Domestic Internet of Things: Aotearoa New Zealanders' Privacy Concerns and Behaviours

Erika Pearson
Esther Jaspers

Funded by a Privacy Good Grant from the
Office of the Privacy Commissioner

Domestic Internet of Things: Aotearoa New Zealanders' Privacy Behaviours and Concerns

Erika Pearson and Esther Jaspers, Massey Business School, Massey University Wellington

July, 2020

CONTENTS

Executive Summary

This research aims to better understand the specific issues around privacy concerns versus privacy behaviour related to domestic Internet-of-Things (IoT) devices in Aotearoa New Zealand. Domestic IoT refers to any home-based device that is connected to the internet and uses data to perform or automate home tasks. Though smart speakers such as Echo(™) and Homepod(™) are perhaps the most well-known, domestic IoT encompasses a wider range of internet-enabled home appliances including fridges, kettles, toothbrushes, lighting, and even childrens' toys.

Precise figures for Aotearoa New Zealand are unavailable, but global trends suggest sales of domestic IoT devices are continuing to climb[1]. However, whilst New Zealanders' attitudes towards privacy and data collection through websites, e-commerce platforms and social media have all been assessed[2], there is still a knowledge gap around privacy concerns and behaviours with respect to domestic IoT.

The most recent InternetNZ survey into New Zealanders' opinions on broad issues around the internet and digital society identified the privacy of personal data as a key concern[2]. This is in line with wider research into privacy perceptions, concerns and behaviours in relation to other digital information tools and platforms like social media sites and mobile phones. Research suggests that privacy and control of personal data in a digital ecosystem is of significant concern to segments of the NZ user base. While users' privacy concerns around social media and wearables are well-known in New Zealand and abroad, less is known about the privacy intentions and behaviours of users of domestic IoT, especially in New Zealand.

To explore these issues, we conducted a mixed-methods study incorporating a large-scale online survey of 930 New Zealanders, and 12 in-depth open-ended interviews with early adopters/innovators who already own one or more such devices. The large-scale online survey examines general relationships between trust, privacy concerns, and privacy behaviours of users and non-users of IoT devices. The in-depth interviews explore in detail the actual behaviours and dilemmas of early users who engage regularly with domestic IoT devices.

Our findings predominantly confirm the presence of paradoxical privacy behaviour in New Zealand IoT use. Furthermore, we identify a range of concerns that impact privacy behaviours: from privacy trade-offs, use of personal data, impact on vulnerable groups, and impositions from third parties and advertising. This report summarizes the main themes uncovered in the research, and we conclude with recommendations for users, corporations, and government and suggested areas for further research

[1] Moore, 2018

[2] InternetNZ, 2019

Summary of Recommendations

1. That New Zealand users are made more aware of the impact on domestic IoT of the updated Privacy Act (2020), particularly in relation to:
   a) trans-national flows of personal data and movement of their data between multinational corporations and data network;
   b) information about children who may share domestic space with IoT;

2. That further attention be paid to the privacy impacts of third-parties, advertising services and other uses of data that may not be clear to users at the point of disclosure;

3. That corporations explore possibilities to develop persistent privacy settings or privacy personas for users that can be implemented across their device ecosystems as an alternative to privacy as an attribute for a higher price.

4. That specific research be conducted investigating the privacy needs and concerns of marginalised groups' relationship to IoT, including children, the elderly, and those who have IoT devices imposed upon them.

Introduction

With the rapidly decreasing cost and size of sensors, and ever more ubiquitous connectivity, we are entering a world where the 'things' connected to the internet may quickly far outweigh connected people. Analysts suggest that there could be between 45 and 50 billion 'things' connected to the internet by 2030 across a range of applications[3]. Much of the IoT infrastructure already deployed in New Zealand is hidden in industrial applications, but the use of domestic IoT is increasing. Domestic IoT can be thought of as any home-based device that is connected to the internet and uses data to perform or automate home tasks. Examples of consumer-level domestic IoT range from wifi-enabled light bulbs through to video- and audio-enabled 'smart speakers' like the popular Alexa(™), Echo(™), and Google Home(™) models. Estimates suggest that smart home assistant device ownership could be as high as 10 percent of the global consumer market already[4]. These domestic applications are always-on, always-connected tools to enhance efficiencies in the home. Domestic IoT has the ongoing capacity to capture large amounts of personal information through inbuilt sensors, internet-connectivity, and by being linked to other devices such as mobile phones and wearables.

Using domestic IoT can offer consumers significant benefit but also involves the risk of data being used or shared in unexpected and/or unwanted ways. As such, the potential of IoT gives rise to new concerns and challenges, particularly around privacy in people's personal spaces. A recent survey in the United States, Canada, Japan, Australia, France, and the United Kingdom by Consumers International and the Internet Society[5] found that 63 percent of people find connected devices to be 'creepy,' and 75 percent do not trust the way their data is shared by these devices. Recent news articles highlight the growing importance of privacy issues, especially with respect to IoT[6]. Yet this has not stopped consumers from buying IoT devices, as nearly 70 percent of those surveyed said they own one or more connected device(s).

Wider research on smart devices suggests a kind of privacy 'paradox,' in which users' privacy concerns do not align with their privacy-seeking behaviours. Although there are debates about the scope and impact of such a paradox, it is generally agreed that there are differences between users' stated privacy desires and observed privacy behaviours in some contexts[7]. Previous literature has considered several potential drivers for this paradoxical privacy behaviour[8], including prior privacy seeking choices and trades-offs between disclosure and usefulness[9], perceived benefit[7] and risk perception[10]. Users' complex negotiations of needs and wants affect how they use their devices. Other research has found that perception of threats to information privacy, intrusiveness, price, and potential ease of use all present barriers to adoption of domestic IoT[11]. Privacy and disclosure around IoT are recognised as complex issues, drawing on technical factors like networked services, personal technical skills, perceptions of value, understanding of abstract risk and consequence of data use and misuse, corporate issues and regulatory frameworks.

[3] IDC, 2019; Phull, n.d.

[4] Abdi et al., 2019

[5] The Trust Opportunity, 2019

[6] For instance, https://www.dezeen.com/2019/03/05/smart-neighbourhood-brainport-smart-district-unstudio-netherlands/

[7] Kokolakis, 2017

[8] Aguirre et al., 2016

[9] Knote, 2019

[10] Oomen & Leenes, 2008

[11] Mani & Chouk, 2017

This study examines privacy concerns and behaviours among New Zealanders towards domestic IoT devices. It aims to provide insight into relevant factors that impact privacy concerns and behaviours. Privacy is an important topic as misunderstanding or ignorance of privacy issues can have undesired consequences for both consumers and organisations. Known privacy issues can cause users to stop providing personal information via commercially operated IoT devices, decrease their use of these devices, or even completely reject them[12]. Findings confirm that privacy concerns deter almost a third of people who do not own IoT devices from buying one[13]. In addition, negative experiences can lead to the spread of negative word-of-mouth which can result in declining sales and reputational damage.

This study collects data from both users and non-users using a large-scale survey among 930 New Zealanders, followed by in-depth interviews with 12 early adopters or innovators of home IoT. Our findings are largely consistent with global trends around technological adoption, privacy seeking behaviours, and trade-offs. Interestingly, the findings reveal different roles for media and social information, the place of brand identity, price perceptions, and perceptions of the place of domestic IoT in wider technical ecosystems. In New Zealand, the data suggests that while the government is seen as much less of a privacy threat than corporations, the state is viewed as an important monitoring force in relation to global information flows.

This next section will briefly outline the methodology, before discussing the findings of the research. The final section discusses the implications for the future of domestic IoT in New Zealand.

[12] Martin et al., 2017

[13] The Trust Opportunity, 2019

Method

We carried out a large-scale online survey in April 2020. A representative sample of 930 New Zealanders completed the survey. Respondents were aged between 16 and 87 years old with an average age of 33 years and a balance of genders. More than half had completed some type of tertiary education. The average annual income band ranged between $50,000 and $59,999. Of this sample, 397 people indicated they currently own one or more IoT devices at home, and 533 did not. There were some significant differences between IoT users and non-users. IoT users were younger, more frequently male, more highly educated, and had higher incomes compared to non-users. The survey asked questions regarding potential drivers of IoT device usage, as well as limiters, including privacy concern, and behaviour. Multi-item measures were based on existing scales used in the privacy literature, with adjustments made only to fit the context of IoT devices. The measurement scales and their respective items are detailed in the appendix.

The large-scale survey was complemented with 12 separate, in-depth, open-ended interviews with early adopters of IoT devices, carried out in June 2020. Although the recruitment of qualitative participants was disrupted by the global pandemic, 12 quality interviewees were recruited through online advertising on social media, IoT forums and subsequent snowball sampling. These factors result in an interview sample that is non-representative of the New Zealand population. The interviews were conducted via online video conferencing. Disclosing age and gender was optional for qualitative participants. Participants were balanced in terms of gender distribution, but reasonably to strongly self-defined as 'tech savvy' users of devices and could be characterised as innovators or early adopters in regard to domestic IoT. The participants were between 27-47 years of age, with an average age of 36 years. The open-ended interviews covered a similar range of themes to the quantitative measures. The in-depth interviews allowed us to further explore findings and gaps that were identified in the large-scale survey. These interviews were transcribed and coded for thematic analysis before being recombined with the survey data for analysis. The results are discussed below.

Findings

This section discusses the combined findings on the drivers and limiters of IoT adoption, and privacy concerns and intentions. Following the findings, this report will discuss the implications of these results and make recommendations for future research into domestic IoT in New Zealand.

Drivers and Limiters

Wider research suggests that domestic IoT adoption and rejection is shaped by both drivers and limiters of technology adoption, and this is confirmed in our New Zealand-specific results. Key drivers considered and explored in more detail in the in-depth interviews include perceived usefulness, perceived ease of use, curiosity about the devices, and perceived social pressure to adopt. The relative importance of each of the drivers differed between survey takers who already own and use IoT devices, and those who do not.

Survey takers on average perceive IoT devices as both useful and easy to use. As expected, current users of IoT devices rated the perceived usefulness, ease of use, and perceived social pressure higher than non-users (all drivers were measured with multiple items, responses ranged from 1 = strongly disagree to 5 = strongly agree).

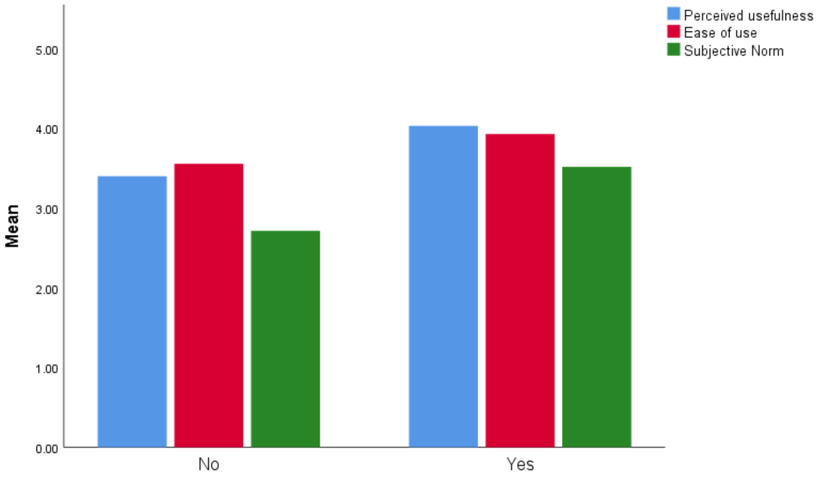

Figure 1. Average scores on key drivers for IoT users and non-users

For both current users and non-users of IoT devices, perceived usefulness is the most important driver of intention to use IoT devices. Thus, the key consideration for people considering IoT adoption is whether an IoT device is perceived to be useful for their purposes. These instrumental drivers were borne out in the in-depth discussion with users of these devices. Across the interviewees, common themes of basic functionality, extending existing digital tools, and ease of use are repeated.

Speaking about her experience of IoT, for example, Grace[14] says, “to be honest, it’s just a novelty, really, with an added bonus of being able to talk to things when your hands are dirty, like honestly, my hands are dirty a lot. So it’s actually quite good to be able to change the music or, you know, put on a timer or whatever.” She adds, “I’m really tech savvy. But I’m also that kind of tech savvy that knows that most of it’s

[14] all names used are pseudonyms. Some quotes have been lightly edited for clarity

a gimmick...I like them. If I didn't think they were working or there was a better option, I would probably give it away or sell it or just swap it for something that's a bit more functional." The ideas of functionality and easy integration into life flows are perhaps the most consistently articulated drivers for continued use of domestic IoT among the interview group. Unsurprisingly, given that the interview subjects are often tech savvy and self-identified as innovators or early adopters of domestic technology, curiosity about what and how it could be integrated into the home is a parallel driver for acquisition alongside usefulness, which aligns with wider research into the adoption of smart home technology[15].

Although perceived social pressure is considered an important driver by non-users of IoT devices, it is not for those who had already adopted and were already using IoT devices. Consistent with this, social pressures are not a key driver for the tech savvy early IoT adopters interviewed. Many interviewees note that they were the ones that others in their social group came to for advice and support in acquiring and using domestic IoT, so the weight of social pressure to use may change as domestic IoT becomes more mainstream. However, interviewees note concerns they had for *other less technically adept users of these devices.* For example, Fiona notes "I'm not concerned about me. But the more our houses get filled with these devices, the more potential there is for the person who controls the devices and who has the most knowledge about the devices to use them to hurt people in ways that are not obvious from the functionality of the device, like you would think that, like lights, that's not a big deal. But gas lighting literally comes from controlling the lights." This concern is evident in relation to several other drivers and limiters of IoT adoption.

Overall, the survey suggests that the intention to use IoT devices is higher for younger people, and those with higher incomes. Younger people also report being less concerned about privacy as compared to older people. Gender, education, and the number of children in the household do not affect either intentions to use IoT devices or overall privacy concerns.

Responses offer additional potential drivers for uptake. Interviewees hold notably strong views on the companies that make and service these devices, and the devices themselves. Although there has been limited discussion in the wider literature about these user-corporate relationships, our interviewees hold clear opinions about their devices and how they connect through corporate entities and with global data networks. Respondents consider the device as part of an often explicitly branded information system, embedded in corporatised and commercialised exchanges, and connected to international information flows.

William considers IoT devices as "a constantly evolving product that is only represented as the tip of an iceberg by the physical piece of hardware in my house. And you know, in reality...it's not a static purchase where you buy an X and you expect it to be an X and do X things until it is broken and can no longer do those things. It's really a service that you opt into in the guise of hardware." Many respondents articulate an explicit awareness of all the hidden connections behind the device that made the device run—whether this awareness would extend to less technically savvy users is an area for further study.

Many of the responses concern issues related to data sovereignty and overseas data centres (which this report will return to when discussing issues of context). Surprisingly, many respondents also explicate a link between the ethical reputation of the provider companies and the interviewees' own levels of trust or distrust in those branded devices. As William bluntly notes, "Amazon is a company that I have deep moral objections to and therefore steer as clear from as I possibly can." Sam refers to the reputation of a

[15] Ford & Peniamina, 2016

corporation more broadly to make a similar point as a driver for technological adoption: “Because Apple is just really pro privacy. Like, they’ve refused the police and investigations on user data before and so that was important to me.” For these users, reputation matters.

This reputational effect extends to the devices themselves. This effect is framed either as a positive or negative association, based upon these wider corporate associations, familiarity with particular types of devices, or even perceptions of device quality. Often, familiarity with the device ecosystem is the decisive driver for choosing between different domestic IoT options. This is in part related to comfort and knowledge of user experience (UX), partly acceptance of the brand associations, partly convenience of devices seamlessly integrating into wider digital lives, and partly a trade-off between disclosure and functionality or a way of keeping personal information bounded to one set of user agreements. Sometimes, though, the expressed attitude is one of pragmatic resignation, such as when Jake notes “Yeah, I’ve let these devices into my house. They should be doing things appropriately, but I can’t guarantee that’s the case.”

Concerns and Contexts

The in-depth interviews provide further insights into more specific privacy concerns that users of IoT devices have. These concerns centre around a few common themes: use of data beyond the device; third-party access to data; surveillance; and issues of data sovereignty. Furthermore, this research highlights several points related to data collection and use that respondents reportedly baulk at when these occur in their daily digital environments. These include dark patterns, perceived targeted marketing and wider data spread.

In this study, surveillance or privacy intrusions from state entities are generally of little concern to New Zealand users. As Thomas summarises, “this is very privileged to be able to say this. We don’t live under a surveillance state”. However, for several users, problems arise once they consider the possibility of their data leaving their home and their home country. Andrew notes, “In general, private data from New Zealand ending up in the States is a given and those are the concerns that I have with Amazon, and Google, they are centralised in the US, which means—I don’t like US law. It’s very commercially driven, whereas New Zealand law, I would consider it more people driven.”

Andrew is not the sole participant concerned about issues that might be grouped under the banner of data sovereignty. Several of the interview respondents had looked at their network traffic and noted the amount of information going to overseas services and sites. This concern is partly in response to the jurisdiction of data. These tech-savvy users realise that once their data leaves the country, it may be subject to different standards and rights, and that is a source of mild concern. There may be space, within the wider discussion regarding domestic IoT, about localising data traffic or more clearly communicating legal rights and responsibilities, and this idea will be discussed further later in this report.

Beyond sovereignty, and considering the amount of personal data in circulation, some respondents see the movement of their data to overseas jurisdictions as a continuation of the mindset that ‘the privacy horse has bolted’. For others, the loss of control of their data is a source of mild anxiety—but as users, they had accepted that trade-off as part of their use of the device. As William summarised a sentiment held by many of the interviewees, “the tradeoff to my mind is kind of around picking your poison privacy at this point.”

Use beyond the device and its network is a recurring theme in these interviews. While the interviewees sometimes see the benefit of their data being used in larger data sets within the ecosystem of the device, their information escaping that space to third parties or other uses is significantly concerning. As Fiona bluntly notes, “I would say that consumer [surveillance] concerns me more day to day, because it’s the more real threat. And to the best of my knowledge, there is currently no one, you know, who is interested in surveilling me. So, that’s a hypothetical, but it’s not an immediate issue, whereas Amazon is definitely trying to sell me shit.” For many users, this reuse of their data betrays the unspoken agreement between themselves and their devices. As Alice adds, “selling [data] to third party retailers. That’s the killer. It’s a killer. Yeah. As soon as it did that, I’d be like, No, no, no. Because, again, I’m willing to negotiate with the government about data merging from data sets. I don’t trust third party providers at all.” These savvy users are willing to trade their personal information for functionality but want to know who they were trading *with*. This notion of third-party access to data is perhaps one of the bigger concerns raised across the interviews. While there is an acceptance that using domestic IoT involves trade-offs of data for functionality, there are points at which the trade-off becomes too unbalanced for user comfort.

Part of this lack of trust in who interviewees are trading-off data *with* is linked to the use of data patterns. These patterns are UX design choices that attempt to coerce users into particular behaviours or disclosure. As William notes, “when it comes to things that intrude in my life and encourage me through the use of dark patterns to do things I do not want to do, that’s certainly a space at which I would go no, absolutely not. Gone. I’m going to… I’m going to make a stand and I’m going to stop using the service because it is now putting advertising in front of me or because it is now asking me to do something I do not want to do.” For many, this idea of coercion is a critical pain point in managing their IoT devices’ data and their own disclosure. This is often interwoven with users’ perceptions of the ethics and practices of the company and their trust in the device.

Jane views her devices as part of a trusted ecosystem that is not entirely data-tight: “I think they’re leaking. I think it’s a leaking container.” Robert has an even broader scope of concerns: “Anything they collect is going to be commodified because they’re usually businesses and that’s what they do. And you never know where it’s going to be sold and what it’s going to be sold for.” For respondents, whether the information is directly or indirectly acquired by companies outside the device ecosystem, the impact and erosion of their trust and comfort is the same. Distribution of personal data is acceptable in return for the functionality of the data, *but only to a point*.

Thomas has a slightly different view, doubting that personalisation comes from data leaks directly from these devices: “I think that those stories are apocryphal. I think it would be a lot more widely known if that was actually a feature. I mean, if I said the password to make it listen, and then started talking about a particular product and asked it for a review of the book, then yeah, but no I have never witnessed any ads that have come through based off of conversations I’ve had.” This aligns with our survey findings which suggest that media coverage of privacy breaches have little impact on intentions to use IoT.

Beyond marketing, there are also wider concerns about data use and reuse. Fiona notes, “they’re using this data to kind of draw ‘Big Data’ conclusions in unethical and fallacious ways. And I don’t want to contribute to that, regardless of whether it’s going to come back on me personally about the specific data.” These wider concerns about data use and reuse are often tied to other concerns, including trust in the device, perceptions of the company providing the service, or worries about less technically adept users attempting to negotiate trade-offs with these kinds of devices as mentioned earlier.

Throughout the interviews, after expressing such concerns or reluctance about data leaks from the ecosystem of the IoT device, interviewees often become pragmatic about their wider data contexts, noting all the other ways that personal information is scraped, gleaned and shared from endless sources. In a way, they see their entire digital lives as ‘leaky,’ and their domestic IoT use as simply a further extension of encroachments into their personal information sphere. Some respondents raise examples like shopper loyalty programs as their first step into becoming comfortable with the idea of trading personal information for benefit. This comfort extends into the realm of social media use as a forum where personal data becomes a public commodity. For many, this varying level of comfort impacts directly on behaviour around IoT devices, and the rationale for privacy seeking behaviours.

Respondents point to a number of other contextual issues that may influence future domestic IoT use beyond the trade-offs of functionality. Some interviewees mention acquiring domestic IoT already built into traditional devices (with varying levels of functionality). Phillip explains that "it was kind of a gradual creep of all of these technologies and then getting devices which are specifically for that feature." This is a common experience, as isolated 'smart-dumb' devices slowly link together in an emerging domestic IoT ecosystem. Some IoT is more dumb than smart, as Phillip has experienced: "even the toothbrush has Bluetooth features as well, which was an enormous gimmick and I stopped using it pretty much, I think I talked about it like 10 times more than I ever actually used it." Fiona had a similar experience with a wifi-enabled heater, noting "we didn't go out to get our app controlled heater and I'm like, this is stupid."

This scope creep links to economic trade-offs. In line with other research[16], interviewees were asked to consider whether they would pay more upfront for a more secure or 'dumb' device. Some claim that they would pay a small premium, but there would be a point where the economic cost would not be worth the trade-offs given the amount of information already in the wider data ecosystems. As Robert explains, it "would depend on the price value, the price point. So like, if it's significantly more than what we did [pay], it's the cost benefit calculation. Yeah. Like, how much are we willing to pay to maintain [privacy]?"

Other respondents feel that enough data is already circulating, or the existing systems are so 'leaky' that paying a premium for privacy would be paying for a feature that could not be guaranteed. Like many others, Grace notes that she might buy a privacy seeking device but "I'm not sure I'd want to pay [for] it to a company because you're still putting your faith in that company...and how often do we do that by someone and it doesn't work." She adds, "if there was such a thing as a privacy plus [paid account], I think it should just be privacy full stop, you know, they shouldn't be paid services for extra privacy. It should just be, you know, you have it or you don't, basically." William summarises a common underlying thread throughout these conversations: "[p]rivacy is now the domain of the wealthy and that's a really sad state of affairs." These comments hint at two possible future frames, where either privacy is a premium for the wealthy, or that the cost to trade-off equation flattens out until it becomes uneconomical to offer privacy as a premium feature. This is an area that could benefit from future study.

Scope creep could represent either a benefit or a concern, depending on the instrumentality of the functions encroached upon by IoT. One area of particular sensitivity, however, is the collection of data by IoT devices from minors in the household. Children are singled out as a potentially vulnerable class who are simultaneously growing up with domestic IoT as part of their home landscape. Respondents either restrict IoT from children's spaces (such as bedrooms) or analyse the device with much more care than they do devices that collect their own (adult user) data. Interestingly, adult interviewees report that children identify similar drivers for acquisition—curiosity and functionality. Andrew sums up the experience when he notes that "The Echo Dot, [it] was my daughter [who purchased it], she was wandering through a store and it was an impulse buy for her birthday...But then I got a hold of it, I was going, alright this is listening all the time. Okay, what can she get out of it? And I went through all of her accounts, and after about twenty minutes, I came to the conclusion that there's nothing [the device gathers that] isn't available in about a thousand other places. So I think we came to the conclusion that well, she's got this thing we may as do things [such as control lights]... it's convenient for those things."

Interestingly, in our large-scale survey, people with one or more children in the household on average report having slightly more trust in IoT companies than those without children. However, having children

[16] Elvy, 2017

did not affect users' privacy concerns, intentions, or behaviours. These perceptions may change when people are asked about their privacy concerns, intentions, and behaviours specifically in the context of their children using IoT devices, as suggested through the in-depth interviews.

Much of the existing literature focuses on the one-to-one relationship between a single user and their domestic IoT and there is a need for future research considering the place of these devices in relation to different domestic arrangements, including families with children or flatmates.

Finally, interviewees mentioned the physical context of the device in relation to continued IoT use. Beyond the focus of personal data as ephemeral information traveling globally for benefit and use, users are quick to articulate issues around the physical presence of the device in the home. For many, the device is confined explicitly to one room or area of the house, most often away from bedrooms or similarly personal spaces. Some users are conscious of the extent to which the devices can 'hear' or 'see' and sought to position the device according to their personal preferences. Again, the trade-off between functionality and privacy is impactful here: kitchens often represent a middle ground, not too private, but within earshot when the device needs to be useful.

Extending this theme, users are to varying degrees wary of devices with active cameras or microphones. For some, smart IoT is limited to what can be controlled through the mobile phone. Interestingly, many interviewees are adamant about not introducing devices with live mics or cameras in the home, only to then reflect that they own tablets or phones with this functionality. For others, active mics are primarily acceptable, depending on their placement in the home. Cameras, in contrast, have limited acceptability and are mostly pointed at external doors or otherwise facing outwards from the domestic space. Again, though, these devices are primarily instrumental, and it is rare that users seek to specifically defeat active microphones or cameras once the device is situated in the home, though they do take some mitigation steps that will be discussed in more detail in the following section. Once acquired, the device's ability to 'see' or 'hear' is mostly accepted. The spatial orientation of the physical manifestation of domestic IoT is linked to others in the home, to wider data ecosystems and to issues of trust. Retaining IoT functionality while maintaining a level of desired privacy is an area that may benefit from future research.

Trust and Privacy

Throughout and underlying much of the data collected are themes of trust and privacy. As has been noted, many of the interviewees contextualise their use of domestic IoT through already-held trust in brands and companies, and often extend that trust into these new devices as they satisfy their curiosity about what such home devices can do for them. Trust in companies to maintain both formal and implicit covenants about users' data, and trust in devices to respect the boundaries of the home have already been discussed. But trust is also developed in the wider context of the information economy.

The results from the large-scale survey indicate that lack of trust in the IoT provider, previous invasions of personal privacy, and prior knowledge of potential misuse of computerised information all lead to increased reported privacy concerns. On average, survey takers report moderate levels of trust in IoT providers, but non-users have significantly less trust than users. Moreover, most survey takers indicate that they have personally been the victim of an improper invasion of privacy in the past, with only 6.9% indicating that this had never happened to them. And, although most survey takers indicate having heard and read at least a moderate amount about the use and potential misuse of computerised information, 38.6% report having heard and read 'a little' or 'none at all'. This could indicate that a large proportion of people are largely unaware of the risks and potential damage associated with privacy violations.

For non-users, lack of trust in the IoT company is the most important contributor to privacy concerns, but this differs for users. Lack of trust, previous experience, and prior knowledge, all contribute equally to users' privacy concerns. Interestingly, and consistent with previous research findings[17], this survey's results indicate no link between privacy concerns and the intention to use IoT devices. Although people are concerned about their privacy, these concerns do not affect their intentions to use IoT devices. Figure 2 shows survey takers' reported privacy concerns (1 = not concerned at all, 5 = very concerned) and intentions to use, or continue using, IoT devices (1 = no intention, 5 = high intention).

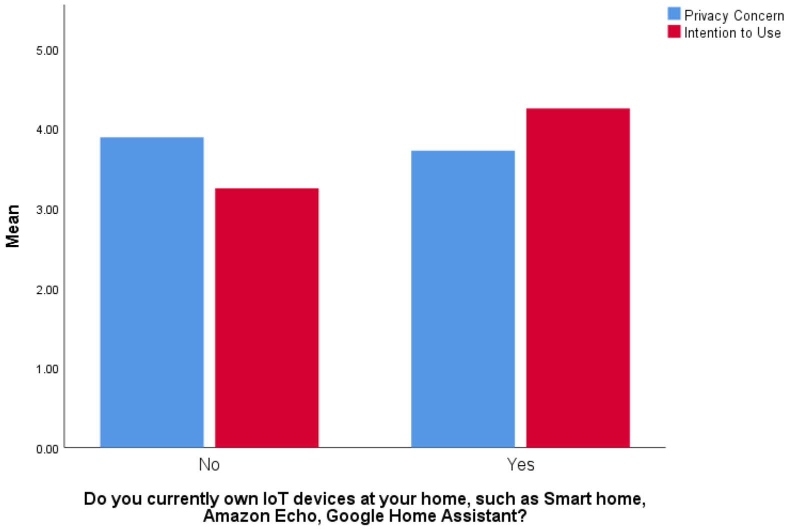

Figure 2. Privacy concern and intention to use for IoT users and non-users

Further to the survey data, the interviews break down different aspects of trust concerning domestic IoT ownership and use in relation to ongoing privacy negotiations. Interviewees frequently articulate complex negotiations in their daily use of these devices. Respondents, as part of how they evaluate their trust in disclosing personal data, refer to their wider information architecture, patterns of disclosure, and the amounts of information already freely shared and stored, both online through platforms like social media, but also in everyday information tracking projects such as shopper loyalty programs. Robert pragmatically notes "you can tick those boxes and say, you don't collect this forever and you'll find out in 10 to 15 years that they've completely ignored it, and there is a certain level of acceptance that in this current climate and how our society works, that that's going to happen." Thomas has a similar attitude, saying "I just accept [privacy] as dead as part of the world that we live in." For these users, seeking privacy is not worth the extra effort, as enough information about themselves is already captured and stored outside their control.

However as hinted at in the preceding discussion, privacy is something some users seek to a point, after which the discomfort and work of privacy exceeds any perceived benefit. These concerns are often aligned with what might be termed privacy fatigue. Sam, for example, states, "I'm reasonably concerned. But I'm not paranoid concerned. If I was paranoid concerned, I would have that separate network already, I would have had it set up and I'm just not quite fussed enough for that. But I am worried about privacy." Some fatigued users also comment on often-changing privacy and data policies that users are required to agree to in order to continue to use sometimes very expensive devices. Respondents even link their level of trust in the company to the frequency of 'privacy updates' they receive; more frequent updates result in less trust, which ties back to issues around trust in corporations that service these devices, which as Lisa noted meant

[17] Church et al., 2017; Hallam & Zanella, 2017

“going through and checking, you know, all your settings are still private whenever they update the policies [it’s] super annoying.”

While interviewees often make references to wider media coverage and prior knowledge of breaches of trust and privacy on IoT devices, for many these are points of interest rather than information that shapes their use decisions. This level of confidence in their knowledge might be expected of early adopters. Thomas’ comments reflect the general mood of interviewees: after talking about the articles he read on privacy issues and IoT while researching which device to buy, he notes, “I read them and I tend to have a laugh. And then I just move on and continue living my life.” Where media coverage impacts users, it is in very specific cases, and does not significantly change overall reported behaviour.

Overall, users negotiate their trust in various parts of the domestic IoT infrastructure in the context of their own perceptions of their privacy values and their perceptions of wider data use and capture. This negotiation happens primarily during the acquisition and setup phases. Although some privacy-seeking behaviour is ongoing (such as spatial placement of the device), ultimately users purchase a device to be functional; and to achieve this, they must permit it to access personal information.

Privacy Protection Behaviours

On average, survey takers report being relatively careful about sharing their personal information while using IoT devices. There is no relation between intention to use IoT and privacy protection behaviour. Moreover, users and non-users report almost the same level of protective behaviour. Both age and gender are significant predictors of privacy protection behaviour. Our survey confirms what previous research has indicated, that older people and females are more protective of their personal information.

In their device use, interviews offered a range of practical approaches to maintaining a desired level of privacy control while using domestic IoT. These behaviours often represent complex negotiations across a range of factors already discussed. That they have domestic IoT is often the first choice; although, as noted, scope creep has begun to impact this decision-making process. For the more complex domestic IoT there is a deliberate decision to use the device, which includes the initial choice of device, whether it includes active microphones or cameras, and the ecosystem in which the device is embedded. Once acquired, most interviewees remember at least skimming the terms of service and privacy policies for their device(s). Their behaviour in engaging with these policies tends to fall across three broad approaches.

Firstly, some users read quickly, looking for clauses that are out of the ordinary in comparison to their experiences within their wider data ecosystem. Grace is representative of this approach. As she recollects, “I just sort of flick through ...to see if there’s any, you know, key points that I need to know go through or if I’ve signed my life away and usually answers yes. But that’s also a decision that’s usually overwritten by the fact that you’ve got the device you need to get it working.” This approach aligns with ideas of privacy fatigue where there is a conflict between the work of maintaining privacy and achieving adequate functionality (through providing access to personal data).

The second approach is more in line with ideas of curiosity and experimentation outlined earlier. Some users go through their settings more carefully, but tactically allow the device access to help improve the device or service. William, for example, describes himself as “the kind of person that goes through every single possible setting and signs up to every possible data program and continue to give a certain amount of feedback and data back to improve the products...Because I think one of the fundamental reasons that I do what I do when I’m in the industry that I’m in is to make good things accessible.” He is not alone in feeding the device carefully curated data in this way to see what it then does.

The third approach is perhaps the most privacy seeking. This group of users deliberately work through all policies and settings to lock their devices down as tightly as possible while still retaining the desired functionality. These users are perhaps the most acutely aware of the trade-offs of data for function. As Jane bluntly explains: "I've set my own account to ultimate privacy mode, as close as I can be without disconnecting myself from that system entirely." However, as these interviewees are the first to acknowledge, this is a time- and skills-intensive process that can disable the device. And, as Jane demonstrates mid-interview, devices persistently seek to increase access to personal data through reminders and suggestions to connect—reminiscent of the dark patterns discussed earlier.

Once in the home and operating, some (but not all) interviewees report sometimes controlling the device's access to private information. Much of this work takes place in setup, including location of the device or putting IoT on its own, tightly fenced network. Less common strategies take place post-setup and include unplugging the device when not in use or when the primary user is not home, or moving away from the device when dealing with sensitive matters or conversations. This latter behaviour is perhaps the most common, representing a trade-off between functionality and privacy, and reflecting the idea of different spatial areas of privacy (aka: bedrooms as being more private than kitchens). Thomas, for example, explains how, when discussing commercially sensitive matters, he walks to the other end of the house away from their smart speaker to have the conversation (despite having the conversation on a phone that shares the speaker's ecosystem). Clearly, the focus of privacy seeking is on the person's behaviours, rather than the device itself: specific functionality such as active mics are not isolated for focused privacy protection behaviour[18].

In line with other concerns, users also report taking steps to prevent surveillance, particularly commercial surveillance or third party access to their data. These include ad blockers, filters and other tools at the DNS level, or co-managing different ecosystems to keep searches of interest to marketing services separate from the day-to-day use of their primary information ecosystem.

It is not just advertising and commercial surveillance that interviewees reportedly attempt to defeat. Non-commercial, non-governmental use of data is a theme of emerging concern. Users, especially those who have consolidated in a single ecosystem by staying a branded product suite, report concerns regarding different data categories, and talk about exploring tools to prevent data 'mingling'—whether this be between, for example, their work and home persona, or between different users in a household. Some express frustration at their inability to act more directly in this area. As Alice notes, "I'd love to be able to wall off. I mean I already do to a certain extent; I wall off my work and my personal stuff to different apps and different applications and I do that specifically. Um I'd really like to be able to say...just don't touch it, it's work. And then everything else is something that you [the device] can access." This concept of segmenting data disclosure to manage trade-offs is an area for future research.

Overall, user behaviour in relation to domestic IoT devices is best understood as a series of trade-offs between disclosure and functionality, framed within users' expectations of privacy, perceptions of their information environment, and sense of previous data disclosure. As these devices improve in functionality and use—more than one interviewee mentions issues with smart speakers and Kiwi accents—the trade-off leans more towards functionality and obscures the issues of disclosure and data use these early adopters experience.

[18] For example, ultrasonic jamming hoods for the Echo: https://techcrunch.com/2020/07/27/mschf-drops-an-ultrasonic-jamming-device-add-on-your-amazon-echo/

Implications

The key driver for IoT adoption and usage for NZ users was the functionality that these devices offer. The benefits of owning IoT at the moment clearly outweigh perceived privacy risks, as privacy concerns were seen to be unrelated to people's intention to use, or continue to use, IoT. Users do take some steps to manage that trade-off, such as containing their usage within familiar ecosystems, or only interacting with certain providers or types of services. But they acquire these devices to be useful in their day to day lives, and privacy and disclosure concerns easily fade from view. As the interviews demonstrate, users speak of the functionality 'to me' and the concerns of breaches or privacy violation as mostly happening 'to others'. Although media stories and prior experiences contribute to privacy concerns, particularly for non-users, interviewees report that privacy violations reported in the media or by peer groups do not encourage an immediate sense of privacy concern for themselves, but could elicit concern for others. This is in line with wider research, which notes that risk is often an abstract threat compared to the tangible observed benefits of use.

Alongside this, users come to domestic IoT having experienced other types of networked identity, including social media and other services predicated on data aggregation. Their successful use of these kinds of services further foregrounds functionality and trust and helps diminish privacy risk. It also contributes to a feeling of trust in specific (often commercial) ecosystems with which they are familiar or have a history of successful use. This is underlined by a mistrust in third parties that may also access personal information, or through the use of dark patterns or other perceived coercion. Finally, users invest in these devices to fulfil a need, which drives continued use and commitment to use. These practical drives often involve committing to a trade-off between disclosure and use to receive the full benefit will little perceived room to negotiate a reduced disclosure.

Moreover, privacy management itself is often perceived as difficult. Beyond tactical decisions regarding the device itself, users largely accept that at least sometimes their personal information is available to and used by different corporations. Sharing personal information becomes problematic for users when they do not know where the information goes and for what purpose —users feel in control when they know who they are trading-off with (such as a large and well-known corporation). Only when they sense that their data is traveling beyond that arrangement do they start to express discomfort.

Our research also suggests that this sense of control also applies in the home. Users often speak about accepting the trade-offs between themselves and their devices, but being worried about others, such as children, or reporting the worries that others in the home have towards the devices. Users also often develop ad-hoc solutions to any specific domestic concerns, such as carefully considering the placement of the device.

Scope creep is a minor concern for users interviewed. This could possibly be because they have already made the decision to engage with domestic IoT and so additional internet-enabled devices could be slotted into this existing domestic ecosystem with minimal disruption and an existing pattern of use. In this situation, IoT functions are understood purely within the context of whether the new device can 'talk' to the network. Interviewees note the lack of choice about, or coerced entry into, owning domestic IoT which also links to concerns about other users managing their own control of their data. However, scope creep may be a more significant concern to non-users. The moderate trust in IoT companies reported by the survey may be impacted if new users are forced by scope creep and IoT pricing to engage with IoT devices, rather than seeking it out themselves to fulfil a need. However, wider trends in IoT suggest that, at least below premium price points, IoT functionality may soon be the norm rather than the outlier, and there is need for more research to understand how this might change perceptions of trust, functionality, intention to use and privacy seeking behaviour.

Negotiations of trust and disclosure are complex, and users' responses imply a sense of covenant with their devices that is reinforced when they perceive 'their' ecosystem doing the right thing. This covenant is shaken by direct threats like dark patterns or indirect ones such as regularly updating and changing privacy policies. As noted, as long as the device is seen to offer a useful benefit, users are willing to relinquish a certain level of personal information. However, alongside this is the recurring theme of concern around the selling of personal information to third parties. For the users we spoke to, the trade-off is with a corporation for functionality, and should not be a means to be marketed to by unknown third parties.

For corporations it is important to understand that consumers' trust and privacy perceptions are linked to reputation—users value consistency. Interviewees suggest, for example, that frequent updates of privacy policies negatively impact their trust. As privacy is considered a complex issue, it is beneficial for corporations not only to be transparent but also to establish some sense of user agency in relation to these devices. This also ties to interviewees who expressed concern about non-technical users, as already mentioned. A user's ability to audit and monitor one's data trail should not be reserved for the highly technically skilled.

Another trade-off some users are willing to make is the one between the price of the IoT device and perceived privacy. Users are conscious that part of the 'price' of the device is the data it gathers, but when asked if they would prefer to see that cost on the price-tag, respondents either did not wish to pay or would only pay a little more for retaining their data and retaining full functionality before they felt the financial trade-off wasn't worth the level of privacy potentially offered. Again, corporate reputation is a factor here in splitting the consumer cost between the sticker and the disclosure, and being explicit about the 'cost' of disclosure.

For the interviewed users, IoT is considered an extension of their device networks, such as their mobile phone. They do not see IoT as a separate product category. This further embeds both trust in the providing corporations and a sense of control over their data ecosystems as key to their trust in the device and the data it could potentially gather. However, users expressed a desire for more fine-grained controls, such as being able to segment their data to better represent their lived experiences (such as a work self versus a family self).

Moreover, IoT devices are often used in a household setting which can involve other users, including more vulnerable groups like children. As yet, little work has been done to take into account these secondary relationships between users' domestic social networks and domestic IoT devices, but these results suggest that the spatial context and wider user group(s) of these devices need to be considered when designing and building protection policies for these devices. These would need to account for both data collection, storage and use, but also increasing users' trust that when the device is not meant to be 'listening' it is truly inactive.

For governments and national agencies, domestic IoT is a growing market presenting interesting risks and challenges. For the users we spoke with, data sovereignty is a critical issue. Impending updates to the Privacy Act that address extraterritoriality concerns may go a long way to calming user worries and increase their comfortable using these devices. However, in order to allay user concerns, this localisation of privacy standards will need to be seen in action and enforced.

Currently, users report a high trust/low concern relationship with the State, although this may in part be due to biases in the interview panel. Users in different socio-economic groups, users whose experience of domestic IoT is punitive or more explicitly around surveillance for control, or who have had wider negative experiences of state agencies in the home, may report different levels of trust, and this is an area for future dedicated research. For our users of consumer-market devices, concern about the use or misuse of their data in regards to criminality or state sanctions is low, although again concern for others in this space is noted.

What does concern our respondents is the lifespan of the data collected and a constantly changing national and international political landscape. Users are starting to become conscious of the amount of data in circulation and what could be deduced from connecting these datasets. Expiry dates on data collected commercially may be an area of future enquiry.

Overall, the trend is for increasingly widespread and domesticated IoT in New Zealand. While users here share the concerns and intentions of users in many other countries, they are also concerned about their impact and ability to steer nationally- and culturally-specific functionality and restrictions on the device, whether that be to recognise kiwi accents and slang or to trust that the device will respect NZ privacy expectations. For users, particularly those unwilling to pay an upfront premium for 'dumb' devices, reassurance that the trade-offs they make for functionality are honoured is key to comfortable and empowered uptake of domestic IoT.

Recommendations and Future Research

As domestic IoT is an emerging area for New Zealand, this research identifies several lines of enquiry that may benefit from future research.

Firstly, this research indicates a need for further enquiry into the needs, desires and concerns of late adopters, vulnerable groups, and others in an IoT-enabled home. Parents and childless survey takers responded similarly when asked about their own privacy concerns, intentions, and behaviours. However they may of course have responded differently if specifically prompted regarding vulnerable groups, such as their children. A recurring example from the interviews was whether and to what extent users needed to consider children in the household who interact with domestic IoT devices. Beyond smart speakers, heaters, and light bulbs, there are even a range of connected toys including connected action figures, robotics, and learning development toys which are directly targeted at children, and further research is needed to assess if paradoxical privacy behaviour is observed in this context.

Interviewees also identify less technically savvy users as vulnerable when using IoT. They note the need to more carefully consider this group's specific needs at the design and purchase stage to assist them in managing trade-offs and disclosures on complex IoT data networks. It must be noted that, due to the nature of sampling and the online survey instrument, this study skews towards technically-enabled groups representing on a narrow socio-economic strata, and future work could look more specifically at those currently at risk of being left behind in a digital divide. There is also scope for work exploring what types of messaging may empower this user group to engage with IoT in ways that align with their privacy desires. Further, our study reveals that gender and age do not influence privacy protection behaviours. Our survey was conducted among a representative sample of adult New Zealanders, only six survey takers were aged 80 years or older. We can therefore not draw conclusions about differences between older and younger people. However, a growing segment of domestic IoT includes accessibility, mobility and independence aids, and within an aging population, the specific concerns and needs of older users should be accounted for more fully in future research.

This research notes the importance of the spatial dimensions of domestic IoT as a thing. As a new technology, users are still experimenting and engaging with the physical functionality and their interactions with their devices. For some devices, how they are situated in the house is determined by function, such as light bulbs. For other IoT, users renegotiate their physical space as part of how they adapt to their devices. Whether this will continue is an interesting question for service providers and device designers. It is possible, given the skew to less privacy protectionism from younger potential users, that when they do acquire devices they will be less concerned with where the device is in the home which will in turn drive future functionality.

As our interview subjects note, domestic IoT is still an emerging field. Many of the major providers are not officially available in New Zealand as of the date of this study, and several of our usergroup either purchased their devices overseas or acquired them through grey or parallel import services. As such, our user group may be more conscious of data traffic, extra-territoriality and data sovereignty issues than a generalist user population. Although impending changes to the NZ Privacy Act may preempt some of the concerns raised in this study, finding the right messaging to reassure and empower users in regards to their privacy rights on these devices may be a key project in the coming years, and ongoing research may assist in assessing if these concerns continue or diminish.

This research notes the potential impact control and commercialisation of personal data may have on device adoption and use. Dark patterns, third parties, personalised marketing and big data are examples of concerns users report having about their personal and private information once it is on the internet of things. The tension between data privacy and personalisation for commercial purposes has been referred to in the literature as the 'personalisation privacy paradox'[19]. The use of personal data for commercial purposes has previously been studied in the context of website personalisation[20], and Facebook[21]. Future research may study the personalisation privacy paradox in the context of IoT devices, focusing on the trade-offs between functionality, information transparency, and willingness to partake in, or be exposed to commercial personalisation in the context of IoT, and its impact on continuing trust and use of these devices.

Finally, as part of these concerns, 'privacy as a premium' is still a possible outcome in balancing commercial and user interests in the operation of domestic IoT. Our users are divided, with some willing to pay a small premium to retain personal information, whereas others see privacy as an, if not extinct, at least dying concept not worthy of financial investment. There is space in this area for further research, including experimental models, to assess the scope and continued engagement with privacy premium approaches. As an emerging field with a range of potential applications, there is significant work still to be conducted in this space.

[19] Awad & Krishnan, 2006

[20] Gurau et al., 2003; Lee & Cranage, 2011

[21] Jamal et al., 2013

Conclusion

This research aimed to assess the extent of the privacy paradox between the self-declared privacy concerns and behaviours of New Zealand adults with respect to IoT. We used a large-scale survey among 930 New Zealanders to examine people's drivers, limiters and privacy concerns regarding IoT. We conducted 12 in-depth interviews with tech-savvy early adopters to further explore users' specific privacy concerns, behaviours and the relevant contexts of their concerns and behaviours. Although most people indicated that they are relatively concerned about their privacy, we still found evidence of a privacy paradox among NZ users.

The main driver for domestic IoT adoption and usage is the functional benefits that IoT device(s) offer, and interviewees express a willingness to trade-off privacy and personal information for this functionality. Additionally, perceived ease of use and social pressure are also important drivers to adopt IoT, especially among people who are not already users of domestic IoT. There is space for further research into coerced IoT adoption, scope creep of devices or punitive domestic IoT, as these user groups may raise additional privacy concerns.

But for domestic IoT, trust is a key factor mitigating privacy concerns. Interviewees frequently spoke of being reassured by familiar, often branded, ecosystems when they extend their digital footprint into domestic IoT. If personal information is already shared within an ecosystem there is a sense that there is no significant additional risk of adopting IoT within that ecosystem. Hence, familiarity contributes to trust at a number of levels within the complex trade-offs users make when deciding how and to what extent to engage with domestic IoT.

Transparency and control further mitigate privacy concerns among our interviewed users. Information sharing is accepted up to a point, and in certain contexts. Knowing where the information is stored, and for which purposes it is used gives users some reassurance and helps foreground functionality over disclosure concerns. Conversely, lack of transparency and a decreasing sense of user control can diminish trust and increase privacy concerns. This lack of transparency also translates across users' device experiences. Trust in IoT providers and data privacy diminishes as users grapple with unclear and constantly updated privacy policies, dark patterns and coercive interfaces, and an environment in which data may be passed to third parties or monetised in unexpected ways. Once trust is undermined, it may be very difficult to recover.

These commercial surveillance concerns completely eclipse any concerns users have about other types of surveillance. However, our research suggests there is a need to further educate and communicate with the growing user base about their rights and privileges as New Zealanders regarding their personal data used in this trade-off for device functionality. Users are concerned they yield control of their data to overseas corporations, data-sets and third parties, and that loss of control is just the cost of using transnational data flows from a tiny country at the bottom of the ocean. Any strategies that can further empower users to negotiate better negotiate satisfactory personal trade-offs will benefit a general New Zealand user group of domestic IoT devices.

Acknowledgements

The authors would like to acknowledge the assistance of Shelley Dixon and Sreejith Pillai during the research process.

They would also like to thank all those who volunteered to participate in this research for their time and involvement.

Many thanks to the Office of the Privacy Commission’s Research Good Fund for supporting this research.

References

Abdi, N., Ramokapane, K. M., & Such, J. M. (2019). *More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants.* Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019). https://www.usenix.org/conference/soups2019/presentation/abdi

Adhikari, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing,* 31(2), 96-110.

Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing,* 33(2), 98–110. https://doi.org/10.1108/JCM-06-2015-1458

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, 30(1), 13–28. JSTOR. https://doi.org/10.2307/25148715

Block, I. (2019, March 5). UNStudio develops smart neighbourhood where residents own their data. Dezeen Magazine. https://www.dezeen.com/2019/03/05/smart-neighbourhood-brainport-smart-district-unstudio-netherlands/

Church, E. M., Thambusamy, R., & Nemati, H. (2017). Privacy and pleasure: A paradox of the hedonic use of computer-mediated social networks. *Computers in Human Behavior*, 77, 121–131. https://doi.org/10.1016/j.chb.2017.08.040

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology,* 23(6), 413-422.

Elvy, S. A. (2017). Paying for privacy and the personal data economy. *Columbia Law Review*, 117(6), 1369-1459.

Ford, R., & Peniamina, R. (2016). *Smart Homes: What New Zealanders think, have, and want.* Centre for Sustainability, University of Otago. https://ourarchive.otago.ac.nz/handle/10523/6641

Gurau, C., Ranchhod, A., & Gauzente, C. (2003). "To legislate or not to legislate": A comparative exploratory study of privacy/personalisation factors affecting French, UK and US Web sites. *Journal of Consumer Marketing,* 20(7), 652–664. https://doi.org/10.1108/07363760310506184

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior,* 68, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

IDC. (2019, Jan 3). IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors. https://www.idc.com/getdoc.jsp?containerId=prUS44596319

Jamal, A., Coughlan, J., & Kamal, M. (2013). Mining social network data for personalisation and privacy concerns: A case study of Facebook's Beacon. *International Journal of Business Information Systems,* 13(2), 173. https://doi.org/10.1504/IJBIS.2013.054334

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2).

Knote, R. (2019). Towards Solving the Personalization-Privacy Paradox for Smart Personal Assistants. *Hawaii International Conference on System Sciences (HICSS)*, Maui, HI, USA. https://www.alexandria.unisg.ch/255502/

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, 32(5), 987–994. https://doi.org/10.1016/j.tourman.2010.08.011

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336–355. JSTOR.

Mani, Z., & Chouk, I. (2017). Drivers of consumers' resistance to smart products. *Journal of Marketing Management*, 33(1–2), 76–97. https://doi.org/10.1080/0267257X.2016.1245212

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing,* 81(1), 36–58. https://doi.org/10.1509/jm.15.0497

Moore, B. (2018). IDC - Smart home device sales up with no sign of slowing. *IT Brief.* https://itbrief.co.nz/story/idc-smart-home-device-sales-no-sign-slowing

Mun, Y. Y., Jackson, J. D., Park, J. S., & Probst, J. C. (2006). Understanding information technology acceptance by individual professionals: Toward an integrative view. *Information & Management,* 43(3), 350-363.

Oomen, I., & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In Policies and research in identity management (pp. 121–138). Springer.

Phull, T. (n.d.). Our roadmap to the future of IoT. Vodafone Australia. Retrieved July 22, 2020, from https://www.vodafone.com.au/red-wire/internet-of-things-business-home-future

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research,* 6(2), 144-176.

The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things. (2019). *Consumers International and the Internet Society.* https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.

Appendix 1: Survey scale items

All items were measured on a scale from 1 = strongly agree to 5 = strongly disagree.

Perceived usefulness—5 items (Davis, 1989):
Using IoT devices enables (would enable) me to accomplish my tasks more quickly.
Using IoT devices improves (would improve) my productivity in my daily life.
Using IoT devices enhances (would enhance) my effectiveness in daily tasks.
Using IoT devices makes (would make) my life easier.
I find (would find) it useful to use IoT devices at home.

Perceived ease of use—6 items (Davis, 1989):
Learning to operate IoT devices is (would be) easy for me.
I find (would find) it easy to get IoT devices to do what I want them to do.
My interaction with IoT devices is (would be) clear and understandable.
I find (would find) IoT devices to be flexible to interact with.
It is (would be) easy for me to become skillful at using IoT devices.
I find (would find) IoT devices easy to use.

Subjective norm—2 items (Taylor and Todd, 1995; Venkatesh and Davis, 2000):
People who influence my behaviour think that I should use IoT devices.
People who are important to me think I should use IoT devices.

Trust—5 items (Jarvenpaa, Tractinsky, and Saarinen, 1999; Malhotra, Kim, and Agarwal, 2004):
IoT companies are (would be) trustworthy in handling my information.
IoT companies tell (would tell) the truth and fulfill promises related to the information provided by me.
I trust that IoT companies keep (would keep) my best interests in mind when dealing with my information.
IoT companies are in general predictable and consistent regarding the usage of my information.
IoT companies are always honest with customers when it comes to using information that I provide (would provide).

Privacy concern—5 items (Adhikari and Panda, 2018; Dinev and Hart, 2004):
I am (would be) concerned that my personal information gathered by IoT devices could be used for wrong purposes.
I am (would be) concerned that my personal information gathered by IoT devices could be accessed by unknown parties.
I usually think twice (would think twice) before providing my personal information gathered by IoT devices.
I feel IoT devices are (could be) collecting excessive personal information.
I am (would be) concerned that my personal information gathered by IoT devices could be used in a manner I am unaware of.

Intention to use—2 items (Venkatesh and Davis, 2000; Mun, Jackson, Park, and Probst, 2006):
I intend to use (or continue to use) IoT devices in the future.
I intend to use (or continue to use) IoT devices to improve my daily tasks.