Crime Science

RESEARCH

Open Access

What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices

John M. Blythe[1], Shane D. Johnson[1*] and Matthew Manning[2]

Abstract

The Internet of Things (IoT) is considered the next technological revolution. IoT devices include once everyday objects that are now internet connected, such as smart locks and smart fridges, but also new types of devices to include home assistants. However, while this increased interconnectivity brings considerable benefits, it can and does increase people's exposure to crime risk. This is particularly the case as most devices are developed without security in mind. One reason for this is that there is little incentive for manufacturers to make devices secure by design, and the costs of so doing do not encourage it. The principle aim of the current paper was to estimate the extent to which consumers are willing to pay for improved security in internet connected products. The second aim was to examine whether this is conditioned by their exposure to security-related information. Using an experimental design, and a contingent valuation method, we find that people are willing to pay for improved security and that for some devices, this increases if they are exposed to information about security prior to stating their willingness to pay. The implications of our findings for industry and the secure by design agenda are discussed.

Keywords: Internet of Things, Security, Willingness to pay, Priming

Introduction

The internet has transformed society, generating new opportunities for social interaction, business opportunities, and communication. Recently, manufacturers have taken advantage of the interconnectivity that the internet facilitates to produce electronic products that can send and receive data over the internet, and be controlled remotely. Such devices are collectively known as the Internet of Things (IoT) and include internet connected security cameras, thermostats, toys, and even fridges. Like the internet itself, such devices have the potential to improve our lives in a variety of ways. For instance, internet connected security cameras allow us to monitor our homes remotely, making them more secure. Internet connected thermostats allow us to control the temperature of our homes from anywhere on the planet, having the potential to conserve energy as well as increasing our comfort. The IoT is increasing in ubiquity and Wrap (2016) estimate that by 2020, the average UK household will have around 15 internet connected products.

While this increased interconnectivity brings considerable benefits, it can also increase our exposure to risk and opportunities for crime. In recent years, academics, policy makers and industry have taken a growing interest in the security of the consumer IoT (DCMS 2018). The primary reason for this is that these devices are typically shipped with inadequate security features and place the burden for securing them onto the consumer. In fact, studies have demonstrated that seven out of the ten most popular IoT devices have security vulnerabilities (Hewlett Packard Enterprise 2015) and that there are up to forty-three behaviours expected of consumers to protect these IoT devices across their lifecycle (Blythe et al. 2017).

*Correspondence: Shane.johnson@ucl.ac.uk
[1] Dawes Centre for Future Crime at UCL, University College London, London, UK
Full list of author information is available at the end of the article

More generally, the concerns noted above are well-founded as this kind of scenario has played out many times before. As Pease (1997) points out, market innovations—such as products and services—are generally introduced without those who manufacture or provide them giving due consideration to their crime and security implications (see also, Ekblom 1997). Unfortunately, these vulnerabilities *are* considered by those who might exploit them, which can lead to a "crime harvest". Examples of crime harvests include vehicle theft in the 1980s and 1990s (e.g. Laycock 2004) and mobile phone theft in the 1990s and 2010s (see, Whitehead and Farrell 2008). While these vulnerabilities may subsequently be addressed, victims will have already suffered the consequences of them before retrofitted (and possibly partial) solutions are implemented.

In the case of the IoT, reports of misuse have already begun to emerge. For example, devices without adequate security have been misused to launch attacks (discussed in more detail below) against major online services such as Netflix and Twitter (BBC News 2017) and have the potential to leak information regarding users' activities and habits. Furthermore, consumer safety is at risk as critical household services (such as heating, home security) can be (and are increasingly) Internet connected and thus, vulnerable to potential exploitation. Purchasing devices with greater security features will reduce consumers susceptibility to online risk, but there is a cost to manufacturing secure devices and no existing studies have evaluated empirically whether consumers are willing to pay for this. Given the associated costs, and an absence of legislation, at present manufacturers have little incentive to secure their products, which perhaps explains why many have been found to be insecure. Arguably, manufacturers will be less likely to produce secure devices unless they are required to do so, or they perceive a demand in the market. In this paper, we investigate the extent to which consumers care about security by estimating the extent to which: (i) they are willing to pay for the security of consumer IoT devices; (ii) their willingness to pay (WTP) is influenced by the level of improvement in security offered; and (iii) their WTP is influenced by exposure to security-related information. The rest of this paper is organised as follows. In the next section, we briefly review what is currently known about the security of the IoT, barriers to improving it, and existing research on consumers' WTP for online security. We then describe the methodology employed to estimate consumer WTP for security in the context of the IoT and present our findings. We conclude with a discussion of our results, their implications for the security of the IoT, and suggestions for further research.

Crime and the security of the IoT

Presently, one in ten adults are victims of cybercrime (Office for National Statistics 2017), a figure that is expected to rise as more products and services become Internet connected and criminals exploit the opportunities afforded by greater connectivity. Indeed, a range of consumer IoT devices have been shown to have vulnerabilities including smart toys, which allow attackers to eavesdrop on children's conversations (Which? 2017), smart locks which allow unauthorised access to people's homes (Ho et al. 2016), and smart TVs which are open to the potential spreading of misinformation (Bachy et al. 2015). Cyber criminals can exploit the vulnerabilities in these (and other) IoT devices to access, damage and destroy consumer data and hardware, and facilitate cybercrimes. The potential crimes that may be committed from consumer IoT are far ranging, with horizon scanning research with experts identifying crimes including blackmail, sex crimes and terrorism, to name a few (Tzezana 2016; for a systematic review, see Blythe and Johnson 2019).

Some of these may be crimes of the future but the IoT is already being exploited for malicious purposes. In 2016, the Mirai malware exploited Internet connected IP cameras and home routers by targeting devices that used default login credentials and infected them with the malware. These infected devices were then combined to form a 'botnet'—a network of compromised devices—and used to launch Distributed Denial of Service (DDoS) attacks against online services and other connected devices (BBC News 2017). In simple terms, DDoS attacks involve sending more requests to a server than it can cope with, rendering it inoperable. What made Mirai particularly interesting is that it was the first known example of consumer IoT devices being used in strategic attacks to cause disruption to online services. In 2017, "Reaper", an evolution of Mirai was discovered (TrendMicro 2018). This version uses known and available exploits to compromise devices instead of guessing their passwords. Whilst Reaper has not been used in any major attacks, it demonstrates how devices can be exploited by cybercriminals through the lack of adequate security in consumer IoT devices, and how quickly these attacks can evolve.

In response, there has been a recent push by governments and security experts to motivate manufacturers to build security into products at the point of manufacture (DCMS, 2018; Schneier, 2017). In the past, such appeals (see Karmen 1981)—which speak to issues of corporate responsibility—have been made in relation to automobiles and other products (Whitebread and Farrell 2008) and have in some cases been successful (e.g. Laycock 2004). However, providing greater security in devices can be a barrier to market for manufacturers as the incentive for being first to market is a key motivation, as well as, the cost-effectiveness of using existing software and delaying security until the final stages of product development (Sadler 2017). Furthermore, security is not considered a market differentiator as consumers do not currently prioritise security over the functionality and features of a product, and do not discriminate between good and bad security at the point of purchase (DCMS 2018). One reason for this is that existing well-documented IoT risks such as DDoS attacks impact upon third parties rather than the owners of IoT devices (Schneier 2017). However, at present there is little opportunity for consumers to consistently choose the most secure products as the security of devices is hard to discern based on the information provided to consumers (Blythe et al. 2019). Understanding the purchasing behaviour of consumers may therefore be key to incentivising manufacturers to take security more seriously.

Interestingly, consumers purchasing of IoT devices is not consistent with their attitudes and concerns towards the security and privacy of consumer IoT devices. Research has shown that 90% of consumers are worried about how their data is kept secure and the associated crime risks that may arise from this insecurity (The Economist Intelligence Unit 2018). Other research suggests that only 9% of consumers trust that their data is secure in the IoT, but 42% are not willing to disconnect due to the value afforded by it (Cisco 2017). This gap in attitude and behaviour is known as the privacy paradox—that people have concerns about their privacy but do little to protect it (Acquisti et al. 2015). Whilst consumers have a stated preference for greater security and privacy and such concerns are a well-documented barrier to IoT adoption (Accenture 2016; Bullguard 2016), at present it is difficult for consumers to differentiate between products that are more and less secure, and there is a lack of research on whether consumers are actually willing to pay for greater security in consumer IoT devices. Absent consumer demand, as discussed above, there is currently little to incentivise manufacturers to improve the security of the IoT devices they produce. As such, evidence concerning consumers WTP for improved security in the context of the IoT is clearly important and may provide that incentive, either alone or in conjunction with other market "levers".

WTP denotes the maximum amount of money a consumer is willing to pay to acquire a product or service (Kalish and Nelson 1991). WTP is a useful measure as it can inform future policies, tactical pricing, the development of new products (and services) and customer segmentation. In the security context, WTP allows researchers to estimate the highest price a consumer would be willing to pay for a product, service, or in the current context, greater inbuilt security or security services. Such information is useful for understanding what form or level of (government) intervention is needed to leverage manufacturers to take security more seriously. Previous research has shown that consumers are willing to pay to reduce crime in general (Cohen et al. 2004) and to improve online security in particular. For example, with respect to the latter, Nguyen et al. (2017) found users were willing to pay between $9 and $11 per month extra, as well as wait between 8 and 9 additional minutes, and forgo access to 21–29 per 100 emails, in exchange for more effective phishing detection that reduces the amount of spam and phishing emails they receive. Rowe and Wood (2013) explored whether consumers would pay for greater security provisions afforded by their Internet Service Provider to reduce their susceptibility to risks including identity theft and computer crashes. They found that on average they were willing to pay approximately $7.24/month for greater security, representing a 16% increase on average US Internet bills. This research suggests that consumers are willing to pay for greater security, however to our knowledge, this has not been assessed in the context of IoT devices. As WTP is a potential barrier to the *Secure by Design* agenda as it relates to consumer IoT, this is clearly an important issue.

In comparison to paying for security for computers, consumers may be less likely to pay for additional security for once everyday objects such as thermostats and watches that conventionally were not susceptible to online risks. Conversely, for IoT products that are linked to physical security (such as security cameras) or to safety critical services (such as thermostats), consumers may be willing to pay more. Research has shown that WTP judgements are context sensitive (Bettman et al. 1988) and therefore, in the current case, may differ by the class of IoT device concerned. The current study seeks to explore these issues by assessing WTP across a range of IoT devices.

Additionally, human behaviour is known to be influenced by environmental cues which can be manipulated (for example) through "priming". Priming is considered a largely unconscious process in which cues (such as colour, sensations and presence of positive or negative imagery) influence behaviour (Dolan 2010). In cybersecurity, research has shown that red (warning) and green (safe) colour primes in Wi-Fi selection leads users to choose more secure Wi-Fi networks (Turland et al. 2015). Priming individuals to expect phishing emails also increases their phishing detection (Parsons et al. 2015). Finally, research indicates that priming can reduce personal information disclosure (Acquisti et al. 2012; Grazioli 2004), although this finding is not always consistent (Junger et al. 2017). Understanding the role of priming at the point of purchase is important as it may lead individuals to be more willing to pay for more secure devices. As well as assessing consumer's WTP, we seek to explore whether this can be influenced by priming them with a security-related task.

The research described here was conducted as part of a larger study aimed at understanding consumer security and privacy preferences for different IoT products (see Blythe and Johnson 2018). The aims of the current paper are to address the following research questions. First, to what extent are consumers willing to pay for the security of different Internet connected products? Second, is WTP influenced by the percentage improvement in security afforded and third, is WTP influenced by exposure to security-related information? To test the hypotheses, we use data collected through an online survey that examined (amongst other things) consumers' WTP for improved security in IoT devices.

Method

Design

We examined participant's WTP for five different consumer IoT products, as follows: a Smart Thermostat, a Wi-Fi Router, a Smart Watch, a Smart TV and a Smart Security Camera. These particular types of IoT devices were selected for the following reasons. First, they are already commonly purchased. Second, they vary in terms of the types and sensitivity of data they collect and, if intercepted, might reveal about a person. And, third, because they vary in terms of the extent to which they are connected to actuators that can affect the environment.

To examine people's willingness to pay for security, we would ideally analyse their "revealed preferences" using data on actual sales. However, for scenarios that concern hypothetical (or future) situations, such as the one examined here, such data simply do not exist. Consequently, we employed a stated preference WTP measure, specifically contingent valuation. This approach is commonly used in studies of WTP (see, Cohen et al. 2004; Kling et al. 2012) and involves asking participants what they would be willing to pay for a particular good or service. The specific measure used here was adapted from Rowe et al. (2013), who asked organizations how much they would be willing to pay to improve the security effectiveness of their Information Technology systems by 10%. We modified the percentage improvement to either 50% or 90%. This allowed us to assess whether percentage improvement played a role in consumers' WTP estimates. We also tailored the security incidents discussed in the framing of the question to the IoT context in line with known consequences associated with breaches in IoT security (Schneier 2017). The cost of the products used was derived from the average cost of the ten most commonly sold products across four online UK retailers and was specific to the IoT product (Smart Thermostat (£180), Wi-Fi Router (£40), Smart Watch (£230), Smart TV (£500) and Smart Security Camera (£160).

An example instruction given to participants was as follows:

> *"If you were buying a Smart Watch which costs around £230, how much more would you be willing to pay for a 50% improvement in the security built into the product, as measured by the number of incidents (e.g. loss of your personal data, disruption to the functioning of your product, viruses on your product) you experience each year? Please answer numerically in pound sterling (£): _____________"*

Finally, participants were either asked to complete the WTP task before or after they completed another task (discussed below) that required them to think about security. In summary, we used a 5 (Type of IoT product: Smart Thermostat, Wi-Fi Router, Smart Watch, Smart TV and Smart Security Camera) × 2 (Percentage improvement in security afforded: 50%, 90%) × 2 (exposure to security-related task: pre, post) between-subjects design yielding 20 experimental conditions.

Participants

Participants were recruited from the online panel company "prolific.ac" and awarded £0.95 as reimbursement. They were eligible to take part if they: (i) were aged ≥ 18 years; and (ii) lived in the UK. 971 UK participants (484 female and 485 male) with a mean age of 40 years (SD = 16, range 18–85) took part.

In terms of education, 2% had no formal qualifications, 17% had secondary education (GCSE/O-levels or similar), 20% had post-secondary education or equivalent (e.g. A levels/High school diploma or similar), 12% had vocational qualifications or equivalent (e.g. Diploma or similar), 30% had an undergraduate degree (BA, BSc etc.), 15% had a master's degree (MA, MSc etc.) and 4% had a doctorate (PhD, MD).

Procedure

Before commencement of this study, full ethical approval was received from the Department for Security and Crime Science at University College London. All participants were recruited to the study via a link listed on the prolific platform where they were notified that they would receive a flat rate of £0.95 for participation in the study. Participants were first provided with information about the study and asked to provide consent to take part. They were then randomly allocated to one of the 20 conditions.

Table 1 Means (and standard deviations) of WTP by product type and exposure to security task in pounds sterling (£)

	Thermostat (£180)[a]	Wi-Fi router (£40)[a]	Smart watch (£230)[a]	Smart TV (£500)[a]	Security camera (£160)[a]
Pre-security task	38.86 (49.44, N = 98)	22.69 (17.73, N = 111)	70.12 (81.61, N = 83)	69.01 (54.99, N = 96)	52.68 (64.69, N = 105)
Post security task	62.07 (81.24, N = 96)	27.98 (19.39, N = 100)	76.24 (91.22, N = 91)	68.37 (62.22, N = 91)	78.22 (74.17, N = 82)
Overall	50.29 (67.83, n = 194)	25.20 (18.68, n = 211)	73.03 (86.45, n = 174)	68.82 (54.99, n = 187)	63.86 (69.81, n = 187)

[a] Cost of device

Participants were asked about their WTP for increased security for one IoT device, either before or after completing a task concerned with device security. For the security task, participants were provided with information about (existing) consumer labelling schemes they may be familiar with such as the traffic light system used for food products, and the energy efficiency labels used for electronic devices (see Blythe and Johnson 2018). They were then informed that we were interested in developing a similar label for Internet connected products based on what is important to consumers. Participants were asked to rank-order 17 attributes (e.g. whether software updates are automatic or not, the support period of the device, whether default passwords are used) in terms of what information they would like such a label to communicate to them prior to making purchasing decisions. For this and the WTP task, they were asked to do this for one particular product and were provided with a short description alongside that item. We chose not to explain the risks or benefits associated with each feature so as not to influence participant responses. The survey concluded with questions concerning participants' demographics (e.g. age, gender) and debriefing information.

Results

The aggregate mean WTP values are shown in Table 1. The mean values are significantly greater than zero in all cases. With the exception of Smart TVs, those who were asked about their WTP before completing the security rating task reported a lower WTP than those who were asked about their WTP after completing it. Overall, the raw mean WTP value was highest for the Smart Watch, followed by the Smart TV, Security Camera, Thermostat and Wi-Fi Router. In relative terms, however, participants were willing to pay the most for better security in Wi-Fi Routers (62.5% of the product price) and Security Cameras (40% of the product price), and the least for Smart Watches (32% of the product price), Thermostats (28% of the product price) and Smart TVs (14% of the product price).

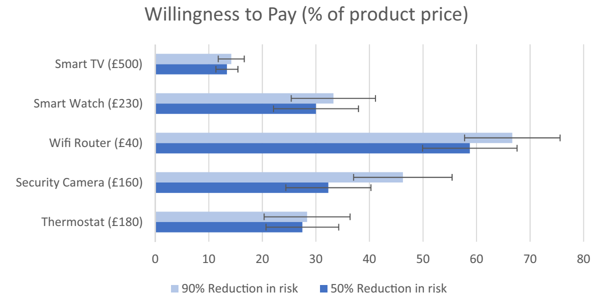

Fig. 1 Mean amount participants reported that they were willing to pay for different types of products and different levels of reduction in risk (cost of device shown in parentheses)

Figure 1 shows the mean amount that participants reported that they would be willing to pay to enjoy a (50% or 90%) reduction in cybercrime risk for each type of product as a percentage of the product price. This varies by product, and *prima facie* it appears that participants tended to be willing to pay more to enjoy a greater reduction in risk.

Prior to statistical analysis, we inspected the data and found that it was right skewed and hence transformed all values using a logarithmic transformation. We also removed outliers (identified as extreme values from boxplots[1]) from the dataset. A 2 (50% vs 90% reduction in risk) × 5 (product type) analysis of variance (ANOVA) of the log transformed data showed that there was a main effect of product type ($F(4,943) = 52.25$ $p < 0.001$), and a marginally non-significant main effect associated with the level of reduction in anticipated risk ($F(1,943) = 3.0$, $p < 0.10$). The interaction failed to reach statistical significance ($F(4,943) = 1.87$, $p > 0.10$).

However, the above analysis ignores the order in which participants completed the WTP and rating tasks. Figure 2 takes account of this. A 2 (50% vs 90% reduction in risk) × 5 (product type) × Order (WTP first vs WTP second) ANOVA of the log transformed data showed

[1] Eighteen participants provided WTP values of over £500 (£500–£100). These were extreme relative to the overall distribution of WTP values (being over 10 times the interquartile range above the third quartile of the data) and for the products for which they were provided. We suspect that these were typing errors and so excluded them. However, while the inclusion of these data affected the mean values for some products (Smart TVs and WiFi Routers) they did not affect the trends or (with the exception of one interaction) the outcomes of the statistical analyses. Analyses that include the outliers are reported in Appendix A.

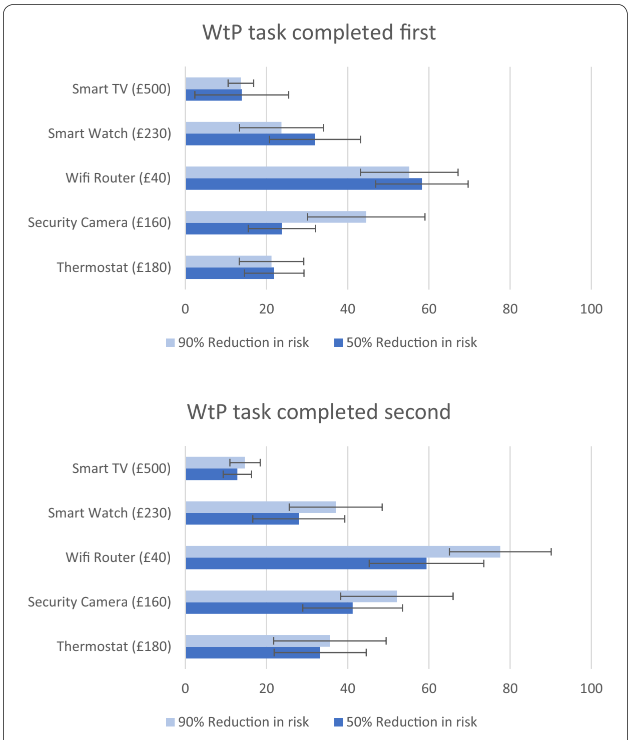

Fig. 2 Mean (prior to log transformation) amount participants reported that they were willing to pay for different types of products and different levels of reduction in risk as a function of the order that they completed tasks (cost of device shown in parentheses)

that there were significant main effects of product type (F(4,933) = 52.93, p < 0.001), the order in which participants completed the tasks (F(1,933) = 4.37, p < 0.05) and a non-significant main effect associated with the level of reduction in anticipated risk (F(1,933) = 2.42, p > 0.1). Considering the interaction terms, all were non-significant (ps > 0.1) except for one case. The exception was the interaction between product type and the order with which participants completed the tasks (F(4,933) = 2.53, p < 0.05). Thus, the amount participants' reported being willing to pay was largely influenced by the type of product under consideration, the order in which they completed the WTP and rating tasks, and the interaction between the two. Pair-wise follow-up tests of the estimated marginal means revealed that the interaction was largely due to the effect of order on participants' WTP for smart security cameras (F(1,933) = 7.85, p < 0.005). In all other cases, the differences observed were non-significant (p > 0.1).

Discussion

In this paper we aimed to assess the extent to which consumers are willing to pay for the security of different Internet connected products, whether their WTP is influenced by the percentage improvement in security afforded and their exposure to security-related information. The current data suggest that participants are willing to pay more for a secure device but the relative percentage in risk reduction offered did not significantly impact on WTP. Furthermore, we found that the simple presentation of security-related information (in this case a security task) may act as a nudge to encourage consumers to pay more for secure devices. In other words, the presence of security information may prime consumers and consequently influence their purchasing behaviour.

The current study thus supports existing research that has found that consumers are willing to pay more for secure services or products (Nguyen et al. 2017; Rowe and Wood 2013), in this case, internet connected devices. This suggests that there *is* an economic incentive for manufacturers to take this issue more seriously and to place greater priority on security during the product development cycle. Furthermore, recent work has demonstrated that the potential crime risks of the consumer IoT are wide ranging and include crimes such as burglaries, stalking and domestic violence (Blythe and Johnson 2019). Thus, whilst the current well-publicised security risks associated with the IoT, such as DDoS attacks, may represent an externality that does not affect consumers directly, in the near future, crimes facilitated by the IoT have the potential to do so. Reducing such risks represents an incentive for consumers to purchase secure devices over insecure ones and hence for manufacturers to ship products with better security by design. Moreover, although the WTP estimates presented in Table 1 may not appear particularly large, when expressed relative to their current cost (Figs. 1, 2), they are substantial. This was particularly evident for WiFi routers for which participants were prepared to pay an additional 63% for a secure product. That participants reported that they were willing to pay the most (in relative terms) for security for a router is perhaps unsurprising given that routers are the gateway to the home network and hence a first line of defence against cyber-attacks. Apropos the other devices, participants reported being willing to pay the least (in percentage terms) for the Smart TV. This might be explained by the fact that the other devices collect more sensitive or personal data (e.g. the smart watch and security camera) and control physical systems (the thermostat) that would be perceived as important to consumers. While our data do not allow us to test these hypotheses, the findings demonstrate the importance of considering the type of product in empirical work and any policy interventions.

To some extent, the effect of the security task is supported by existing work on nudging and cybersecurity behaviour more generally (Acquisti et al. 2012; Parsons et al. 2015; Turland et al. 2015). This has shown that the presentation of information (such as social proof, information about consequences) reduces the likelihood a user will follow the less protective choice, although none of these have explored consumer purchasing behaviour. Further research might explore the range of nudging and behaviour change techniques that can be employed (Dolan 2010; Michie et al. 2013) to influence consumers IoT purchasing behaviour. As governments are currently setting their policy agendas around consumer IoT, there have been a number of calls for a labelling scheme to inform consumer choice by governments (DCMS 2018), industry (Jamieson 2016) and academics (Blythe and Johnson 2018). These echo calls that have previously been made for electronic goods more generally from which lessons might be learned (see Armitage and Pease 2008). The current study has implications for this agenda as it suggests that priming individuals with security information (e.g. using a label) may influence their purchasing choices. Future research might look at this in greater depth by priming individuals with different types of labels or other forms of communication and assessing their effectiveness in nudging consumer purchasing behaviour.

The current study is, of course, not without its limitations. First is the fact that we used a contingent valuation approach to estimate WTP to explore consumers stated preferences. The reason for this is that access to data about actual purchasing behaviour (i.e. revealed preferences) are not available. There are some limitations associated with this approach. Research has suggested that consumers sometimes overestimate their WTP on contingent valuation questions (Loomis et al. 2011) which may mean that their WTP for security is slightly overestimated. Despite this, the current study is the first to explore WTP for the security of consumer IoT devices. Future research would benefit from using other methods to elicit WTP, such as discrete choice experiments, which allow a more nuanced understanding of how consumers make trade-offs in their decisions around the attributes of different products or services that are important to them (Tinelli 2016).

Studies might also look at consumers' revealed preferences by assessing the extent to which they actually purchase more secure devices over less secure ones. At present, such a study would be difficult since it is hard to systematically assess device security (see Blythe et al. 2019), and market data are hard to acquire. The former challenge, however, would be easier to address if devices were to feature a label that indicated if they were secure by design (or not).

Additionally, studies might consider what citizens are willing to pay to reduce the risk of IoT-based crime for wider society as well as themselves. Cohen et al. (2004) examined such a question in relation to urban crime by asking what participants would be willing to pay to reduce crime by ten percent in their community. Taking a similar approach in the context of the IoT may provide a more complete picture of the extent to which customers would be willing to pay to secure the consumer IoT.

A second limitation concerns our examination of the effect of different levels of risk reduction on willingness to pay. We asked participants to say what they would be willing to pay to enjoy a 50% or 90% reduction in risk, with the effect of this manipulation being tested using a between-subjects design. We find a trend whereby participants reported that they would be willing to pay more for greater reductions in risk, but this was not statistically significant. There are at least two explanations for this. First, our study may have been underpowered in statistical terms, meaning that we were unable to detect an effect reliably even though one existed. That there was a clear trend in the data speaks to the plausibility of this possibility.[2] Second, it may be the case that participants found it difficult to understand what a 50% (or 90%) increase in security meant as we did not provide details of the baseline level of risk (as this is unknown). If they perceived the risk to already be low, then they may be willing to pay to meaningfully reduce this further (e.g. by 50%), but less inclined to pay still more for further reductions. Future research might explore this in more detail using larger samples, using a within-subjects design (which would increase statistical power), looking at different levels of risk reduction (e.g. 10% versus 90%), or by providing participants with the baseline level of risk and examining the effect of varying this on their WTP.

In conclusion, the results of our study suggest that consumers are willing to pay more for secure IoT devices, but that this is not dependent on the level of risk reduction offered. Moreover, priming individuals with a security task appears to influence their WTP, and represents a promising approach to affect behaviour change in consumers. The findings thus have implications for the *Secure by Design* agenda for consumer IoT devices and suggest that manufacturers should take this issue more seriously.

Authors' contributions

JB and SDJ designed the study, collected and analysed the data and authored the article. MM advised on the study design and co-authored the paper. All authors read and approved the final manuscript.

[2] We avoid computing a post hoc power analysis here and note that it would have been difficult to conduct a power analysis ex ante, as doing so requires estimates of effect size and standard errors from previous studies, which simply do not exist.

Funding

This research was supported with funding from the Engineering and Physical Sciences Research Council (Award EP/N02334X/1) and the Dawes Centre for Future Crime at UCL.

Availability of data and materials

The data reported in the paper will be made available if the article is published.

Competing interests

The authors declare that they have no competing interests.

Author details

[1] Dawes Centre for Future Crime at UCL, University College London, London, UK. [2] ANU Centre for Social Research and Methods, The Australian National University, Canberra, Australia.

Appendix A

ANOVA results with outliers included

As noted in the main body of the text, we removed 18 data points from the analysis as they were clearly outliers. For transparency, Fig. 3 shows the same plot as Fig. 1 but for the data including the outliers. As would be expected—given the presence of outliers—the mean values and standard errors increased for some of the devices (Smart TV and WiFi Router). Below, we also report the ANOVA results with and without the outliers. As discussed in the main body of the text, aside from one interaction (which was of only minor interest), all trends were identical to those reported in the main text.

A 2 (50% vs 90% reduction in risk) × 5 (product type) analysis of variance (ANOVA) of the log transformed data showed that there was a main effect of product type (FULL DATA SET: $F(4,961)=42.68$, $p<0.001$; SUBSET WITHOUT OUTLIERS: $F(4,943)=52.25$ $p<0.001$), and a marginally non-significant main effect associated with the level of reduction in anticipated risk (FULL DATA SET: $F(1,963)=3.10$, $p<0.10$; SUBSET WITHOUT OUTLIERS: $F(1, 943)=3.0$, $p<0.10$). The interaction failed to reach statistical significance (FULL DATA SET: $F(4,963)=1.73$, $p>0.10$; SUBSET WITHOUT OUTLIERS: $F(4,943)=1.87$, $p>0.10$).

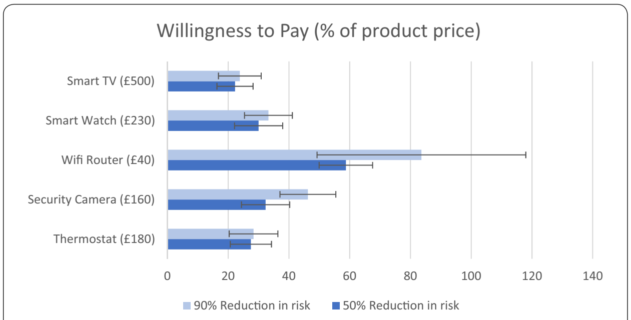

Fig. 3 Mean amount participants reported that they were willing to pay for different types of products and different levels of reduction in risk (cost of device shown in parentheses)

However, the above analysis ignores the order in which participants completed the WTP and rating tasks. A 2 (50% vs 90% reduction in risk) × 5 (product type) × Order (WTP first vs WTP second) ANOVA of the log transformed data showed that there were significant main effects of product type (FULL DATA SET: $F(4,951)=42.94$, $p<0.001$; SUBSET WITHOUT OUTLIERS: $F(4,933)=52.93$, $p<0.001$), the order in which participants completed the tasks (FULL DATA SET: $F(1,951)=7.38$, $p<0.01$; SUBSET WITHOUT OUTLIERS: $F(1,933)=4.37$, $p<0.05$) and a non-significant main effect associated with the level of reduction in anticipated risk (FULL DATA SET: $F(1,951)=2.39$, $p>0.1$; SUBSET WITHOUT OUTLIERS: $F(1,933)=2.42$, $p>0.1$). Considering the interaction terms, all were non-significant ($ps>0.1$) except for one case for the subset of data that excluded the outliers. The exception was the interaction between product type and the order with which participants completed the tasks (FULL DATA SET: $F(4,951)=1.6$, $p>0.1$; SUBSET WITHOUT OUTLIERS: $F(4, 933)=2.53$, $p<0.05$). Thus, the amount participants' reported being willing to pay was largely influenced by the type of product under consideration, the order in which they completed the WTP and rating tasks, and (for the subset of data excluding outliers) the interaction between the two. Pair-wise follow-up tests of the estimated marginal means revealed that the interaction was largely due to the effect of order on participants' WTP for smart security cameras (FULL DATA SET: $F(1,951)=9.73$, $p<0.005$; SUBSET WITHOUT OUTLIERS: $F(1,933)=7.85$, $p<0.005$). As can be seen, despite the interaction term failing to reach statistical significance for the full set of data, the results of the follow-up tests were identical. In all other cases, the differences observed were non-significant for both the full set of data and that which excluded the outliers ($p>0.1$).

Received: 22 December 2018 Accepted: 19 December 2019
Published online: 08 January 2020

References

Accenture. (2016). *Igniting growth in consumer technology* (pp. 1–15).

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–515. https://doi.org/10.2139/ssrn.2580411.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research, 49*(2), 160–174. https://doi.org/10.1509/jmr.09.0215.

Armitage, R., & Pease, K. (2008). Predicting and preventing the theft of electronic products. *European Journal on Criminal Policy and Research, 14*(1), 11–37.

Bachy, Y., Basse, F., Nicomette, V., Alata, E., Kaaniche, M., Courrege, J. C., & Lukjanenko, P. (2015). Smart-TV security analysis: practical experiments. In *Proceedings of the 45th annual IEEE/IFIP international conference on dependable systems and networks smart-TV* (pp. 497–504). https://doi.org/10.1109/DSN.2015.41.

BBC News. (2017). Mirai botnet: Three admit creating and running attack tool. Retrieved from http://www.bbc.co.uk/news/technology-42342221.

Bettman, J. R., Luce, M. F., & Payne, J. W. (1988). Constructive consumer choice processes. *Journal of Consumer Research, 25*(3), 187–217.

Blythe, J. M., & Johnson, S. D. (2018). The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. In *Proceedings of the living in the internet of things: Cybersecurity of the IoT conference*.

Blythe, J. M., & Johnson, S. D. (2019). A systematic review of crime facilitated through consumer IoT devices. *Journal of Experimental Criminology, 15,* 1–29.

Blythe, J. M., Michie, S., Watson, J., & Lefevre, C. E. (2017). Internet of Things in Healthcare: Identifying key malicious threats, end-user protective and problematic behaviours. *Frontiers in Public Health*. https://doi.org/10.3389/conf.FPUBH.2017.03.00021.

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

Bullguard. (2016). Despite fast adoption of Internet of Things, a shocking 72 per cent of consumers don't know how to secure their connected devices. Retrieved from http://www.bullguard.com/press/latest-press-releases/2016/03-17.aspx.

Cisco. (2017). *The IoT Value/Trust Paradox*.

Cohen, M. A., Rust, R. T., Steen, S., & Tidd, S. T. (2004). Willingness-to-pay for crime control programs. *Criminology, 42*(1), 89–110.

DCMS. (2018). *Secure by design: Improving the cyber security of consumer Internet of Things report*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

Dolan, P. (2010). Influencing the financial behaviour of individuals: The mindspace way. In A. Oliver (Ed.), *Behavioural Public Policy* (pp. 191–215). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781107337190.009.

Ekblom, P. (1997). Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk, Security and Crime Prevention., 2*(4), 249–265.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the internet. *Group Decision and Negotiation, 13*(2), 149–172. https://doi.org/10.1023/B:GRUP.0000021839.04093.5d.

Hewlett Packard Enterprise. (2015). *Internet of Things Research Study 2015 Report*. Retrieved from http://fortifyprotect.com/HP_IoT_Research_Study.pdf.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security* (pp. 461–472). https://doi.org/10.1145/2897845.2897886.

Jamieson, A. (2016). *IoT Security—It's in the Stars!* Retrieved from https://www.slideshare.net/AndrewRJamieson/iot-security-its-in-the-stars-169-v201605241355.

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66,* 75–87. https://doi.org/10.1016/j.chb.2016.09.012.

Kalish, S., & Nelson, P. (1991). A comparison of ranking, rating and reservation price measurement in conjoint analysis. *Marketing Letters, 2*(4), 327–335.

Karmen, A. A. (1981). Auto Theft and Corporate Responsibility. *Comtemporary Crises*, *5*, 63–81.

Kling, C. L., Phaneuf, D. J., & Zhao, J. (2012). From Exxon to BP: Has some number become better than no number? *Journal of Economic Perspectives, 26,* 3–26.

Laycock, G. (2004). The UK car theft index: An example of government leverage. In *Crime Prevention Studies 17* (pp. 25–44). Cullomptun, Devon: Willan.

Loomis, J. B., González-Cabán, A., & Chami, J. (2011). Testing the roubstness of contingent valuation estimates of WTP to survey mode and treatment of protest responses. In *The international handook on non-market environmental evaluation* (pp. 102–121).

Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., et al. (2013). The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: Building an international consensus for the reporting of behavior change interventions. *Annals of Behavioral Medicine, 46*(1), 81–95. https://doi.org/10.1007/s12160-013-9486-6.

Nguyen, K. D., Rosoff, H., & John, R. S. (2017). Valuing information security from a phishing attack. *Journal of Cybersecurity, 3*(3), 159–171. https://doi.org/10.1093/cybsec/tyx006.

Office for National Statistics. (2017). *Crime survey for England and Wales*. London: Office for National Statistics.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*. https://doi.org/10.1016/j.cose.2015.02.008.

Pease, K. (1997). Crime reduction. In M. Maguire, et al. (Eds.), *The oxford handbook of criminology* (2nd ed.). Oxford: Clarendon Press.

Rowe, B., Pokryshevskiy, I. D., Link, A. N., & Reeves, D. S. (2013). *Economic analysis of an inadequate cyber security technical infrastructure*. Gaithersburg: National Institute of Standards and Technology.

Rowe, B., & Wood, D. (2013). Are home internet users willing to pay ISPs for improvements in cyber security? In B. Rowe (Ed.), *Economics of information security and privacy III* (pp. 193–212). New York, NY: Springer.

Sadler, M. (2017). Securing our connected world. Retrieved from https://dcmsblog.uk/2017/10/securing-connected-world/.

Schneier, B. (2017). Click here to kill everyone. Retrieved from http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html.

The Economist Intelligence Unit. (2018). *What the Internet of Things means for consumer privacy*.

Tinelli, M. (2016). Applying discrete choice experiments in social care research. *Methods Review, 16,* 12.

TrendMicro. (2018). New rapidly-growing IoT Botnet—REAPER.

Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015). Nudging towards security: Developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI conference on—British HCI'15* (pp. 193–201). New York, New York, USA: ACM Press. https://doi.org/10.1145/2783446.2783588.

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research, 4*(1), 18. https://doi.org/10.1007/s40309-016-0107-z.

Which? (2017). Safety alert: see how easy it is for almost anyone to hack your child's connected toys. Retrieved from https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/.

Whitehead, S., & Farrell, G. (2008). Anticipating Mobile Phone 'Smart Wallet'Crime: Policing and Corporate Social Responsibility. *Policing: A Journal of Policy and Practice*, *2*(2), 210–217.

Wrap (2016). Smart Devices and Secure Data Eradication. Last accessed Nov 2019. http://www.wrap.org.uk/sites/files/wrap/Data%20Eradication%20report%20Defra.pdf.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.