Internet of Things (IoT) Privacy and Security: A User-Focused Study of Aotearoa New Zealand Home Users

Lisa Patterson, Sue Chard, Bryan Ng, Ian Welch
School of Engineering and Computer Science
Te Herenga Waka - Victoria University of Wellington
{lisa.patterson, sue.chard, bryan.ng, ian.welch}@ecs.vuw.ac.nz

Abstract

This study focuses on behavior of everyday Aotearoa New Zealand (Aotearoa) home users of Internet of Things (IoT) consumer devices. It considers Protection Motivation Theory (PMT) as an approach to modification of user behavior to improve safety in terms of privacy and security. Our aim is to better understand safety for everyday users of IoT consumer devices in the home. We want to understand human barriers to safety in Aotearoa users' perceptions and behaviors, and learn what everyday users perceive and understand about IoT privacy and security at home. This study aims to investigate IoT user behavior alignment with PMT. The main contributions of this paper explore Aotearoa users' perceptions and behaviors towards IoT devices in the home through the theoretical lens of PMT, and determine which of the four factors of PMT contribute to user behavior.

1. Introduction

IoT is expanding at a rapid rate and is becoming ubiquitous in our society, and increasingly our homes. Existing privacy and security protections are not keeping pace with changes, and many dangers are posed to users. User-focused IoT privacy and security for everyday Aotearoa users in the home is under explored in the literature.

It is important to state technical definitions for the terms privacy and security, in respect of this paper. Data privacy can be described as "the aspect of information technology that deals with the ability of an organization or individual to determine what data in a computer system can (or cannot) be shared with third parties" [1], or "the controlled release of information" [2]. In the context of cyber security, security is concerned with protecting information integrity, confidentiality and accesssibility [3] [4].

The concepts of privacy and security are joined; without some degree of privacy (an ability to control the release of personal data) people have concerns about security (confidentiality, integrity and availability). Issues concerning privacy and security relating to information that is stored, processed and transmitted by traditional computers have caused problems for many years [2].

Current privacy and security protections are not keeping pace with the many dangers that users face. User behavior is also shaped by the policy and legislative environment, therefore this is another facet that must be considered in relation to IoT privacy and security. IoT technology has evolved rapidly, leading to a rapid innovation cycle. There is a rush to get devices to market quickly, leading to severe deficiencies in security. It is a very heterogeneous market, and design solutions are diverse. There are competing or lacking regulations, standards, protocols and frameworks for manufacturers to adhere to, leading to poorly tested devices with complex communication being released to market [5] [6] [7]. Everyday Aotearoa users are ill-prepared to manage and mitigate the risks that arise. The rush to market with new devices results in a lack of standards and protocols, and the legislative environment is lagging in response to the new challenges that arise from IoT.

In this study, privacy and security issues related to user behavior with IoT consumer devices are explored. A qualitative study was conducted which used PMT as a theoretical lens through which to examine behavioral aspects. This research is concerned with establishing current IoT privacy and security problems, and understanding why these issues exist. This work provides new insight to the field, and aims to add to understanding to increase the level of privacy and security for the everyday Aotearoa user of IoT in the home.

2. Related Work

Investigation into human behavioral aspects of IoT data privacy and security in the home is under

URI: https://hdl.handle.net/10125/71152
978-0-9981331-4-0

investigated in Aotearoa. We could find no Aotearoa based academic research publications with a user focus on IoT privacy and security for everyday Aotearoa users in the home. An industry report from Unisys (September 2019) surveyed one thousand customers across Aotearoa and found that approximately one quarter had experienced the virtual assistant on a smart device (speaker, watch or phone) listening in when it had not been actively turned on. Interestingly, only half of these customers (half of the quarter affected), considered that occurrence to be a cause for concern [8].

In 2018 Dupuis and Ebenezer conducted research focusing on USA users, using PMT as a theoretical framework to see whether users cared about privacy violation by IoT devices. The first part of their research centered around examining customer reviews of home IoT devices. Fifty reviews were selected for each of ten top rated IoT devices sold via the online retailer Amazon.com. The researchers examined the extent to which privacy issues came up in customer reviews. Secondly, they conducted eighteen interviews with university students to study their comprehension of, and concern with, privacy relating to IoT devices. The last part of their study was a survey examining the constructs of PMT in relation to these devices. Dupuis and Ebenezer were particularly interested in how participants evaluated IoT smart home devices from the perspective of privacy, if at all, when they were making purchase decisions. They were also interested in the importance of the privacy issue based on the customer reviews chosen. The study concluded that users do care about having their privacy violated by an IoT device, and the associated risks. The study also found that users are more willing to act to protect themselves if they believe they can understand ways of doing so, but only if they do not consider the costs to be too high. Interview participants in this study were supplied with a report detailing security concerns and vulnerabilities directly before their interview, to establish a baseline knowledge [9].

A 2016 Aotearoa study Compromising Privacy for Convenience and Wellbeing on the Internet of Things (IoT) investigated the extent to which potential IoT users in Aotearoa were prepared to compromise their privacy for the sake of convenience and wellbeing, and specifically the use and attitudes of Aotearoa residents toward emerging IoT, particularly relating to the collection, storage and use of Personally Identifiable Information (PII) by organizations. Scenarios were constructed in Second Life and shown to a group of 15 researchers and industry participants, and a questionnaire was rolled out to a selection of Aotearoa residents, resulting in 1200 usable responses. Results from this study showed a high level of concern surrounding the collection, storage and use of personal data relating to IoT devices [10].

3. Data Collection

Figure 1 depicts the steps that were followed in our interview process for data collection.

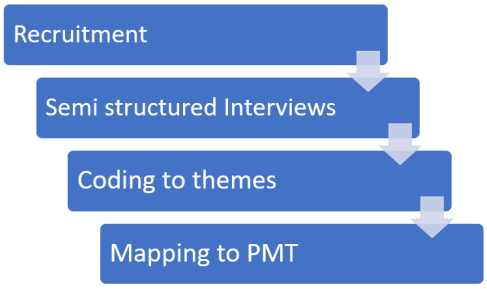

Figure 1. Interview process steps

3.1. Methodology

We chose a qualitative research method to fully explore the topics included in this study, as the technique of qualitative research is particularly well suited to small scale studies [11]. This approach is suited to the nascent stage of phenomena investigation [12]. This research was a small-scale study, conducting semi-structured interviews with the intended result of gaining insights into the level of risk involved with IoT use for everyday (non-expert) Aotearoa users.

3.2. Research Design/Participant Recruitment

A convenience sample was chosen, with voluntary participation. In an effort to avoid any bias, individuals were recruited from different demographics. Five participants were recruited via personal contacts, from a suburban area in the Greater Wellington region of Aotearoa. A range of participants took part, with a spread in age from teenagers to older adults, and a mix of genders, occupations and life experiences all represented in this study. This study looked at adult users' behavior, so one eligibility criterion for participants was that they were aged eighteen or over. The target audience was everyday users, therefore participant selection precluded those could reasonably be perceived as having either an expert level of knowledge, or conversely those who would not purchase internet technology themselves. No vulnerable members of society were invited to participate.

Participants were invited to take part, and were

advised that they were under no obligation to do so. It was made clear that their responses were confidential to the research team, that their information would be securely stored and destroyed within a stated time period, and that no PII would be attributed to them. It was indicated to them that they were welcome to leave the interview at any time, and would still receive a koha (compensation) for taking part.

3.3. Interview Structure

We constructed an interview question guide in the form of questions, with deeper probing questions to be used as appropriate to encourage responses. Questions were designed in the form of opening (general) questions, specific (key) questions and broader (closing) questions all included in the interview guide. In a semi-structured interview approach, a conversational style was used in the delivery of questions, with some new questions arising organically as the interviews progressed.

The interview question guide was organized into sections that each covered a certain theme or topic. Questions were framed around PMT. Rogers first formulated PMT in 1975. The variables determining protection motivation were stated as severity (of an event), vulnerability (probability of the event occurring if no protective behavior was performed), and response efficacy (efficacy of the recommended behavior). PMT was updated in 1983 by Maddux and Rogers, and presented as a more general theory of persuasive communication. Personality and past experience (stimulus variables) believed to influence an individual's cognitive process were identified. The theory was also updated with new constructs including rewards associated with the threat, response costs and self-efficacy [13], [14], [15]. PMT posits that when faced with a threatening event, people carry out two processes of appraisal. One is focused on the threat itself (the threat appraisal), and the other focus is on their ability to counter the threat (the coping appraisal). When people are conducting the threat appraisal, they will consider how negative any consequences of the threat might be (the perceived severity) and consider what is the likelihood of the threat occurring in a way directly affecting them (the perceived vulnerability). When conducting their coping appraisal, people will consider whether following a recommended course of action will result in the removal of the threat (response efficacy), and consider how confident they would be to carry that action out (self-efficacy) [14], [16], [17]. PMT is a well-established theory, which was originally developed to provide an explanation of how to influence risky behavior, and to determine what components a persuasive message should include. PMT builds on the theory of fear appeals. At its core is the idea that an individual's behavior is influenced by their threat appraisal (the severity and likelihood of an unwanted consequence), and their coping appraisal (the efficiency, manageability, and cost of the risk reducing behavior) [14]. Simply put, the PMT posits that the behavior individuals form is the result of a cost benefit analysis, where associated behavioral risks are compared to the cost of trying to reduce (or eliminate) the risks [15]. Each question was mapped to a specific objective to elicit appropriate data.

Participants were initially asked questions regarding general technology and internet usage habits. The next section focused on awareness of privacy and security using two internet connected toys as interview aids. These toys were consumer devices, readily available and marketed as fun, modern, internet connected devices that would appeal to children. One was marketed to children aged 3+, and provided real-time audio communication plus access to web based resources, in an appealing soft-toy exterior. The other was marketed as ages 8+, and provided mobile, real-time photo and video communication, inside a fun automotive vehicle. Our intention was to use these toys as a discussion prompt, to draw out users' understanding of the privacy and security risks that exist with internet connected devices readily available to the everyday consumer, and marketed towards children. Participants were asked about their perception of the safety of these toys, whether they would research security aspects if they were (hypothetically) going to purchase the toy for a child or family member, and where they might search for security advice. Participants were then asked about security risks including their perception of the severity of a threatening event, and their perception on the probability of the occurrence, or vulnerability.

Participants were asked about potential mitigations, the efficacy of recommended preventative behaviors, and their own self-efficacy. Effects of changed ownership were discussed, and a general reflective question concluded the interview. No actual testing of privacy or security has taken place on these devices at this point. Ethical Approval for this study was gained from the Human Ethics Committee at Victoria University of Wellington, approval number 0000027885.

3.4. Coding and Themes

The process of coding involves organizing the data by analyzing text then writing a word that represents a

theme in the margin [18]. Audio recordings taken during the data collection were reviewed and coded into themes [19]. These themes were: Awareness of Risks; Trust; and Level of Concern relating to Risks. Reviewing the findings, it became apparent participants gave multiple, varied responses which could be further interpreted into multiple categories. The three themes and 15 categories are discussed below.

3.4.1. Awareness of Risks An individual's awareness of risks has an effect on what private information they disclose [20]. When interviewed for this piece of research, participants showed varying degrees of awareness of risks. To allow for sufficient richness in data from interview responses, the participants were not prompted with any literature prior to the interviews. Nor were they questioned about their understanding of the terms risk, privacy, or security. Participant risk awareness responses were coded into three categories of risk including users who were unaware of risks, users who were aware of only some of the potential risks, and users with a general lack of IoT knowledge (and therefore a lack of knowledge about the inherent risks).

Users were Unaware of Risks Some users indicated that they were unaware of the risks present when using IoT devices in the home. This applied to both the extent and the types of potential risks. Some risks had not even occurred to the participants before the interview. One participant did not recognize the inherent danger present in the privacy and security of these types of devices.

The following data points from two participants highlights a lack of awareness. When asked about hesitation giving the toy to child or family member, P2 responded "I feel like I'm saying yes because of the interview but if I just saw it on an ad or the shelf it wouldn't seem dodgy, but because I'm thinking about it more it seems like it would have potential. I probably wouldn't think about the danger". When probed about where recorded or streamed footage would be stored, P1 stated "The child sees the picture on the tablet", and confirmed they would have no hesitation in giving the toy to a child, calling it "a cool thing to give to a child".

Users were Aware of only a Limited Aspect of Risk In addition to the users who were not aware of any risk to using IoT devices in the home, some users identified only certain aspects of potential risks, and were not aware of the full extent of those risks. These participants showed an awareness that some degree of risk was present, but either underestimated this risk or did not fully comprehend the full dangers that the risks may present to a user. "If (the toy) was being used by a child with another child it could be a risk because you don't know who could be at the other house. It could be totally abused. At both ends". In making this observation, P5 identified risks stemming from user misuse, but did not mention other risks that could be present, such as the device being hacked into, or a database being compromised. P1 identified risks in one area only, therefore their concern centered around the child causing mischief rather than risk posed to the child as a victim of malicious activity from outside sources observing "It looks like it's aimed at children and they could get up to all sorts of mischief".

Users Lack Technical, or IoT-Specific Risk Knowledge, Contributing to level of Risk Awareness In 2002, Donald Rumsfeld, former United States Secretary of Defense stated "as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know" [21]. In this sub category of the research, users did not know the unknowns, with responses indicating that users had a lack of technical, and IoT-specific knowledge.

Even though all users interviewed were users of technology, there was a lack of awareness or confidence in their knowledge of how the technology actually operated. Users were not shy to admit their lack of technical expertise, appearing unconcerned about their lack of technical and IoT-specific knowledge. It is important to recognize that risks may be posed by this lack of knowledge, and the apparent indifference to it. Over half the participants exhibited a lack of knowledge in the technical area.

Examples supporting this claim include P2 stating "I don't know how the smart speaker works, I think it just connects itself to the internet, I don't really know". P5 said they would have to believe what they were told as they do not have the technical expertise to know differently, so they would "Have to take their word for it". P1 stated "No, I wouldn't have a clue". As well as a generalized lack of technical knowledge, one participant showed a clear lack of understanding of IoT-specific technology, with P2 stating "I didn't even know what Internet of Things was until today". This was somewhat surprising, given that this participant was a prolific user of general technology, and used multiple IoT devices within their home environment.

From this observation it could be deduced that IoT devices designed for home use are easy enough to set up

and use, without the user possessing a full understanding of either device operation or security.

3.4.2. Trust When observed from the angle of human factor, trust can be viewed as two main categories. Firstly, inherent characteristics (part of the individual), and secondly situational characteristics (outside of the individual). Trust as a human factor in relation to risk assessment in cyber security also relies on understanding how different mental models and risk postures impact both the level of trust given to individuals and the biases that affect the ability to give that trust [22].

Trust-related responses from interview participants were coded into multiple categories. The categories of trust included users who believed that 'someone else' would manage the risk for them, users who had an inherent trust in human nature, users who believed that technology would protect their privacy and security, and users who were willing to believe what they were told by other sources.

Users Believed Someone Else was Managing the Risk for them Threat risk can be categorized into four risk response strategies which include Avoidance, Transference, Mitigation and Acceptance [23].

In their interviews, it appeared as though some users were unconsciously applying this model, with some users believing that other people would assume the responsibility of managing privacy and security on their behalf. One participant expected the companies they were dealing with to manage the security of their data, as part of the usual business process. Two of the participants believed that their network security was being attended to by their Internet Service Provider (ISP). These participants were comfortable in their belief that their security was adequately attended to by other parties. The following responses illustrate these claims.

P3 relinquished the responsibility for dealing with privacy and security issues to their ISP and other companies they are dealing with, stating "I expect the companies who I trust with my data to protect it", and "Like Spark or Vodafone... they control the security". In a similar statement, P1 said "I think (security) is just set up by the Vodafone guy".

Users had an inherent Trust in Human Nature Some users showed trust in human nature, trusting that other people would not act in a manner detrimental to them. This trust in human nature poses a risk, as unfortunately not all people may be worthy of this trust. This lack of trustworthiness does not only apply to strangers. The high trust in human nature was summed up by P3, who recognized that they could definitely see privacy and security risks when selling or giving away a pre-owned IoT device, observing "Your account info is still in there. You'd have to trust the people". However, the same participant said that they would reset a device when selling or giving it away to a stranger, but would not be so concerned if it was going to someone they knew. As the recipient of a pre-owned device, P3 would also be trusting of someone they knew, saying they "Wouldn't think about (risks)... I would trust someone I knew, and would expect them to have reset (the device)". This indicated that whilst P3 was aware of at least some potential risks posed, they would choose to trust people they knew, assuming them to be trustworthy.

Users Believed that Technology would Protect their Privacy and Security Also fitting in the area of trust were the participants who trusted that technology would assist in the preservation of their privacy and security. Responses from two participants showed their belief that in-built technology features would be adequate to act in defense of any risks posed. Both participants appeared to believe that technology features would eliminate the risk to them. When asked about operating a pre-owned device, P3 commented "There's usually a reset feature". Similarly, P2 stated "If you could factory reset it, it would be just like new".

Users were Willing to Believe what they were Told by Other Sources Some users displayed a willingness to believe what they were told by others. The following responses from two participants demonstrated a willingness to believe what they were told regarding privacy and security, even if the participants were at least partially aware that some level of risk was present.

When participants were asked whether they would believe that a device was safe to use if they had been led to believe that it was, P1 responded "Yes, I would feel at ease if we set our own rules around use", and "I would talk to the salesperson about it and ask whatever questions I wanted to know". This showed that P1 trusted the information given to them by sales staff. Similarly, P5 admitted that they would "Have to take their word for it" as they "don't have the technical know-how to know differently". This statement indicated that P5 was willing to believe information from someone they perceived as having greater knowledge than themselves.

3.4.3. Level of Concern relating to Risks A widely accepted definition for risk is Risk = Likelihood* Impact [24]

The level that users are concerned with risk has an impact on their behavior. The use of security technologies is invalidated where users do not follow cyber security protocols, or engage in activities that place themselves at risk [25]. Human factors are gaining increased attention, in particular where using security technologies has failed to prevent cyber attack [25] [26].

Participant responses relating to concern about risk were coded into various categories. Some of these categories included users who were aware of risks but were unconcerned, users who were aware of risk but chose to ignore it, and users who were aware of risk, but believed 'it won't happen to me'. Other categories included users who believed that risk was reduced because their data were not particularly interesting, and users who prioritized various other things over risk. These priorities included users who prioritized time over risk, users who prioritized effort over risk, users who prioritized price over risk, and users who did not prioritize ongoing security.

Aspects of this study also highlighted various risks associated with different phases of the IoT life cycle, from purchase of the device, to using the device, the time when the device becomes unsupported, and decommissioning (and potential rehoming) of the device.

Users were Aware of Risks, but were Unconcerned This category included participants who were aware of risks, but chose not to be concerned about them. Responses from two participants highlighted this awareness or risk, and lack of concern about it.

P1 indicated they would set up the toy, "Figuring out how to do it without the instructions if possible, then I'd never look at anything again". P1 acknowledged they would not be concerned about security of operating a pre-owned device, saying "Maybe I might clean it (just) to have it nice and fresh to start using it, but not to make sure I was being safe. Even if I bought it off someone I didn't know", and "I know from CSI and stuff that they do have that big disky thing you can't clear completely but I'm not worried". P2 said "If got a new device in my home I would do nothing, just interested in getting it up and running". P1 admitted "I don't even know what I'd do for privacy and security. Probably because I don't worry about it that - I've never really thought that far". P2 stated "I'm not that interested in it... doesn't concern me". P1 said if they had to download an app, they'd just "Click yes, yes, yes without reading the privacy statement or anything". P1 just assumed that their partner was dealing with network security, but did not bother asking "It's not really even a conversation we had".

Users were Aware, but Knowingly Chose to Ignore the Risk Some users were aware of risks, but chose to ignore them. Some participants elected to take an 'ignorance is bliss' approach, and one chose to not think about it so they would not get worried about the consequences of risks. The following responses from two participants highlighted their awareness of risk and choice to ignore it.

P1 said "I don't feel it could be that much of a threat. I'm not sure whether it's just ignorance is bliss and I'm happy to bury my head in the sand, or if it's like I don't really want to put any energy into something that might not happen", and explained "I do like having that whole outlook the less I know the better, because I don't really want to freak myself out over what could happen". P4 said "Maybe ignorance is bliss, I hadn't given it much thought".

Users believed the Risk 'Won't Happen to Me' Some participants were aware that risks were present, but chose to take the view that an undesirable occurrence would not happen to them. This could be a way of dealing with their own fear, or feelings of helplessness about how to address this risk. The following examples from two participants showed awareness of risks, but a belief that the risk would not happen to them.

In the first example, even though P2 recounted hearing about an actual data security breach only two days earlier, and discussed the breach in the interview, they described the likelihood of a threat occurring as 'very low'. P2 observed "I honestly wouldn't even think about it". P1 said "I don't feel it could be that much of a threat", "I feel it's unlikely". P2 shrugged and said "It doesn't concern me cause it's just something you hear stories about. Apart from (breach victim) I don't know anyone it's happened to, and it hasn't happened to me. So…".

Users Believed their Data were not of Particular Interest, and that this Reduced Risk Three participants displayed a self-deprecating attitude, that their personal data would not be particularly interesting to anybody else. Because they perceived that their data were not interesting, they seemed to believe that this lowered the risk of a security breach occurring, and that they did not have much to lose if their security was breached. The following responses are examples of their perceptions that their personal data were not particularly interesting, so risk was therefore reduced.

P3 felt they currently have "No data of interest" but that sometime in the future they will increase their level of data privacy and security because "I might have more to lose when my data is more valuable". Two participants found the potential risk scenario amusing. P2 laughed as they commented "They'd have a fun time if someone was listening, I don't know why they'd bother... So no, I don't think about it". P1 also laughed as they explained "I also feel that if (a breach) happened it's not the end of the world... good luck looking at my photos or if you took my money, there's not much there to take".

Users Prioritized Time over Risk At times, desire to complete a task quickly can take priority over being careful, which may lead to a security risk. For example, computer users may automatically click 'OK' to boxes that appear, even when they know that they should not [27]. Many things were given a higher level of priority by participants than addressing risk. Responses from three participants highlighted the presence of time pressure, and served to illustrate the point that saving time was afforded a higher priority to them than concern around risk. P1 said they "would go for the shortest time frame". P5 made the observation that "Time is precious". Interestingly, P3 actively lowered security in order to save time, reporting that on one occasion they removed the requirement to enter a password because "Doing it the Mac way saves time". Therefore, even though P3 reported that password protecting a device would 'definitely' improve security, they actively chose to remove this from their laptop.

Users Prioritized Effort over Risk Another thing that participants chose as a higher priority than managing risk was reducing effort. Responses from three participants illustrated how the desire to conserve energy was higher than the desire to mitigate risk. As participants did not want bother putting effort into reducing risk, it obviously was not something of major concern to them. One participant was aware of risk but chose to ignore it as they did not want to bother exerting effort to mitigate the potential threat unless it became an actual threat. When asked whether they realistically would take any action to make usage of devices safer, P3 replied "Probably not... The more passwords, the less user friendly. And it takes longer to start and do what you want". P1 said "I don't want to put any energy into something that might not happen". In response to the question of whether they would research security, P1 observed "I think it would be really effective, especially if you did more than one. But I wouldn't bother." Participant P3 had their passwords saved in the browser, which they identified as a potential security risk. However, rather that taking action now, they chose to wait and hope for the best stating that if their laptop was stolen, they would "Just cancel their credit card".

Users Prioritized Price over Risk Sometimes the price of devices can lead participants to make risky decisions. The well known paper "The Market for Lemons: Quality Uncertainty and the Market Mechanism" investigates how the quality of goods traded in a market may degrade in the presence of information asymmetry between buyers and sellers, which leads to only "lemons" being left behind [28]. The choice of price over quality, and therefore potential bad decision making was displayed by some participants where the cost of buying a device took priority over risk. Two participants admitted that they would be unlikely to research security for a cheap item. Participants indicated that price was a motivator as to how much they would research online reviews. This indicates that the participants place a higher priority on saving money than managing risk. P2 said "It depends how much it is. If it's a big purchase I would research more, if it's cheap I don't really care", "nope I wouldn't consider it. I'd just say yay, cheap". P1 said "If it was an expensive toy I would".

Users Did Not Prioritize Ongoing Security Some participants indicated that maintenance of security was not a high priority to them. At times, participants showed a lack of interest in keeping security up to date. Responses from two participants illustrated the low importance of ongoing security to them. P1 said "I'd figure out how to do it without the instructions if possible, then I'd never look at anything again. Unless I needed to troubleshoot or someone pointed out something cool it could do… I would set up and forget". P5 acknowledged they should probably change their Wi-Fi password saying "Heaps of people know my password… friends and ex partners of the kids over the years".

3.5. There was a Relationship Between General Privacy and Security, and Data Privacy and Security

From the interviews conducted, there appeared to be relationship between an individual's general security behavior, and their data privacy and security behavior.

Comments offered by all five participants indicated that there was a relationship between their general physical security practices, and their cyber security practices. Three participants were unconcerned with

general security, and also took a casual approach to their online privacy and security. As an example, P3 considered themself to be at the "lower end" with physical security of doors and windows at home, and "leaves the door unlocked". The reason given was that they didn't "have anything valuable". They currently were unconcerned, but felt they would increase their level of data privacy and security sometime in the future when their data were more valuable.

Two participants found their attitude toward general and cyber security amusing. P1 laughingly explained "I'm really bad, I can leave the house unlocked and I'm not too worried about it. I always feel safe", saying "You know how they say are you sure or they give you the messages? 'do you accept', well I just ignore them and keep going next, next, what's next". P2 said "I'm not (security conscious), I just don't really think about it". In contrast, two participants were conscientious toward both their physical and their cyber security. P4 considered themself to be 'fairly security conscious', and P5 described themself as 'quite security conscious'. These two participants were the only ones interviewed who said that they would realistically try to make usage of devices more secure. P4 had already password protected their smart television, and P5 said "I would password protect (the device), if I could". One of these security conscious participants attributed their security attitudes to growing up overseas, in a country they perceived as less safe than Aotearoa.

3.6. Analysis of Themes using PMT

PMT posits that people protect themselves based on four factors including perceived severity, perceived vulnerability, efficacy of a recommended preventative behavior, and perceived self-efficacy. PMT proved to be a useful theoretical lens through which to examine this topic. When related back to PMT, the themed codes relate to each of these four factors as shown below:

3.6.1. Perceived Severity of a Threatening Event Perceived severity refers to the extent of severity or consequence of risk. For example parents will more likely engage in mediation behavior of their child's smartphone use where they perceive that the consequences of addiction are severe (a high perceived severity) [29].

In our study, we found that lack of risk awareness among participants led to a low perceived severity of a threatening event. Responses confirmed that users' perception of severity was linked to their awareness of risk as illustrated below. Several themes concerning awareness relate to perceived severity of a threatening event. The themes identified include users were unaware of risks, users were only partially aware of risk, and users had a general lack of technical knowledge. Most of the participants did not understand the severity of risks involved with using IoT devices in the home. This lack of awareness highlights a need for education on potential risks.

3.6.2. Perceived Probability of Occurrence or Vulnerability It has been reported that perceived vulnerability to privacy risks positively affects information privacy concern [30]. In our research, interview participants showed mainly low levels of concern about risk, which may be based on perceived probability of occurrence or vulnerability. Many users were aware of risk (to some degree) but were unconcerned for a variety of reasons. Themes relating to a lack of concern around risk related to a user's perceived probability of the occurrence of a threat. For the small scale interview participants these included the following themes, demonstrating low levels of concern based on low probability of occurrence or vulnerability. Some users were aware of risk, but were unconcerned. Other users were aware of risks but choose to ignore them, some users were aware of risk but believed it 'won't happen to me'. Some users perceived a reduced risk because their personal data were not particularly interesting. Other themes corresponding to perceived probability of occurrence included users prioritizing time, effort, and price over addressing risk, and users not placing a high priority on ongoing security. These findings confirmed both the need for education on addressing risk, and a need for behavioral modification.

3.6.3. Efficacy of the Recommended Preventative Behavior Response efficacy refers to a user's evaluation of the perceived effectiveness in performing a behavior in order to prevent a threat. For example, parents monitoring their child's smartphone use would more likely engage in mediation behaviors where they perceive their mediation behaviors would be effective in preventing addiction (have a high level of response efficacy) [29].

In our research, users placed trust in the efficacy of recommended preventative behaviors when managing risk. Many users were willing to trust in the advice supplied to them, or actions taken, by trusted others. The following themes concerning trust relate to the efficacy of the recommended preventative behavior. Users believed someone else was managing the risk for

them, users had an inherent trust in human nature, users believed that technology would assist in the protection of their privacy and security, and users were willing to believe what they were told by other sources. Users trusted in the information or services supplied to them by people they considered trustworthy, or perceived as more knowledgeable than themselves. However, no proof of efficacy was sought by participants. This demonstrates the need for support from reputable sources.

3.6.4. Perceived Self-Efficacy How an individual judges their own ability to complete a computing task influences their decisions around how they will use computers [31]. Computer Self Efficacy has demonstrated significant positive contribution to cybersecurity computing skills, whilst not showing significant contribution to misuse intentions [32].

In this research, all interview participants lacked confidence in their own technical ability, leading to low perceived self-efficacy. One theme demonstrated this, that the users were aware of risks but were technically inept to address that risk. This low level of self-efficacy showed a need for education and training, with different types of resources required to assist users in managing risk. This low level of confidence may have been a limitation of this piece of work, although this was not apparent, or specifically asked during the recruitment process.

4. Discussion

This study aimed to investigate whether the behavior of users of IoT in the home aligned with PMT. It investigated which of the four factors of PMT contribute to user behavior. Interview results showed that the coded themes all related back to factors in PMT.

We questioned what behavioral aspects affect the privacy and security of everyday Aotearoa users of IoT in the home. We sought to address the question of what were human barriers to safety in users' perceptions and behaviors. We pondered why everyday users may act in an unsafe manner regarding IoT safety in the home, and asked what everyday users perceive and understand about IoT safety in the home, querying why they behave in the ways that they do. Initial information was sourced from literature, then deductions were drawn from the semi-structured interviews that were conducted as part of the small-scale survey.

Results showed that human barriers to IoT safety included users being either unaware of risk, or aware of only limited aspects of risk. Where risk was identified, users often had low levels of self-efficacy, and were therefore ill equipped to address that risk. Users were willing to trust the information of others, including some who were potentially unqualified to deliver recommendations, including sales-people or online reviews by members of the public.

Regarding the perception and understanding of IoT safety by users, where they have some awareness of risk, many users found justifications for not addressing the risk. Users prioritized time, effort and money over addressing risk. Users chose to place trust in others they knew, and others they perceived as more knowledgeable than themselves. Users also believed that technology would aid in managing their security risks. Users were often unconcerned about risk, or chose to believe that occurrences or vulnerabilities would not happen to them.

There was a belief among users that other people possessed superior knowledge regarding IoT privacy and security. Trusted sources included potentially unqualified sources such as sales people or authors of online reviews. There was a relationship shown between users general privacy and security habits and their cyber security habits. Many users acted with a small town mentality regarding cyber security, even though connection to the internet meant that they were now part of a global community.

Limitations of this research include the low number of participants, as it was a preliminary study. In this study, participants were not questioned about their mental models of how the technology worked, or their understanding of effective security practices. This study highlights areas of concern including knowledge of who to trust; lack of risk awareness; low levels of perceived self-efficacy; and the scale of internet exposure for Aotearoa users of IoT in the home.

5. Future Work

Future work will include a consideration of whether behavioral economics techniques such nudges and commitment devices may be appropriate methods to alter user behavior. We will also look to other fields to identify what behavioral mitigations have been attempted in those areas, and gauge the efficacy of these. We will draw on research utilising PMT in general security, and cyber security.

Some potential behavioral mitigation strategies were discussed with participants during their interviews. Various differing strategies should be tested to determine the most effective techniques for increasing knowledge of trustworthy sources for users; raising awareness of IoT risk to everyday users; work to

increase users' confidence in their self-efficacy to address risks; and promote understanding of the global scale of internet privacy and security issues.

References

[1] M. Rouse, "Data privacy (information privacy)," 2013.

[2] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau, and M. E. Lesk, "Privacy and cybersecurity: The next 100 years," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1659–1673, 2012.

[3] P. Pype, G. Daalderop, E. Schulz-Kamm, E. Walters, and M. von Grafenstein, "Privacy and security in autonomous vehicles," in *Automated Driving*, pp. 17–27, Springer, 2017.

[4] H. S. M. Lim and A. Taeihagh, "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications," *Energies*, vol. 11, no. 5, p. 1062, 2018.

[5] S. Marksteiner, V. J. E. Jimenez, H. Valiant, and H. Zeiner, "An overview of wireless IoT protocol security in the smart home domain," in *Proceedings of the 2017 Internet of Things Business Models, Users, and Networks*, pp. 1–8, IEEE, 2017.

[6] M. Miettinen and A.-R. Sadeghi, "Internet of things or threats?: On building trust in IoT (keynote)," in *Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis*, p. 1, IEEE Press, 2018.

[7] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[8] "The downside of IoT: Kiwis uncomfortable with smart devices listening in." accessed 2019-10-28.

[9] M. Dupuis and M. Ebenezer, "Help wanted: Consumer privacy behavior and smart home internet of things (iot) devices," in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, pp. 117–122, 2018.

[10] X. Garry, Harwood, "Compromising privacy for convenience and wellbeing on the internet of things (iot)." accessed 2020-06-07.

[11] J. A. Hughes, *Sociological analysis: methods of discovery*. London; Don Mills, Ont.: Nelson, 1976.

[12] A. C. Edmondson and S. E. McManus, "Methodological fit in management field research," *Academy of management review*, vol. 32, no. 4, pp. 1246–1264, 2007.

[13] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology*, vol. 91, pp. 93–114, Sept. 1975.

[14] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology*, vol. 19, pp. 469–479, Sept. 1983.

[15] T. Sommestad, H. Karlzén, and J. Hallberg, "A meta-analysis of studies on protection motivation theory and information security behaviour," *International Journal of Information Security and Privacy (IJISP)*, vol. 9, no. 1, pp. 26–46, 2015.

[16] M. Conner and P. Norman, eds., *Predicting health behaviour: research and practice with social cognition models*. Maidenhead: Open Univ. Press, 2. ed., repr ed., 2007. OCLC: 253898882.

[17] A. Bandura, "Self-efficacy: the exercise of control," 1997. accessed 2019-09-23.

[18] G. B. Rossman and S. F. Rallis, *Learning in the Field: An Introduction to Qualitative Research*. SAGE, July 2011. Google-Books-ID: EZTwZLWYAtcC.

[19] J. W. Creswell, *A concise introduction to mixed methods research*. SAGE publications, 2014.

[20] B. Mvungi and M. Iwaihara, "Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features," *Computers in Human Behavior*, vol. 44, pp. 20–34, 2015.

[21] D. Rumsfeld, *Known and unknown: a memoir*. Penguin, 2011.

[22] D. Henshel, M. Cains, B. Hoffman, and T. Kelley, "Trust as a human factor in holistic cyber security risk assessment," *Procedia Manufacturing*, vol. 3, pp. 1117–1124, 2015.

[23] C. L. Pritchard, P.-R. PMP, *et al.*, *Risk management: concepts and guidance*. CRC Press, 2014.

[24] J. Williams, "Owasp risk rating methodology." accessed 2020-06-07.

[25] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, 2009.

[26] L. Hadlington, "Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, p. e00346, 2017.

[27] R. Anderson, "Security engineering: A guide to building dependable distributed systems. 2001: Jonh wiley & sons," *Inc., New York*.

[28] G. A. Akerlof, "The market for "lemons": Quality uncertainty and the market mechanism," in *Uncertainty in economics*, pp. 235–251, Elsevier, 1978.

[29] Y. Hwang, I. Choi, J.-Y. Yum, and S.-H. Jeong, "Parental mediation regarding children's smartphone use: Role of protection motivation and parenting style," *Cyberpsychology, Behavior, and Social Networking*, vol. 20, no. 6, pp. 362–368, 2017.

[30] N. S. Al-Saqer and M. E. Seliaman, "The impact of privacy concerns and perceived vulnerability to risks on users privacy protection behaviors on sns: A structural equation model," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 5, pp. 142–147, 2016.

[31] G. Piccoli, R. Ahmad, and B. Ives, "Web-based virtual learning environments: A research framework and a preliminary assessment of effectiveness in basic it skills training," *MIS quarterly*, pp. 401–426, 2001.

[32] M. Choi, Y. Levy, and A. Hovav, "The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse," in *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP)*, 2013.