related, those that are not home IoT device related and “I don’t know”.

The older the age range of a participant is, the more likely they would be to report discussing those topics more closely aligned to cyber security aligned to home IoT device use — see Table 4.

## 4.2 Interviews

**4.2.1 Summary of findings.** This paragraph gives a high-level overview of the interview findings presented below. Both parents and children talked about threats and risks in the language of online safety — stranger danger, cyber bullying and so on — and scams, without association to the home IoT devices that they were discussing. The ability for children to spend money through home IoT devices was recognized by both parents and children, but often not acted upon until the children had spent money without permission. Other types of financial fraud were not taken particularly seriously by parents (and was not considered at all by children) as the mechanisms for reimbursement through UK financial institutions were considered to be robust. Data loss from IoT devices was not raised as a concern.

Much as with their description of risks and threats, families described discussing online safety issues, when asked about how cyber security was discussed at home. Evidence of robust cyber security knowledge was relatively limited among both adults and children, with application of that knowledge poorer still. Much stronger concerns arose, from both parents and children, about other aspects of home IoT device use — not security or privacy, but the costs of the devices, the interoperability capabilities of the devices, and the necessity of careful use to extend out their useful life.

### 4.2.2 What do families consider the threats and risks of home IoT device use to be?

**Stranger danger, scams: the same threats as posed by using the Internet directly.** All interviewed families did not differentiate between the threats and risks that home IoT devices pose, compared to other digital technologies that allow you to browse the Internet, and connect to social media in particular. Participants, too, presented no understanding of specific threats based upon their personal situation, but rather focused on generic threats with no clearly defined adversary.

The most talked about threat was that of “stranger danger” and that of inappropriate online contact with strangers. This is less applicable to home IoT devices, which participants recognized (“*Well, you can’t chat to anyone on the [Amazon Fire] stick.*” (C5, aged 10)). The second most commonly considered threat was that of financial loss, through falling victim to scams, e.g., “*... giving your password, your bank password, to someone and they then transfer all your money out. That kind of thing, I suppose. I can’t think what else they could do that would bother me that much, or as much as that*” (AF2). This was a risk that parents felt strongly, and children were much less cognisant of, with suggestion that this was because they were not individually capable of managing their own finances. Interestingly, children who had seen attempted scams were likely to recognize them as such precisely because they targeted accounts they were not old enough to have (“*...I’ve got like, 10 [text messages] this week [telling me that] my PayPal account has been hacked...but I don’t even have an account.*” (C13, aged 12)).

Some parents felt that they could rely upon being reimbursed, should financial fraud occur, which minimized the harm (“*... my PlayStation 4 account was hacked. And they spent a lot of money. I got it all back. It was fine.*” (AM9)); this was from an expectation that any form of fraud would be reversed, or at least properly investigated, by traditional financial services firms, such as banks and credit card companies (“*... [if] someone’s in your bank account, you’d call your bank, and they’d resolve it*” (AM7)). A couple of adult participants had experience of fraud through less traditional

financial services firms, such as PayPal:<sup>14</sup> “*I just noticed all this abnormal spending activity. PayPal weren’t particularly interested, I have to say.*” (AF8). The participant here was not reimbursed.

**Unauthorized spending on devices is not as concerning as fraud.** Unauthorized spending on devices did not appear to be considered “financial fraud” for our adult participants, despite being a much more possible threat of home IoT devices. Perhaps as a result of being interviewed during periods of COVID-19 lockdowns, limiting the number of people that could enter the home, any unauthorized spending was considered almost exclusively in terms of children in the home, and as such was considered to be a restriction that parents should manage, even if they were unaware of the ability to do so: “*Oh yes, ... you ended up spending £5 on some terrible game, because we hadn’t yet realized we’d not blocked it ...*” (AF6). The prevailing feeling, even among the children who discussed it, was that children might be expected to spend money accidentally when using devices, without realising what they were doing (“*I’ve got a password for my profile...so I don’t spend money by accident.*” C22, aged 8). Those with family accounts on shared devices described instances of receiving an email about online purchases made by the child’s account, and having to have a discussion with the child after the event. Only in one instance did a parent give an example of making the child repay the cost of the downloaded goods – a significant sum was spent on video games, by chance in the run-up to the child’s birthday, making paying the parent back with money received as gifts a straightforward event. Had it been any other time of the year, the child would not have had the money to repay the parent.

**Data loss is not an active concern.** Participants did not exhibit particular concerns about the loss or theft or data of themselves or on behalf of their family from any devices (home IoT or otherwise), or even the ongoing use of personal data by devices and their manufacturers. Some adult participants were sanguine about data loss, e.g., by saying “*we all just live now assuming that our data has been stolen and [we are] waiting for something bad to happen*” (AM23). Children, too, exhibited signs that they were aware of the risks of making their personal data available to others, whether through accident or design. In answer to the question “what is the biggest risk of using home IoT devices?”, some children responded as follows: “*Your information being shared and people knowing what you do on the Internet...because you could get hacked or something*” (C10, aged 13); “*I think, just accidentally giving my information*” (C12, aged 13), “*Accidentally sharing information that is going to come back to you and put you at risk*” (C23, aged 15). Children interviewed under the age of 13 did not talk about data loss as a risk.

Two families with more hands-off devices, such as robot vacuum cleaners, smoke alarms or thermostats, seemed genuinely puzzled by the notion that they would discuss these devices with their children, or that there would be security implications. In both cases, the children were typically reported as being interested and disruptive with the devices for a period, then ignoring them. Upon pressing, one parent explained their thought process about the smart thermostat: “*I would teach them to use it in the same way I would teach them to use anything else ... as [child] gets older, I would like him to load the dishwasher ...*” (AF9). When the time came, they would be showing their children only how to use the manual overrides for the smart devices in the home, not expecting them to use apps, or have any more significant control over the management of the data. When asked about data collection from smart home devices, this family felt comfortable with their expected data use by the manufacturers: “*I know they collect all the information. I know they try and use it to make money.*” (AM9). Another participant, heavily bought into the Amazon ecosystem of home IoT devices, expressed frustration that the most effective way to limit data collection, or to opt out of

<sup>14</sup>PayPal explicitly explains that, because of its choice of location and registration for UK business, “The nature and extent of consumer protections may differ from those for firms based in the UK.” [51]

data use for improvement, was to activate a setting that might see them not receive future features: *“I changed some settings in the app that stopped them because they can listen to your recordings ... And you can turn off the ability for them to listen to it. It’s like a weird setting because it comes up with an option that says why you might not get any of the new features if you turn this off, and I’m like, ‘I like new features!’”* (AM16).

**Linking “hackers” to Internet, not home IoT device use.** Some children considered “hacking” to be the biggest risk, but could not necessarily explain what hacking meant, who might hack or what “being hacked” might look like in anything more than vague terms, e.g., *“they can change your password, so you cannot log into anything”* (C24, aged 8) or *“to me hacking means all data is stolen then it is sold”* (C18, aged 10). Children also framed this data capture in terms of smartphone or social media use (*“... phones have, like, tracking information, so they know where you are”* (C13, aged 12)), rather than home IoT device use. Several parents were unsure whether younger children recognized that home IoT devices connected to the Internet in similar ways to computers or smartphones (*“They don’t understand that Alexa is connected to the Internet.”* (AF20)). When asked, most children were confused by the question of how a home IoT device might work: *“[Alexa] is a program. So people put in questions and answers. So yeah, it’s like Google.”* (C10, aged 12); *“It’s a good question. I don’t know. It’s magic!”* (C23, aged 15). Children seem to have a level of knowledge about data collected when using the Internet directly, but are at risk of not making the link between personal data collection, potential misuse and home IoT devices.

**Threats to the home.** No adult participants raised potential threats to the home from home IoT devices, whether in terms of facilitating burglary or other physical damage. Conversely, two sets of parents explained how their connected home surveillance systems had enabled assistance in arresting a burglar in their neighbourhood (*“We were able to send pictures to the police.”* (AF2)), and in feeling more secure after past events around the house (*“I think just having it there prevents things.”* (AF19)). Children seemed to be more aware of physical damage that might arise from devices, and considered these risks more urgently than risks to personal data in two cases: *“There are a lot of things plugged in down there — they could set fire!”* (C19, aged 12); *“I think the most dangerous thing is getting water inside it...that’s the only thing that’s dangerous about it.”* (C5, aged 10). These concerns were not shared by their parents.

#### 4.2.3 Cyber security knowledge gathering, sharing and adherence within the family.

**Discussion as a family...** The most common way that interviewed families reported themselves managing any type of cyber security was through discussing it as a family. Should a child want to use a new app or device, many families expressed a process of discussing guidelines — length of use at a time, who and how they could communicate with people, what they could download, for example. Despite bringing the topic up when asked about cyber security, families recalled talking more spontaneously about online safety issues that they saw arising from the Internet (posting inappropriate content, not talking to strangers) than more strictly cyber security issues. Whether explicitly understood by the parents or not, the importance of a trusting relationship for this type of discussion was clear: *“... we talk to them a lot, and tell them to tell us in any situation”* (AF7). Children often referred to asking or learning from parents when they were unsure (*“I just call Mum and Dad”* (C7, aged 7), *“I [watch] my parents do it”* (C11, aged 14)).

**...but not about home IoT device security.** There were no reported instances of interviewed families discussing home IoT device security together. Some parents suggested that they might use items in the news as a means of having conversations about specific security topics with their children, although, when asked about what news stories they had seen recently that made them



consider their own home IoT setup, no one interviewed pointed to a specific story about a home IoT device being compromised. Neither parents nor children could explain, when asked, in much detail, as to how the devices they used worked: *“I don’t actually know — no one has ever asked me that question before.”* (C17, aged 8). Yet parents seemed to assume that at some point there would need to be a discussion, without taking steps to understand the technology further. As AF5 explained: *“What I’m guilty of is I don’t really think about it in any depth. You know, and probably because my children are still fairly young that you don’t sort of think any further than what you need to.”*

Some parents with a larger age gap between children reflected how they seemed to have missed having conversations with their older, teenage children, because advances in digital technologies had happened relatively recently. Conversely, their younger children seemed to have grown up with, and just “understood” core functionalities of devices in the home instinctively, expecting devices to have touch screens and to stream programs on demand, for example, without understanding the technologies behind the device: *“He knows what he’s doing when he’s looking at it, but ask him what he’s done. He wouldn’t be able to tell you.”* (AM24).

**Children’s awareness of cyber security.** All children recalled that they had had classes at school about certain aspects of computer use. Most talked of having annual reminders of “stranger danger” and “cyber bullying”, and using programs such as *Scratch*<sup>15</sup> to learn programmatic thinking and the fundamentals of coding. Only one child actively discussed being taught about malware (C23, aged 14). No children reported being taught about IoT products at all, with one child commenting that *“It would be nice to know just how different technologies worked, not just spending all the time on computers”* (C2, aged 12). Many children found school’s approach *“all common sense stuff”* (C7, aged 11), and *“just talk[ing] about the same thing every time”* (C5, aged 10).

Most children interviewed indicated that they knew something about strong passwords, but typically had one core password that they used (*“I have my passwords all the same, so I remember it! But if you hack one account, you hack all of them!”* (C13, aged 12)), varying them should they need to share details with others (*“... if my friend and I may want to make an account where we all have access, I will use a password that is not my original password.”* (C5, aged 10)). Beyond this, children exhibited little cyber security knowledge that could be considered specific to home IoT devices: one child had read an article about how to delete their search history from their smart home assistant: *“I think I probably just saw something about it like on social media: ‘This is how you stop your Alexa from knowing all your secrets.’”* (C23, aged 14).

Seven families had instances where a child expressed knowing more than a parent about the Internet generally, or specific security features. In these instances, children pointed out gaps in their parents’ knowledge, but gave no indication that they would be expected to teach or help their parents further. For example, C13 (aged 12) showed frustration that his mother *“didn’t understand the safe tick”* that the anti-malware software they used provided to show the safety of websites. AF13 followed this by saying *“you’ll have to show me!”*, suggesting that the willingness to learn may be present, but not necessarily obvious to the child. Despite the suggestion that children may be on a par with their parents, there was no instance where a family expected the child to have a part in the security or management of communal devices, even if the child had an interest or exhibited accurate knowledge about security.

**Parents’ awareness of cyber security.** Ten of the adults considered themselves to be quite confident in the security of their homes. Either they thought themselves *“fairly savvy on things”* (AF1) or felt confident that devices come ready prepared to avoid any kind of security breach *“Well, I suppose a lot of the devices such as the Echos ... those kinds of things that kind of come pre-set up to*

<sup>15</sup><https://scratch.mit.edu/>

*be defensive*" (AM2). AM16 was aware of the potential for insecure home IoT devices to be used as a means of getting access to an entire network, but put faith in well-known devices: *"I read something about someone who put a Wi-Fi kettle on their network, and then someone had hacked into it ... and gained access to the whole [network] ... It can be a bit dodgy, but I trust the Amazon system, the Alexas ..."* Participants that were confident of their abilities to secure computers did not provide evidence of having more security measures set up for smart home devices (for example, discussing guest networks, non-standard router settings or additional home networking) than users who were not confident when asked. Almost all adult users, and some of the older children, suggested that, should they need to find information about any aspect of security, they would search online, and assess the responses based on their judgement or prior experiences: *"Slight cliché, but Google, Google, and then I look at what looks like a legitimate organization. I don't have like, a specific way in mind, but I think I'm able to tell based on you know, how the website looks."* (AF9).

When adults were asked how they would like to receive information about cyber security, answers ranged from getting it from trusted technology TV shows, popular UK consumer champions, private companies, or even school. There were some parents who thought that this might be the remit of the government, but were unclear where it might sit (Interviewer: *"Which areas of the government?"* AF25: *"I would say, probably [the Department for] Education ..."*), or if there was even sufficient budget for the government to do it usefully (*"...maybe the government but I don't know how the government actually have the resources."* (AF8)). AM3 reflected that it would be helpful if there was an *"NHS (National Health Service) for cyber security"*. The UK'S NCSC, who run the national security awareness campaign CyberAware,<sup>16</sup> was not mentioned by any participants.

**Parents' cyber security application.** Several adult participants expressed their inability to understand what is needed to secure the home and act accordingly, relying on other adults in the home (*"My husband brings stuff in the house and I have no clue. I can't tell you exactly what we've got ... I've got no clue how it works or anything about it."* (AF2)), or not thinking about it (*"I'm one of those people who probably doesn't think about security. I just go along until the disaster strikes and then yeah, I mean, obviously, I've got you know, passwords for our various things, but I mean, I don't sort of you know, think about it in that much depth."* (AF5)). Three adult participants equated being secure with having anti-malware software (*"Once I download it I am happy for the year."* (AF13)) – even when not being sure that it would carry over to the home IoT devices they had: *"... [using anti-malware software] was just kind of what got drummed into us when we were younger and when we first had computers, but with all the other kind of connected items, you just assume it's ... in there, I guess."* (AF6)). Other participants understood that anti-malware was not the sole means of keeping their home secure, and was not on their home IoT devices: *"I have Norton on everything apart from the TV."* (AF 17). This gap was noted as if the home IoT device did not require any additional protection. Some participants considered free anti-malware to be superior to paid-for versions (*"... I found a lot of them if you'd shop around the free ones are just as safe as the subscription ones. I mean, I swear on AVG Free for most of it. I still swear with that over £60 Norton every time."* (AM24)). Given the practice of selling the data of users of free antivirus software, this may, in fact, open the user up to different security issues [58].

**Where cyber security knowledge was lacking.** Only one interviewed adult participant used a password manager for themselves, with another participant writing passwords down in a notebook. Two other participants expressed awareness of password management software, but dismissed them as too complex and tricky, or incompatible with not having access to technology all the time (one participant, unable to use their smartphone at work, was unable to access their bank account

<sup>16</sup><https://www.ncsc.gov.uk/cyberaware/>

because the details were stored in the password manager). Other adult participants did not consider password management outside of their own memory a necessary practice. Some were confident that they could store a range of passwords adequately without further assistance (“*I’m fairly on the ball myself with it, to be honest, so I don’t ever see the need [for a password manager]*” (AM24)), many expressed some small discomfort, or guilt, at knowing that they did not follow guidance that they knew to be important (“*I have the same passwords pretty much. Just like a couple of letters changed. I’m terrible, yeah I know ...*” (AF21)). Those adults participants asked had not changed the password on their router (“*It’s too bloody long!*” (AM7); “*... I just put that in the too boring/too hard basket.*” (AF1)), and retained the router given to them by their Internet Service Provider. Children did not reference using password management software themselves, or having any discussion with their families about how to manage passwords of home IoT devices, and the potential for misuse when a single account is tied to a communal device.

Few interview participants, and no children, reported using multi-factor authentication (MFA). In the majority of cases where individuals did report using MFA, it was only done after being the victim of a cyber crime, resulting in fraudulent activity (“*[the experience] made me go and turn on 2FA*” (AM9)). MFA is, of course, less obviously used in home IoT devices directly, however equivalent steps, such as requiring a PIN for purchases through an account linked to a home IoT device, were typically not activated by participants. As with password management, there was no report of discussions within the family about the use and benefits of MFA.

Most adult participants were not completely sure as to whether their devices received automatic software updates, or whether they needed to be involved in the process. There were no participants who were aware of how long they expected their devices to be supported for, with some participants misunderstanding the question (“*[supported life] is probably similar to a normal energy bulb*” (AF16)). Software updating was not discussed between families as a necessary process. Three children mentioned the importance of automatic software updates — but only one in relation to a device other than their smartphone (an Amazon Fire Stick). Six adult participants talked of their assumption that updates were automatically done, and took little time to consider it: “*when they get notifications they’ll do it, but it’s not a conscious thing.*” (AF14, about the children in the house). Both adults and children expressed a desire to manage their device updates, either because they did not want to have their use interfered with in the moment (“*I feel like it’s an informed choice when I do things*” (AF2)) or because “*I feel like it slows the phone down*” (C25, aged 16).

**Other home IoT concerns: costs, interoperability.** A much larger concern than security, particularly for those with a larger number of home IoT devices, was how to expand their smart home within their budget, and keep devices functional for as long as possible. Some participants were proud that they had been careful with old smart home assistants that were still functioning: “*... none of [my Echos] have ever broken. Some of them I’ve had since right at the beginning.*” (AF19). One participant with a significant smart home set up recalled that, with individual devices being so expensive, building up a smart home system was a slow process involving second-hand devices and constant interoperability issues. Older devices that this family had did not have full functionality, compared to newer devices, suggesting being out of supported life. Another family, unaware of the security implications, talked at length about how these interoperability issues made life a little more frustrating and a little less smart than they would have liked (“*Having to have a bridge like that is really annoying...why does Phillips [manufacturer of smart bulbs] need a bridge [to work with other home IoT devices] when none of the others do?*” (AF19)).

There were agreed-upon strategies to ensure that children took care of their devices — some children recognized that a device broken by them would not be immediately replaced (“*I don’t want my [device] to break, because I won’t be getting another one!*” (C6, aged 6)), where other families

employed strategies such as this: “*We make them spend their own money on stuff like that. Hopefully promote a sense of like, you know, ‘I bought this, it’s mine and it’s my responsibility.’*” (AF7). Younger children in particular exhibited signs of friendship and care towards smart home assistants (“*[C4, aged 4] considers the Google Home part of the family...they have conversations in a very friendly way.*” (AM4)), or seeing them as integral (“*just part of our house*” (AM16)).

## 5 DISCUSSION

### 5.1 A misalignment of perceived and actual threats and risks

*5.1.1 Perceived threats and risks.* The interviews and the survey showed that families were happy to use and integrate home IoT devices in their homes, and did not take particular steps to inform themselves as to how to make these devices more secure. The underlying concerns of parents in particular, around stranger danger and financial fraud, suggest that they did not recognize the difference in threats and risks posed by home IoT devices, compared to using the Internet in a home computer. Children echoed this, speaking almost exclusively of threats posed to them on social media, and risks typically stemming from “hackers”, external to the family.

The adults and children interviewed had some level of understanding of how having home IoT devices increased the collection of personal data, and that misuse of such data by someone with malicious intent could be bad. The survey showed a complex relationship between the age of the participant and their actions in relation to their children — regardless of the child’s age: although, the older the parent, the more likely they were to report talking to their children about cyber security measures that could be applied to home IoT devices, they were much less likely to offer their children support with such devices. This shift perhaps reflects the adoption of digital technologies over time — younger parents, more likely to have experience of digital technologies as ubiquitous and for interacting with others, seem to focus more on the risks arising from this. The interviews and survey indicated several reasons for the lack of knowledge and subsequent action by participants. As indicated by the survey results, people did not notice news stories about their devices, and may miss stories of data leaks and other breaches, thus not taking actions when needed. The interviews highlighted how adults and older children were resigned to data being taken and occasionally leaked, and the survey results suggest that people are often unaware of, or immediately unaffected by any breach. Regardless of their feelings about this, if individuals want to use such devices, they have to accept the terms of use, which often requires full data collection to be turned on for complete device functionality. Furthermore, cutting corners with, or not using, cyber security measures rarely causes directly applicable, irreversible harms, which reduces the incentive to try to change.

*5.1.2 Actual threats and risks.* There is the overwhelming feeling that threats posed by home IoT devices are too impersonal and too remote for many people to feel compelled to take interest. It has long been considered that individuals do not find themselves interesting enough — or not wealthy or valuable enough — to be hacked [30]; in this light, it is understandable that the families interviewed spent more time discussing the much more manageable and realistic risks of talking to strangers and over-sharing personal data online.

It also does not help that stories, such as the home network being hacked through an insecure smart kettle, as mentioned by one of the interviewees, have a faintly ridiculous edge that undercuts the severity of having a home network compromised. Conversely, other potential threats that can arise from a malicious party accessing the types of data that can emanate from a smart home can be extremely distressing to consider, given the potential of harm to property and person, and how little the user might be able to do to protect the household. The 2019 incident of an individual hacking into a Ring camera in a child’s bedroom and pretending to be Santa, talking directly to the children

[45], is one such upsetting example. Not only is this reported to be an attack widely possible due to software especially designed and distributed for the purpose [12], but Amazon, the owner of the Ring device family, has refused to acknowledge their responsibility for the harm and distressed caused, blaming users’ insecure practices for facilitating the hacking [50]. The psychological harms of an event like this need to be appropriately considered when considering threats, particularly when taking decisions for, and discussing alongside, children or other dependents. Agrafiotis et al. [1], considered the range of potential psychological harms that may occur to victims of a cyber breach – ranging from embarrassment and discomfort, to shame, depression and guilt, over an extended time period. Within a family setting, these types of feelings can be difficult to discuss, or may affect different family members in different ways. The importance of effective cyber security measures – strong and unique passwords, and regularly updated software in particular – is even more important when manufacturers may cite a user’s lack of management of the security features to avoid liability.

Children interviewed did not report witnessing active risk management from their parents. The survey results showed the extent to which users did not know the details of their devices’ security features. The interviews showed that families did not routinely talk about cyber security strategies that home IoT devices may need to use, such as the deploying of password management strategies, using MFA or the importance of regular software updates. Additionally, women were less likely to manage the devices in the home, or understand how to use them, but take more ownership of understanding what their children learn at school, meaning that the parent that may be less capable or confident is the one overseeing the children’s education in relation to applicable cyber security. Instead, children are taught the importance of managing the cost of device use from their parents. Parents may look to second-hand devices to reduce the cost of expanding their smart homes, agree with their children that they must take care of those devices that they use, and use free security software. It is a common practice that software is free at point of use, but is monetized through strategies such as selling data collected about the users. This can be extremely invasive when software is designed to control an entire system, as is the case with anti-malware applications [18, 58]. Additionally, normalizing the downloading of free software may increase the chance of downloading a malicious app [66]; although directly a concern on smartphones, similar threats from careless downloading of skills (the smart home assistant equivalent of apps on mobile devices) have been shown to exist [38].

Parents promoted ideas of relying upon recognized consumer protection regulation, particularly in the case of fraud, but also in ignoring children who believed electrical safety could be an issue. Adults in the UK are accustomed to a rigorous consumer standards framework, with the ability to approach financial services firms for reimbursement where there is fraud without “gross negligence” [21], and levels of assurance around electrical safety.<sup>17</sup> Families also modeled behavior about extending device life through careful use. In a family context, this poses the problem that devices are not necessarily as secure as people might expect, leaving them open to attack in ways that may not be covered by consumer protection regulation, yet remain damaging to those affected.

## **5.2 Neither adults nor children have opportunities to learn appropriate cyber security information**

Both the survey and the interviews show the lack of appropriate education opportunities for both adults and children around cyber security. Children are more easily approached in school settings, but the status quo in the curricula applicable in the United Kingdom is not teaching appropriate

---

<sup>17</sup>Such standards include the Kitemark (<https://www.bsigroup.com/en-GB/kitemark/>) and the CE mark (<https://www.gov.uk/guidance/ce-marking>).

security for home IoT devices or capturing the interest of children. Those children interviewed found cyber education at school repetitive, learning little that they did not already know about some topics (notably the safeguarding aspects of Internet use), and little to nothing about security topics. This confirms the findings of Pencheva et al. [52], focusing on cyber security at school, who found that students generally are very tech-savvy, but treat online safety and cyber security as the same subject. The survey, furthermore, showed how important it is to ensure all children in a family receive the same education in a school setting, as it appears to be the case that the presence of older children in a home setting reduces the amount of attention given by parents to ensuring careful home IoT device use and secure cyber security practices of all the children.

Education for adults in this space, outside of formalized education, is extremely difficult to land effectively [3], and the efficacy of such education depends upon personal and social norms, in many respects. Our interviews did not get as far as asking what types of message would be personally effective for participants, given the basic lack of knowledge as to how the devices worked on the part of the participants. However, participants did give a suggestion of the types of organisations and groups that they would like to hear from. These ranged from the government and related bodies, to trusted people with influence (such as particular TV shows and consumer champions) or manufacturers. The reliance on turning to the Internet for advice shows a lack of knowledge that could possibly be bolstered by these channels. Of course, this depends on how well trusted organizations are, which is a factor that will change from country to country, as will the societal approach to parenting, and managing personal risks. As an example, Kritzinger et al. [36] found that, in comparing cyber security message approaches between the UK and South Africa, the UK’s messaging focused upon the responsibility of the individual to protect themselves, rather than being a communal effort. This ties in with the argument in Renaud et al. [53] that cyber security in the UK is becoming “responsibilized”, with individuals expected to manage their own risks. This is not a particularly unusual expectation, also seen in the USA [25], but, as the interviews showed, if individuals have inaccurate understandings of where and how they are protected, and what the actual threats and risks are, it is extremely unlikely that they will manage these risks effectively.

### **5.3 Recommendations to help families become more secure in their home IoT device use**

*5.3.1 Help families understand where to do better.* Without even a general knowledge, it is hard to take the next step of efficient threat management based upon personal situations. Extending the suggestions from Parkin et al. [48] and Emami-Naeini et al. [19], manufacturers must do more to make the key threats of home IoT device use clearer at point of setup, and periodically throughout device use. Documentation about major threats relating to personal data and device misuse, and the recommended baseline steps to mitigate these issues based upon the specific device may help to increase awareness in adult users, which can, in turn, trickle down to children. Manufacturers may also focus on providing this information clearly online, so that when users are faced with trying to improve their knowledge, official sources are plentiful.

Home IoT devices – particularly those that must have a reasonable expectation of use by multiple people, multiple generations, within a single location – should be provided with better guidance as to how to set them up for the situation it is located in. Every person, and every household has its own particular set of threats and risks that might make certain security options more or less appropriate for them; however, there will be certain baseline security features that should be promoted to users at the point of setup and periodically thereafter. Hiniker et al. [28] and Ko et al. [34] have shown that families are more likely to come to agreements over rules for Internet use if they agree upon these rules as a unit. Our findings agree with this: families instinctively use discussion as a means of managing potentially tricky areas for their children. However, previous research has shown

children and adults may use different words to discuss cyber security [33]. In addition, children may not perceive devices in the same way that adults do, not only, as our interviews showed, failing to understand they are connected to the Internet, but also in understanding how they work [71, 73]. As such, the expectation that using discussion either to agree about home rules about home IoT devices or as a means of providing children with additional knowledge will fail, without further guidance for both parents and children.

*5.3.2 Appropriate levels of base security measures for home IoT devices.* The evidence from the interviews in particular suggest that home IoT devices that are expected to be used by groups of people – especially children – should come with more stringent security measures set by default. For example, although some steps seem to have been taken by manufacturers to allow notifications when things are purchased, further work could make spending money and downloading items harder (requiring purchases to be confirmed with a PIN or other agreement from the primary account holder). Alternatively, a clear signpost to the potential risks of not protecting purchases at the point of setup, should be provided. The interviews show that, for example, adults in the UK are used to being protected by strong consumer protection measures that should cover most cases of fraud – but crucially, not “gross negligence” when, despite being the victims of fraud, they were deemed not to have taken the proper precautions [9]. Although adult interview participants were extremely concerned about financial fraud, few had enabled settings to limit purchases on applicable home IoT devices, and no family considered the ease with which significant sums of money could be spent fraudulently, potentially without recourse.

It must be recognized that there are proposed measures to mitigate some of the security aspects explored here, such as the UK’s Product Security and Telecommunications Infrastructure Bill, mandating some aspects of security by design in consumer smart products [64] and ETSI’s EN 303 645 baseline standard for consumer IoT [20]. Much like the devices they seek to legislate and standardize, these measures are nascent, and may well need to be extended and revised as the market matures. Policy makers should continue to analyze the ongoing harms arising from the increased ubiquity of such devices to understand whether more regulation or legislation may be necessary to protect consumers and specific groups of vulnerable people in the future. An example of regulatory focus on a particularly vulnerable group would be the UK’s Age Appropriate Design Code [32], which requires organizations to consider the safety of children explicitly, when providing those services within the UK. Acting unilaterally, as the UK government is in the case of [15] and [32], works on the assumption that the measures can be applied to – and enforced against – those devices that are for sale in the UK in a meaningful manner, despite home IoT devices being made, and sold, globally. Some small shifts have been seen in large online platforms’ age confirmation processes as a result of the Age Appropriate Design Code [27], but what the effect on the device market will be remains to be seen.

*5.3.3 Up to date education – for children and adults.* Parents and children interviewed and surveyed in this research portrayed the learning provided by school as focusing only on the Internet as a place for socialising and commerce. Curricula must be updated to capture not only the pervasive nature of the IoT, including exploring how the data collection from such devices is even more pervasive than that collected using the Internet, and also why the threats are different to the Internet accessed via a computer. Helping children be able to better comprehend what and who may actually constitute a threat, and how to apply knowledge about cyber security skills to manage such threats would be an excellent start.

However, enhancing school curricula is not enough to improve the cyber security knowledge within the home in the short term – not only do children not typically have the power in the familial relationship to engender change of their parents’ activities, but the accounts for the home

IoT devices are unlikely to be theirs to manage. As Blum-Ross and Livingstone [6] considered, the information exchange between school and parents is poor: there can be no expectation that parents would become significantly more knowledgeable simply because their children are learning more. Parents need to find means of educating themselves, and knowing how to extend this knowledge to their children, where the knowledge is not gained at school.

In the UK there is some expectation of support from the government for personal risk management. However, the interviewees showed a complete lack of awareness of the existence of the body tasked with supporting them with cyber security, the NCSC. There is an interesting case to be made for learning the public health messaging lessons deployed to spread messages around social distancing, and then the promotion of vaccination, in relation to COVID-19. The use of poster campaigns, short slogans and promotion of positive behavior by trusted members of society, whether in a personal capacity or through platforms such as TV shows or recognized websites may serve to normalize good cyber security practices. This should sit on top of school-based education, and would serve to provide knowledge that is currently unavailable to both adults and children alike.

*5.3.4 Better recognition that families try to look after their devices.* The importance of strong security practices becomes more important as countries, including the UK and the European Union, introduce rights to repair in law for certain home electronic goods, including televisions and refrigerators [26]. As these devices are expected to be repairable for up to ten years, so smart instances of these devices need to maintain appropriate software updates and usable security processes for this period. This must happen to ensure that users are not put at risk for being careful with their devices, and that children do not need to learn that the ability to have devices on a budget does not come at the expense of its, and their, security.

## 6 LIMITATIONS AND FUTURE WORK

As often happens in research relating to the home and family life, there was an over-representation of women participating in both the survey and the interviews. Although this may serve to skew some responses, as women may have a tendency to underplay their technology knowledge [54], this is to some degree balanced by the input of other family members in the interview process. Additionally, although there is clearly going to be participant bias in terms of the type of person who would consider answering surveys on Prolific, this does not seem to have produced a respondent group who is extremely technologically aware, for example. It must be considered also that the research is focusing on technology that is, at present, largely discretionary in nature; as such the higher proportion of employed participants may not be entirely surprising.

As is the case with most research based around qualitative work, our findings can be said to be applicable to the situation that families found themselves in the UK, at the time of undertaking the research. Parenting methods, trust in government, governmental entities and consumer protections vary throughout the world: future work could be undertaken to understand where the findings of this piece of research may differ in other jurisdictions and regions globally. Taking the EU Kids Online survey as an example, which in its 2020 review looked at online behaviors of children in 19 EU countries [57], it may even be beneficial to scale such research up to look at the security differences in home IoT devices between countries: as devices are sold globally, so their use, and misuse, need to be understood globally too.

Future work should build on these findings as a means of engaging families more with the elements of cyber security they can discuss and manage appropriately as a specific multi-user case. In particular, work should look not only at what families can be expected to do, but what areas they do not consider significantly threatening enough to spend time managing, and which bodies should



be managing such risks. It is also necessary for further work to be done to integrate knowledge of home IoT devices and the cyber security risks that they pose, into school curricula, to make cyber security education more than an online extension of child safeguarding principles.

## 7 CONCLUSIONS

This research looked to answer two initial research questions: how families in the UK manage the cyber security of their home IoT device use, and how and when they learn and discuss cyber security for home IoT device use. We found that families have limited knowledge around the threats and risks of home IoT device use, falling back on more general knowledge about the risks of using home computers. Furthermore, parents showed much greater concern for modeling and teaching their children efficient and careful device use to extend the device’s life, in part because of the expectation of harm reduction and management through consumer protection regulation in the UK. We also found that children do not receive any education about the concept of the IoT, or cyber security as it should be applied to ubiquitous devices, as part of the school curriculum. These findings pose immediate concerns, in that home IoT devices do require different cyber security management than home computer use; in particular, the expectation of long device use may see families using unsupported, therefore insecure, devices, and the lack of friction around downloads and purchases especially may not be covered by consumer protection legislation as the interview participants may assume. This also has the potential to store up problems for the future: with no education from either home or school, children may grow up without a proper appreciation of how to keep home IoT devices safe.

We discuss how the UK has a relatively individualized approach to personal risk management, albeit with an understanding that governmental agencies and legislation will protect consumers from most active threats. Specifics will change, based upon where citizens of any particular jurisdiction place their trust, but increased messaging from trusted local sources must be leveraged to improve adult knowledge, on top of incorporation of learning about the IoT, and effective cyber security measures, during a child’s school life. In addition, manufacturers must present more details as to the threats, and the specific mitigation factors for their devices, so that, even in the face of a lack of education from the state, individuals can make decisions that are truly representative of the threats and risks to their own families.

## REFERENCES

- [1] Ioannis Agraftotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4, 1 (10 2018). <https://doi.org/10.1093/cybsec/tyy006> arXiv:<https://academic.oup.com/cybersecurity/article-pdf/4/1/tyy006/27126934/tyy006.pdf> tyy006.
- [2] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. 2020. You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships. arXiv:2001.10608v2 [cs.HC]
- [3] Maria Bada, Angela Sasse, and Jason R.C. Nurse. 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. In *Proceedings of the 2015 International Conference on Cyber Security for Sustainable Society*. Sustainable Society Network+, 118–131.
- [4] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders’ Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet*. USENIX Association, 14 pages. <https://www.usenix.org/conference/foci20/presentation/bernd>
- [5] Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing Expectations: Technology Tensions among Parents and Teens. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 1388–1399. <https://doi.org/10.1145/2818048.2819928>
- [6] Alicia Blum-Ross and Sonia Livingstone. 2020. *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children’s Lives*. Oxford University Press.
- [7] John Blythe and Shane Johnson. 2019. A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal* 2019 (2019), 97–125. <https://doi.org/10.1057/s41284-019-00211-8>

- [8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- [9] Miles Brignall. 2020. Bank fraud: couple lose £43,000 but can't get a refund. News report, The Guardian. <https://www.theguardian.com/money/2020/feb/08/bank-couple-lose-43000-but-cant-get-a-refund>
- [10] Sara Cannizzaro, Rob Procter, Sinong Ma, and Carsten Maple. 2020. Trust in the smart home: Findings from a nationally representative survey in the UK. *PLOS ONE* 15, 5, Article e0231615 (2020). <https://doi.org/10.1371/journal.pone.0231615>
- [11] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. “It Did Not Give Me an Option to Decline”: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. Association for Computing Machinery, New York, NY, USA. <https://doi.org/10.1145/3411764.3445691>
- [12] Joseph Cox and Samantha Cole. 2019. How Hackers Are Breaking Into Ring Cameras. News report, Vice. <https://www.vice.com/en/article/3a88k5/how-hackers-are-breaking-into-ring-cameras>
- [13] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents’ and Teens’ Perspectives on Privacy in a Technology-Filled World. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*. USENIX Association, 19–35.
- [14] Department for Digital, Culture, Media and Sport, UK Government. 2018. Code of Practice for Consumer IoT Security. Governmental report. <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>
- [15] Department for Digital, Culture, Media and Sport, UK Government. 2020. Consultation on regulatory proposals on consumer IoT security. Public consultation document. <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>
- [16] Department for Education. 2013. National curriculum in England: computing programmes of study. Web page. <https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study>
- [17] Nils Ehrenberg and Turkka Keinonen. 2021. *The Technology Is Enemy for Me at the Moment: How Smart Home Technologies Assert Control Beyond Intent*. Association for Computing Machinery, New York, NY, USA. <https://doi.org/10.1145/3411764.3445058>
- [18] Anirudh Ekambaranathan, Jun Zhao, and Max Van Kleek. 2021. “Money Makes the World Go Around”: Identifying Barriers to Better Privacy in Children’s Apps From Developers’ Perspectives. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) (CHI ’21). Association for Computing Machinery, New York, NY, USA, Article 46, 15 pages. <https://doi.org/10.1145/3411764.3445599>
- [19] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 ACM CHI Conference on Human Factors in Computing Systems*. ACM, Article 534, 12 pages. <https://doi.org/10.1145/3290605.3300764>
- [20] ETSI. 2020. CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. European Standard REN/CYBER-0048. [https://www.etsi.org/deliver/etsi\\_en/303600\\_303699/303645/02.01.01\\_60/en\\_303645v020101p.pdf](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf)
- [21] Financial Ombudsman. 2021. Fraud and scams. Web page. <https://www.financial-ombudsman.org.uk/consumers/complaints-can-help/fraud-scams>
- [22] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or Do Not, There is No Try: User Engagement May Not Improve Security Outcomes. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*. USENIX Association, 97–111.
- [23] Radhika Garg and Subhasree Sengupta. 2019. “When You Can Do It, Why Can’t I?”: Racial and Socioeconomic Differences in Family Technology Use and Non-Use. *Proceedings of the ACM on Human-Computer Interaction* 3, Article 63 (Nov. 2019), 22 pages. <https://doi.org/10.1145/3359165>
- [24] 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, Article 268, 13 pages. <https://doi.org/10.1145/3290605.3300498>
- [25] Julie Haney, Yasemin Acar, and Susanne Furman. 2021. “It’s the Company, the Government, You and I”: User Perceptions of Responsibility for Smart Home Privacy and Security. In *Proceedings of the 30th USENIX Security Symposium*. USENIX Association, 22 pages. <https://www.usenix.org/conference/usenixsecurity21/presentation/haney>
- [26] Roger Harrabin. 2021. ‘Right to repair’ law to come in this summer. News report, BBC News. <https://www.bbc.co.uk/news/business-56340077>
- [27] Alex Hern. 2021. TechScape: How the UK forced global shift in child safety policies. News report, The Guardian. <https://www.theguardian.com/technology/2021/aug/18/uk-governments-child-safety-regulation-leads-to-global-policy-shifts>
- [28] Alexis Hiniker, Sarita Y. Schoenebeck, and Julie A. Kientz. 2016. Not at the Dinner Table: Parents’ and Children’s Perspectives on Family Technology Rules. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 1376–1389. <https://doi.org/10.1145/2818048.2819940>

- [29] Duncan Hodges. 2021. Cyber-enabled burglary of smart homes. *Computers & Security* 110 (2021), 102418. <https://doi.org/10.1016/j.cose.2021.102418>
- [30] Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. 2012. The Psychology of Security for the Home Computer User. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*. IEEE, 209–223. <https://doi.org/10.1109/SP.2012.23>
- [31] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Article 402, 13 pages. <https://doi.org/10.1145/3313831.3376529>
- [32] Information Commissioner’s Office. 2020. Introduction to the Age appropriate design code. Web page. <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>
- [33] Simon L. Jones, Emily I.M. Collins, Ana Levordashka, Kate Muir, and Adam Joinson. 2019. What is ‘Cyber Security’? Differential Language of Cyber Security Across the Lifespan. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Article LBW0269, 6 pages. <https://doi.org/10.1145/3290607.3312786>
- [34] Minsam Ko, Seungwoo Choi, Subin Yang, Joonwon Lee, and Uichin Lee. 2015. FamLync: Facilitating Participatory Parental Mediation of Adolescents’ Smartphone Use. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 867–878. <https://doi.org/10.1145/2750858.2804283>
- [35] Martin J. Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home. In *Proceedings of the Halfway to the Future Symposium 2019*. ACM, Article 5, 8 pages. <https://doi.org/10.1145/3363384.3363389>
- [36] Elmarie Kritzinger, Maria Bada, and Jason R.C. Nurse. 2017. A Study into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK. In *Information Security Education for a Global Digital Society*. Springer, 110–120.
- [37] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. ‘No Telling Passcodes Out Because They’re Private’: Understanding Children’s Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, Article 64 (2017), 21 pages. <https://doi.org/10.1145/3134699>
- [38] Christopher Lentzsch, Sheel Jayesh Shah, Benjamin Andow, Martin Degeling, Anupam Das, and William Enck. 2021. Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem. In *Proceedings of the 28th ISOC Annual Network and Distributed Systems Symposium*. Internet Society, 18 pages. <https://www.ndss-symposium.org/ndss-paper/hey-alexa-is-this-skill-safe-taking-a-closer-look-at-the-alexa-skill-ecosystem/>
- [39] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 2019. ‘Internet of Things’: How abuse is getting smarter. *Safe - The Domestic Abuse Quarterly* 63 (2019), 22–26.
- [40] Ewa Luger and Abigail Sellen. 2016. “Like Having a Really Bad PA”: The Gulf between User Expectation and Experience of Conversational Agents. In *Proceedings of the 2016 ACM CHI Conference on Human Factors in Computing Systems*. ACM, 5286–5297. <https://doi.org/10.1145/2858036.2858288>
- [41] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. “‘She’ll Just Grab Any Device That’s Closer”: A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 ACM CHI Conference on Human Factors in Computing Systems*. ACM, 5921–5932. <https://doi.org/10.1145/2858036.2858051>
- [42] Kate Muir and Adam Joinson. 2020. An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home. *Frontiers in Psychology* 11 (2020), 424. <https://doi.org/10.3389/fpsyg.2020.00424>
- [43] National Cyber Security Centre, UK. 2019. Smart devices: using them safely in your home. <https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home>
- [44] Peter Nikken and Jos de Haan. 2015. Guiding young children’s internet use at home: Problems that parents experience in their parental mediation and the need for parenting support. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 9, 1 (2015), 1. <https://doi.org/10.5817/CP2015-1-3>
- [45] Poppy Noor. 2019. Ring hackers are reportedly watching and talking to strangers via in-home cameras. News report, The Guardian. <https://www.theguardian.com/technology/2019/dec/13/ring-hackers-reportedly-watching-talking-strangers-in-home-cameras>
- [46] Office for National Statistics. 2021. Population estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2020. Web page. <https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/bulletins/annualmidyearpopulationestimates/latest>
- [47] İşıl Oygür, Daniel A. Epstein, and Yunan Chen. 2020. Raising the Responsible Child: Collaborative Work in the Use of Activity Trackers for Children. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 157 (Oct. 2020), 23 pages. <https://doi.org/10.1145/3415228>
- [48] S. Parkin, E.M. Redmiles, L. Coventry, and M.A. Sasse. 2019. Security When it is Welcome: Exploring Device Purchase as an Opportune Moment for Security Behavior Change. In *Proceedings of the Workshop on Usable Security and Privacy*.

- <https://www.ndss-symposium.org/ndss-paper/auto-draft-19/>
- [49] Kari Paul. 2019. Ring sued by man who claims camera was hacked and used to harass his kids. News report, The Guardian. <https://www.theguardian.com/technology/2019/dec/27/ring-camera-lawsuit-hackers-alabama>
- [50] Kari Paul. 2020. Dozens sue Amazon’s Ring after camera hack leads to threats and racial slurs. News report, The Guardian. <https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats>
- [51] PayPal (Europe) S.à r.l. et Cie, S.C.A. 2021. Send Money, Pay Online or Set Up a Merchant Account - PayPal. Web page. <https://www.paypal.com/uk/home>
- [52] D. Pencheva, J. Hallett, and A. Rashid. 2020. Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy* 18, 2 (2020), 68–74. <https://doi.org/10.1109/MSEC.2020.2969409>
- [53] Karen Renaud, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. 2018. Is the responsabilization of the cyber security risk reasonable and judicious? *Computers & Security* 78 (2018), 198–211. <https://doi.org/10.1016/j.cose.2018.06.006>
- [54] Jennifer A. Rode. 2010. The roles that make the domestic work. In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*. ACM, New York, NY, USA, 381–390. <https://doi.org/10.1145/1718918.1718984>
- [55] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the design of privacy-empowering tools for the connected home. In *Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems*. ACM, Article 137, 14 pages. <https://doi.org/10.1145/3313831.3376264>
- [56] Wonsun Shin. 2015. Parental socialization of children’s Internet use: A qualitative approach. *New Media & Society* 17, 5 (2015), 649–665. <https://doi.org/10.1177/1461444813516833>
- [57] David Smahel, Hana Machackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Ólafsson, Sonia Livingstone, and Uwe Hasebrink. 2020. EU Kids Online 2020: Survey results from 19 countries. <http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf>
- [58] Jitendra Soni. 2020. Avast reportedly sold user web browsing data. News report, TechRadar. <https://www.techradar.com/news/avast-reportedly-sold-user-web-browsing-data>
- [59] Nick Statt. 2018. Amazon sent 1,700 Alexa voice recordings to the wrong user following data request. News report, The Verge. <https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai>
- [60] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schuab. 2021. Child Safety in the Smart Home: Parents’ Perceptions, Needs, and Mitigation Strategies. In *Proceedings of the ACM on Human-Computer Interaction (CSCW2, Vol. 5)*. Association for Computing Machinery, New York, NY, USA, Article 471, 41 pages. <https://doi.org/10.1145/3479858>
- [61] Leonie Maria Tanczer, Ine Steenmans, Miles Elsdén, Jason Blackstock, and Madeline Carr. 2018. Emerging risks in the IoT ecosystem: Who’s afraid of the big bad smart fridge?. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. IEEE, 1–9. <https://doi.org/10.1049/cp.2018.0033>
- [62] techUK and GfK. 2021. *The State of the Connected Home 2021*. Industry Report. techUK. <https://www.techuk.org/resource/the-state-of-the-connected-home-2021-new-report-launch.html>
- [63] Sarah Turner, Jason R.C. Nurse, and Shujun Li. 2021. When Googling It Doesn’t Work: The Challenge of Finding Security Advice for Smart Home Devices. In *Human Aspects of Information Security and Assurance*, Steven Furnell and Nathan Clarke (Eds.). Springer International Publishing, Cham, 115–126.
- [64] UK Government. 2022. Product Security and Telecommunications Infrastructure Bill. <https://bills.parliament.uk/publications/43895/documents/1050>
- [65] 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. <https://doi.org/10.1145/2632048.2632107>
- [66] Lisa Vass. 2020. Android pulls 24 ‘dangerous’ malware-filled apps from Play Store. News report, Naked Security. <https://nakedsecurity.sophos.com/2020/02/06/android-pulls-24-dangerous-malware-filled-apps-from-play-store/>
- [67] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, Article 11, 16 pages. <https://doi.org/10.1145/1837110.1837125>
- [68] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. “We Hold Each Other Accountable”: Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems*. ACM, Article 478, 12 pages. <https://doi.org/10.1145/3313831.3376605>
- [69] M. Williams, J.R.C. Nurse, and S. Creese. 2017. “Privacy is the Boring Bit”: User Perceptions and Behaviour in the Internet-of-Things. In *Proceedings of the 2017 15th Annual Conference on Privacy, Security and Trust*. IEEE, 181–190. <https://doi.org/10.1109/PST.2017.00029>
- [70] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parents Just Don’t Understand: Why Teens Don’t Talk to Parents about Their Online Risk Experiences. In *Proceedings of the 2017 ACM Conference on*

*Computer Supported Cooperative Work and Social Computing*. ACM, 523–540. <https://doi.org/10.1145/2998181.2998236>

- [71] Ying Xu and Mark Warschauer. 2020. What Are You Talking to?: Understanding Children’s Perceptions of Conversational Agents. In *Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems*. ACM, Article 289, 13 pages. <https://doi.org/10.1145/3313831.3376416>
- [72] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, Article 59 (2019), 24 pages. <https://doi.org/10.1145/3359161>
- [73] Jason C. Yip, Kiley Sobel, Xin Gao, Allison Marie Hishikawa, Alexis Lim, Laura Meng, Romaine Flor Ofiana, Justin Park, and Alexis Hiniker. 2019. Laughing is Scary, but Farting is Cute: A Conceptual Model of Children’s Perspectives of Creepy Technologies. In *Proceedings of the 2019 ACM CHI Conference on Human Factors in Computing Systems*. ACM, Article 73, 15 pages. <https://doi.org/10.1145/3290605.3300303>
- [74] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, Article 200 (2018), 20 pages. <https://doi.org/10.1145/3274469>

## A INTERVIEW QUESTIONS

### A.1 Device questions

#### A.1.1 To each primary school aged child (4-11):

- How do you use the device?
- Do your parents have to help you?
- Do you have your own account? If so, does that limit what you can do with it? Do your parents control what you can do (e.g. with an app)?
- Do you do different things with the device to the adults in the house or your siblings?
- Can you tell me how you think the device works?
- What do you like about the device?
- What would you change about the device?
- Do you know how to turn the device on or off, or make changes to how it works? Have you tried to do this?

#### A.1.2 To each 12-16 year old child:

- How do you use the device?
- Do you have a separate account to other house members? Do your parents have to monitor what you do with the account?
- How do you think the device works?
- What information do you think the device has about you?
  - How do you feel about that?
  - Who do you think can access that information?
- Do you think you use it differently to your parents and siblings?
- Have you ever tried to change the settings of the device? If so, can you tell me more about that?
- Do you think the device is useful?
- What would you change about the device?
- Does the device stop you from doing things, physically or virtually?

#### A.1.3 To each adult (+16) household member individually:

- How do you use the device?
- Do you have a separate account to other house members?
- Have you ever tried to change the settings of the device? If so, can you tell me more about that?
- What information do you think the device has about you?
  - How do you feel about that?
  - Who do you think can access that information?
- Do you think the device is useful?
- Do you use the device for the purpose that you bought it?
- What would you change about the device?
- Do you have to use workarounds to use the device in the way you want to?
- Does the device work as well for every member of the household?
- Do you intend on buying or having any more devices installed in your home in the next year?
- If so, which and why?

### A.2 Cyber security knowledge

#### A.2.1 Questions to all children:

- What have you learned at school about computers and the Internet?
  - Can you describe to me what you know about staying safe when using the Internet?
  - Do you talk about what you’ve learned with your family?

*A.2.2 Questions to 12+ children:*

- How much knowledge do you think you have about using the Internet compared to your parents?
  - Have you ever given them help?
- Could you describe to me what you think the biggest risks of using Internet-connected devices in the house are?
  - What changes would you like to make to stop those risks happening?

*A.2.3 Questions to adults:*

- How well do you think you have secured the devices you have in your home?
  - Can you give details?
  - Is there one person in the house that is more likely to manage issues with technology?
    - \* Is this because of necessity or choice?
    - \* Do the other members of the household wish they could do more?
- What do you consider to be the biggest risk that you have with the IoT devices in your home?
  - Is there anything you feel you could do immediately to minimize that risk?
  - What else would you like to see done to minimize that risk? By whom?
- Are you aware of ever having been the victim of a cyber crime or data breach?
- Who manages the cyber security aspects of the devices that you use in the home?
  - Is that an intentional choice?
- Which sources do you use to get cyber security information?
  - Are you aware of educational schemes run by the government or other non-governmental organisations? If so, have you used them, and did they help?
- What would be your ideal method of becoming informed about cyber security issues that might affect you?
- Are you aware of any issues (on the news or otherwise) that have been raised about the security of IoT devices?
  - How does that make you feel?

## B CODE BOOK

Codes/subcodes	Description of subcode heading
<i>Use of devices within the home</i>	
<b>Family relationship with devices</b>	Elements of the family's relationship with home IoT devices
Limitation of use	
Lack of trust	
Negative managing experiences	
Positive/neutral managing experiences	
Controls that people have	
Negative device experiences	
Positive device experiences	
Joint device use	
<b>Adult relationship with devices</b>	Specific instances of how adults use home IoT devices, as described by both adults and children
Adult device use	
<b>Child relationship with devices</b>	Specific instances of how children use home IoT devices, as described by both adults and children
Overly comfortable with devices	
Child device use	
Child ease of use	
Child managing or altering device	
Child circumvents restrictions	
Child is not careful with devices	
Child is careful with devices	
<b>Confusion over device knowledge</b>	Examples of where any interview participant expressed a lack of knowledge about their home IoT devices
Don't understand how device works	
Lack of personal confidence	
Incompatibility	

*Continued on next page*



Codes/subcodes	Description of subcode heading
<p><b>How do devices work</b></p> <p>Data devices have Always listening? Never considered Not sure how secure it is Comfortable about use in home Not comfortable about use in home How much can they do with the data? Download of personal data</p>	<p>Topics that came up when any interview participant explained their understanding of how home IoT devices worked</p>
<p><b>About the devices</b></p> <p>Just like any other white good Why bought?</p>	<p>Explanations of how interview participants viewed the devices and why they bought them</p>
<p><b>Parental relationship with devices</b></p> <p>Devices aren’t different to other technologies Content concerns Destruction of device Kid’s filter is too restrictive Concerns for children Educating yourself to look after children</p>	<p>How parents view home IoT devices with respect to their children’s use</p>
<p><b>Where to get support from</b></p> <p>TV programs Online - specific source YouTube Bank Government No idea</p>	<p>Where participants explained they would get information about security, should they need it</p>

*Continued on next page*

Codes/subcodes	Description of subcode heading
Police	
Family	
Friends	
Online - generic	
<b>Concerns</b>	
Privacy	All concerns listed, by any participant, about digital technology use
Security	
Unintended consequences	
Parental tracking	
Lack of parental control	
Restrictions	
Children believing everything online	
Child/restricted accounts	
<b>Risks</b>	The risks that participants saw in relation to using home IoT devices
Data breach	
Time waste	
Physical damage	
Malfunction	
Inappropriate content	
Viruses	
Lack of accountability for online info	
Identity Theft (real or accidental)	
Unsolicited contact from strangers	
Scams/financial fraud	
"Hacking"	
Doxxing/identifying yourself	
Information theft	
<b>Parent/child discussion</b>	Types of family discussions described by participants
Discussing things learned at school	

*Continued on next page*

Codes/subcodes	Description of subcode heading
Discussion as a means of solving problem Children learn from parents Safeguarding Child telling parent what to do	
<b>Cyber security management in the home</b>	
<b>Knowledge</b>	Instances in which the participant’s level of, or means of acquiring, knowledge were explained
Tech negatively in the news	
Tech in the news	
How to do it	
Not that concerned	
Self-confidence	
Too difficult to think about	
Good level of security in the house	
Unsure of level of security in the house	
What is taught at school	
What school could cover	
<b>Strategies</b>	Examples of specific cyber security strategies
Turning off WiFi	
Password manager	
Awareness of malicious things online	
Smishing	
Old devices	
Biometrics	
2FA	
Data deletion	
Anti-malware	
Password reuse/weak passwords	
Personal data use	
Passwords	

*Continued on next page*

<b>Codes/subcodes</b>	<b>Description of subcode heading</b>
Software updates	