Privacy in the Internet-of-Things: Perceptions and Behaviour

Meredydd Williams
Department of Computer Science
University of Oxford
Oxford, United Kingdom
meredydd.williams@cs.ox.ac.uk

Jason R. C. Nurse
Department of Computer Science
University of Oxford
Oxford, United Kingdom
jason.nurse@cs.ox.ac.uk

Sadie Creese
Department of Computer Science
University of Oxford
Oxford, United Kingdom
sadie.creese@cs.ox.ac.uk

Abstract

Through opinion polls and surveys, the public appear to value their privacy. However, they are often judged to act to the contrary when using technology. This disparity between opinions and actions has been labelled the ‘Privacy Paradox’. While the Internet-of-Things (IoT) offers many benefits, it can also place privacy at risk. Through our continued research, we explore the influence of the IoT on the Privacy Paradox. In this article, we discuss our recent and ongoing work. We first present our privacy opinion survey [N = 170], conducted with the general public. Through it, we found IoT products were considered less private, familiar and usable, with this potentially constraining protective behaviour. We move on to describe our public interviews [N = 40], where we compare privacy opinions and actions. We found the Paradox is significantly more prevalent in the IoT, particularly on wearable devices. Attempting to mitigate this issue, we finally describe our prototype smartwatch games. These apps will comprise one component of training sessions, in which we seek to incentivise privacy protection.

Author Keywords

Privacy; Internet-of-Things; behaviour change

ACM Classification Keywords

H.5.m [Information inferences and presentation (e.g., HCI)]: Miscellaneous; K.4.1 [Public policy issues]: Privacy

#	Question
1	How usable would you rate this technology?
2	How familiar are you with this technology?
3	How much does this technology respect your privacy?
4	How useful would you rate this technology?
5	Do you own this technology?
6	Why do/don't you own this technology?

Table 1: Survey questions

Demographic	%
Male	57
Female	43
18-25	26
26-35	50
36-45	14
46-55	6
56-65	3
66+	1
GCSE	4
A-Level	15
Degree	38
Masters	36
PhD	7

Table 2: Survey demographics

Introduction and Background

Through a range of opinion polls and surveys, the public claim to value privacy. A 2015 Pew Research Center study [6] found 93% of respondents wanted to control access to their data. The response to the Snowden Revelations also suggested that citizens value this principle. However, when interacting with modern technology, individuals often act to the contrary. Carrascal et al. [2] assessed privacy through an auction scenario, finding participants would sell their browsing history for only €7. Williams et al. [13] compared privacy opinions with disclosure behaviour. They found while 92% reportedly valued the principle, 99% divulged information needlessly. Although people claim to appreciate privacy, their behaviour often appears misaligned.

This apparent disparity between opinion and action is known as the 'Privacy Paradox'. Acquisti and Gross [1] conducted a social network study, comparing stated attitudes with actual behaviour. They found even those with concerns would join Facebook and share their data. Woodruff et al. [15] surveyed 884 people, exploring the relationship between privacy attitudes and intent. They found no correlation and suggested this might imply an 'attitude-consequence dichotomy'. As technology continues to proliferate, this disparity might place user privacy at risk.

The Internet-of-Things (IoT) refers to the growing agglomeration of connected devices. These technologies pervade our environments, blurring the physical and the virtual. The IoT offers many benefits to our society, from smart-grids to patient-led healthcare. However, these exciting devices can also pose a threat to privacy. Products suffuse the environments around us, enabling surreptitious data collection. Displays are often constrained [7], contributing to interfaces which deviate from mental models [5]. As the IoT continues to grow, user privacy might be placed under threat.

In our continued research, we posit that the Internet-of-Things will exacerbate the Privacy Paradox. We believe the IoT aggravates many of those factors which contribute to the disparity [14]. The relationship between IoT challenges and contributory factors is summarised in Figure 1. For example, smart devices are frequently novel and heterogeneous. Individuals who lack experience of products are more likely to make costly errors. Therefore, IoT unfamiliarity could lead users to neglect their privacy [14].

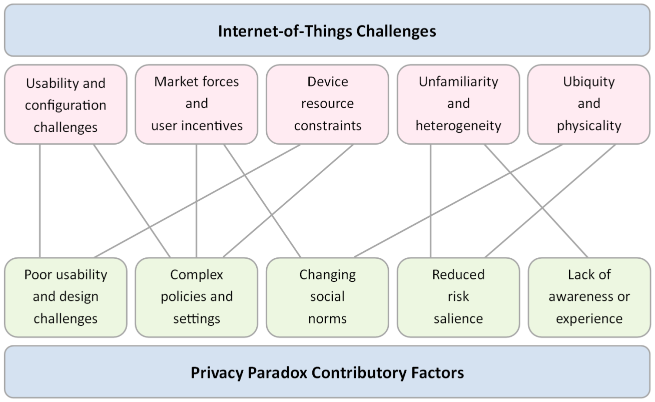

Internet-of-Things Challenges
Usability and configuration challenges
Market forces and user incentives
Device resource constraints
Unfamiliarity and heterogeneity
Ubiquity and physicality
Poor usability and design challenges
Complex policies and settings
Changing social norms
Reduced risk salience
Lack of awareness or experience
Privacy Paradox Contributory Factors

Figure 1: IoT challenges in relation to the Privacy Paradox [14]

In this work, we outline our ongoing research on the privacy implications of novel technologies. First, we describe our online privacy survey with the general public. The questions and demographics from this study can be found in Tables 1 and 2, respectively. We move on to highlight our contextualised interviews, where privacy discussions were grounded around participants' devices. Through these conversations, we were able to compare non-expert concerns with actions. Finally, we describe our new smartwatch games, which seek to improve the privacy behaviour of wearable users.

T	Question
O	How would you feel if someone deleted your device's data without your consent? Why?
O	How would you feel if someone shared your device's data without your consent? Why?
O	How would you feel if someone monitored everything you do on your device? Why?
O	How would you feel if someone sold your device's data without your consent? Why?
A	Does your device allow you to set a password? Have you set a password? Why?
A	How much time have you spent reading your device's privacy policies? Why?
A	How much time have you spent configuring your device's privacy settings? Why?

Table 3: Interview questions: Type (T) - Opinion (O) or Action (A)

Privacy Opinion Survey

We were interested in the privacy perceptions of the public. To explore IoT influence, we compared opinions of smart devices with those of less-novel technologies. First, we categorised gadgets based on novelty, ubiquity and autonomy. Through this, we selected (*wearables*, *smart appliances*, *smart home*) for IoT and (*desktops*, *laptops*, *tablets*) for non-IoT. While products do not exist in a strict dichotomy, research firms agree with this division [4, 9]. In future work, we seek to explore how users categorise devices.

We conducted an online survey with 170 members of the public (demographics in Table 2). These participants were recruited through both Twitter and online ad boards (e.g., GumTree). As shown above in Table 1, respondents rated devices based on four factors: privacy, usability, familiarity and utility. The non-privacy factors were selected both to disguise the topic and for their greater interest to the study. We also asked participants whether they owned the product, and required a qualitative justification for their decision.

In our results, we found IoT products were considered significantly less privacy-respecting ($p < 0.001$), particularly wearables. IoT devices were also rated less usable ($p < 0.001$) and familiar ($p < 0.001$), suggesting private actions might be constrained [5]. Although smart devices were considered a privacy risk, this was rarely given as a rejection justification. Price was mentioned four times as often, implying popularity might increase as the market matures. We then considered privacy opinions alongside purchasing actions. 8.91% bought non-IoT products despite perceiving a risk, compared to 14.96% for smart devices. While the difference was not significant ($p = 0.056$), the low p-value might suggest our sample was too small. With the IoT both considered less usable and less familiar, we were curious whether constrained action leads to misaligned behaviour.

Contextualised Interviews

To explore the relationship between privacy concerns and actions, we required qualitative data. Therefore, we designed a series of contextualised interviews. In these discussions, we grounded opinion and action questions around each participant's device. Rather than comparing abstract concepts to practical behaviour, individuals could draw on their own experiences. Questions are found in Table 3, with interview findings (Figure 2) described on the next page.

We sought to overcome the criticisms of previous Privacy Paradox work [12]. Rather than considering the nebulous concept of 'privacy', discussions were contextualised around a specific device. We also solicited reactions to defined violations, drawn from Solove's taxonomy [11]. Instead of using student-composed samples, we conducted interviews with a non-expert public. Finally, our actions were selected based on simplicity, utility and applicability. We believe this enabled a fair comparison between opinion and action.

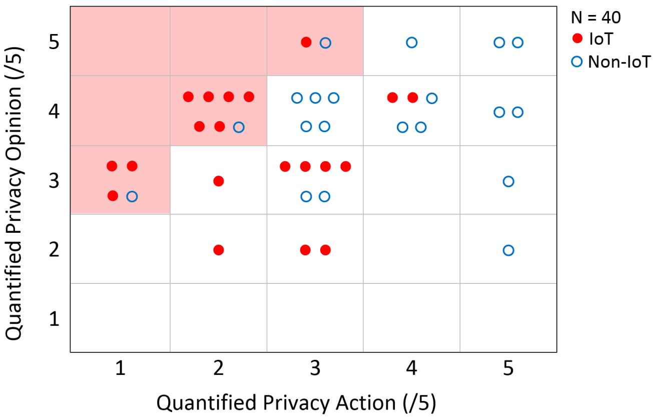


Figure 2: Interview participant opinion-action distribution. Red highlights a disparity between privacy opinions and actions.

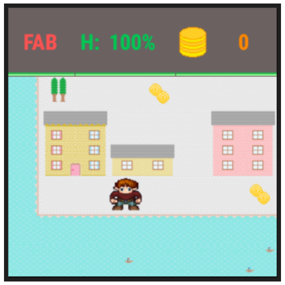
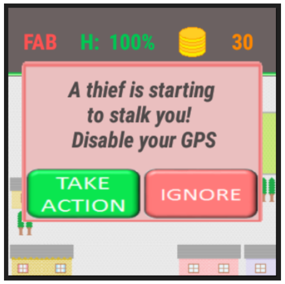
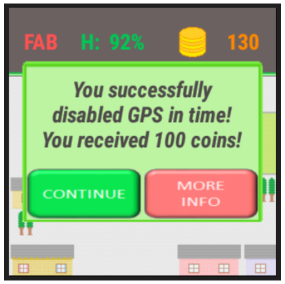


Figure 3: Smartwatch game: Main gameplay screen



A thief is starting to stalk you! Disable your GPS

Figure 4: Smartwatch game: GPS privacy task screen



You successfully disabled GPS in time! You received 100 coins!

Figure 5: Smartwatch game: Task success screen

We interviewed the public [N = 40], with participants recruited from city ad boards. 20 had IoT products (as defined earlier), while 20 owned less-novel technologies. We performed thematic analysis before translating our codes to a 1-5 quantitative scale. We found IoT owners cared significantly-less about their privacy (p = 0.049), with this often blamed on ephemeral data. Smart device users also took significantly-less action to protect themselves ($p <$ 0.001), with this justified by a lack of awareness. To explore the Paradox, we compared each participant's opinions and actions. 33% displayed a disparity, with the phenomenon significantly-more prevalent in the IoT (p = 0.041). Wearables were found most prone, contributing to 54% of the issues. The distribution of opinions/actions is presented above in Figure 2. As shown, many individuals expressed privacy concerns in excess of their protective actions.

Smartwatch Educational Game

With wearables appearing to contribute to the Paradox, we are exploring approaches to realign perceptions and behaviour. In qualitative comments, a lack of awareness was cited as the main justification. If users do not know how to protect themselves, they will continue to place their privacy at risk. To encourage private wearable behaviour, we are developing smartwatch games, as shown right in Figure 6.

Interactive games have been found more influential for behaviour than instructor-led sessions [8]. Furthermore, while public campaigns can raise awareness, individuals must be incentivised to change their actions. Previous games, such as Anti-Phishing Phil, have successfully influenced user behaviour [10]. By rewarding privacy-conscious actions, our app might encourage improved conduct. The game has been designed through learning science principles, such as reflection. Users reflect on privacy lessons after each task, with this found to increase retention [3].

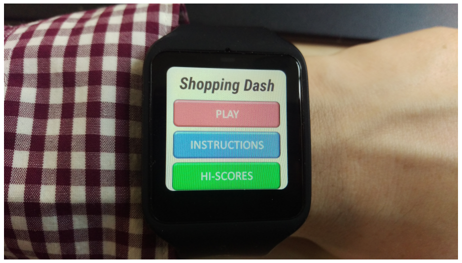


Figure 6: Smartwatch game: Shopping Dash

In our Android Wear and WatchOS prototypes, dubbed *Shopping Dash*, users navigate their character around a town (Figure 3). They receive points for collecting coins and occasionally encounter a privacy task. This task might include disabling GPS (Figure 4) or restricting app permissions. If the user is incorrect or too slow, their health depletes and the game ends. If they succeed, they receive points and continue their journey to the shop (Figure 5). By using an accessible gameplay scenario, we hope to both highlight and encourage smartwatch privacy.

Next Steps

In future research, we plan to evaluate the influence of our games. The apps are intended to comprise just one part of a comprehensive training approach. Individuals would first be instructed on wearable risks and how to protect their privacy. They would be shown device settings and the content of common privacy policies. They would then play the smartwatch games to both test and reinforce their learning. Through a pretest-posttest design, we could compare their behaviour before and after the session. Following a longitudinal approach, their actions could be further evaluated one month later. If participants continue to act in a private manner, then the session might be influential. Such efforts are crucial for privacy as the IoT continues to expand.

REFERENCES

1. A Acquisti and R Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies in Lecture Notes in Computer Science* 4258 (2006), 36–58.

2. J P Carrascal, C Riederer, V Erramilli, M Cherubini, and R de Oliveira. 2013. Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd International Conference on World Wide Web*. 189–200.

3. M S Donovan, J D Bransford, and J W Pellegrino. 1999. *How people learn: Bridging research and practice*. National Academies Press.

4. J Duffy. 2014. 8 Internet things that are not IoT. (2014). `www.networkworld.com/article/2378581/internet-of-things/8-internet-things-that-are-not-iot.html`

5. C Hochleitner, C Graf, D Unger, and M Tscheligi. 2012. Making devices trustworthy: Security and trust feedback in the Internet of Things. In *Proceedings of Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use*.

6. M Madden and L Rainie. 2015. Americans' attitudes about privacy, security and surveillance. *Pew Research Center* (2015).

7. D Miorandi, S Sicari, F De Pellegrini, and I Chlamtac. 2012. Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks* 10, 7 (2012), 1497–1516.

8. A Nagarajan, J M Allbeck, and A Sood. 2012. Exploring game design for cybersecurity training. In *Proceedings of the 2012 International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*. 256–262.

9. J Rivera and R van der Meulen. 2013. Gartner says the Internet of Things installed base will grow to 26 billion units by 2020. (2013). `http://www.gartner.com/newsroom/id/2636073`

10. S Sheng, B Magnien, and P Kumaraguru. 2007. Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the Third Symposium on Usable Privacy and Security*. 88–99.

11. D J Solove. 2008. *Understanding privacy*. Harvard University Press.

12. S Trepte, T Dienlin, and L Reinecke. 2014. Risky behaviors: How online experiences influence privacy behaviors. In *From the Gutenberg Galaxy to the Google Galaxy*. 225–244.

13. M Williams and J R C Nurse. 2016. Optional data disclosure and the online privacy paradox: A UK perspective. *Human Aspects of Information Security, Privacy, and Trust in Lecture Notes in Computer Science* 9750 (2016), 186–197.

14. M Williams, J R C Nurse, and S Creese. 2016. The perfect storm: The privacy paradox and the Internet-of-Things. In *Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 644–652.

15. A Woodruff, V Pihur, and S Consolvo. 2014. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *Proceedings of the Tenth Symposium on Usable Privacy and Security*.