How to Ensure Users Have Awareness and Control of the Collection, Storage and Processing of their Personal Data within IoT Systems – Project Report

By

Bradley Clemson
160946

Supervisor: Dr Paul Grace

A Dissertation
Submitted to the Department of Computer Science
Aston University
In Partial Fulfilment of the Requirements
for the Degree of Master of Computer Science
September 2020

Project Summary

Internet of Things (IoT) devices create new ways through which personal data is collected and processed. As such, end users frequently have little awareness of, and even less control over, their personal data collection, storage and processing. Given privacy behaviours of individuals are often inconsistent with their stated attitudes (a phenomenon known as the “privacy paradox”), the challenges of managing privacy choices in the IoT, will aggravate these inconsistencies and potentially lead to troublesome or regrettable experiences. To help people address these privacy inconsistencies, this project proposes a conceptual architectural model and mock-up prototype design of a privacy awareness and control interface for the IoT. Its personalised privacy notification approach juxtaposes users’ general privacy attitudes towards IoT technologies and the privacy riskiness of particular nearby IoT resources. The system notifies users of the existence of nearby IoT sensors and, by highlighting any privacy discrepancies, nudges users toward making decisions to control their privacy in alignment with their privacy attitudes. Although the infrastructure of “IoTAware” intends to be applicable to a wide range of IoT scenarios that involve notifying users of nearby IoT sensors, the solution is envisaged in a setting of IoT cameras using facial recognition technology. This paper provides an overall evaluation of the solution, primarily through a user study carried out as two online experiments. The findings suggest that the privacy discrepancy approach is effective at nudging users to behave in line with their privacy attitudes in the IoT.

Acknowledgements

On the very outset of this report. I would like to extend my sincere gratitude to Dr Paul Grace for his constant guidance, feedback and encouragement for me throughout this project, particularly amidst an unprecedented six-month period given the ongoing COVID-19 pandemic. In particular, Dr Grace was able to, on multiple occasions, guide me in the correct direction with regards to conducting a thorough literature review to justify my motivation for the objectives of this project. I would also like to thank Dr Sylvia Wong for her inaugural guidance to the assessment, structure and ethics of my project. At last but not least, I extend my gratitude towards all my family, friends and classmates who have supported me in completing this project.

Table of Contents

1 Introduction

Previous research has revealed that individual's actual behaviours occasionally divert from their stated privacy attitudes, a phenomenon known as the privacy paradox (Spiekermann, Grossklags and Berendt, 2001). Privacy attitudes represent individual's views of what aspects of their privacy they consider important and/or how their privacy should be protected, whereas privacy behaviours denote their actual actions that might impact their privacy. The privacy paradox occurs in privacy-related circumstances where user intentions and user behaviours are contradictory. In turn, these inconsistencies may lead to troublesome or regrettable experiences. For instance, although people often state concerns about disclosing their personal information to companies, they share their personal information when creating accounts in online shopping sites to receive small discounts. All while not realising the potential harmful ramifications (e.g., being profiled and/or their data being shared or sold to third parties).

As everyday objects with computational abilities become internet-connected, they form an "Internet of Things" (IoT). From digital cameras to smart watches, the lack of disclosure to consumers about device capabilities and data practices (Yurieff, 2019) makes the IoT very fertile grounds for privacy invasions (IoT for All, 2017). Without adequate user controls nor the existence of notice and consent mechanisms, IoT devices are likely to contribute toward people's inadvertent disclosure of personal data. This paper focuses on addressing the privacy paradox in the attendance of IoT cameras with facial recognition technology. This is because of the increasing widespread implementation of facial recognition technology in public and commercial places (Dormehl, 2014). Reports claim that 30% of general shops and 59% of fashion retail stores on the UK high street are using cameras connected to the internet to covertly gather people's personal biometric data (Frey, 2017). This increasing use of covert facial recognition is concerning in terms of liberty and privacy. However, current applications of facial recognition technology in the IoT lack sufficient/effective mechanisms for notifying users of not only the existence of cameras but also informing and allowing users control of the collection, storage and processing of their personal data. This paper's proposed system, in the facial recognition domain, hopes to lead to giving users better awareness and control of the collection, storage and processing of their personal data within IoT systems.

The aim of this project is to answer the research question: *How to ensure users have awareness and control of the collection, storage and processing of personal data within IoT systems?* Objectives to achieve this desired outcome include:

- To accurately and efficiently measuring the privacy risk of IoT devices
- To precisely measure individual user's underlying privacy attitudes in the IoT context.
- To influence informed decision making, highlighting any discrepancy between a user's privacy attitudes and the privacy risk of an IoT device.
- To allow users to control their privacy in IoT systems.

These outcomes will be evaluated based on this paper's four main contributions, including:

- A reusable method for measuring the underlying privacy attitudes and decision processes of individuals in the IoT context.
- A reusable framework for measuring the privacy riskiness of IoT devices.
- A prototype user interface of the IoTAware app which notifies users of the existence of nearby IoT sensors (facial recognition cameras) and nudges users toward making decisions to control their privacy in line with their privacy attitudes.
- To demonstrate the effectiveness of the solution in an application domain.

2 Background Description of the Problem

2.1 Privacy Challenges in the IoT

The IoT has been described as a revolutionary technology (Vasseur and Dunkels, 2010), connecting together vast numbers of ubiquitous devices and sensors which collect and process data. As such, the IoT offers a wealth of opportunities for productivity and new ways to capture revenue and subsequently is predicted to generate trillions of dollars for the global economy (Manyika, 2015). Proliferation of the IoT is gaining momentum, with the number of connected IoT devices predicted to reach 55 billion products by 2025 (Newman, 2020), this indicates the growing scale of IoT data collection and the influence IoT will bring on our societies. However, the open internet-centred infrastructure on which the IoT is based and the pursuit of identification and personalisation of IoT users is seen as a major privacy concern (Misra, Maheswaran and Hashmi, 2017; Ziegeldorf, Morchon and Wehrle, 2014; Gessner et al. 2012). This is for a number of reasons.

Firstly, generally, if device monitoring is noticed, then users have an opportunity to restrict it. However, data collection, storage and sharing among IoT devices is often invisible and surreptitious. For example, the Amazon Echo has raised concerns that our home environments are being monitored (Moye, 2018) and Smart TV's have been discovered to listen to conversations, before sending transcripts to remote locations (Gibbs, 2015). With constrained user interfaces obstructing device configuration, IoT devices and sensors tend to exclude a user's intervention and control of their personal data. This is detrimental given the different privacy sensitivities of users. For instance, between 1978 and 2004 Dr. Alan Westin conducted a set of surveys measuring individual's attitudes and concerns around protection and control of their personal data. The results (Kumaraguru and Cranor, 2005) show altering perceptions between 1990 and 2000. Concern about privacy among the public grew with 88% of the public registering Medium to High consumer privacy concerns. However, over the same period, distrust of organisations handling of personal data did not increase, instead, by 2000 a larger majority of the public believed that organisations should earn the public's trust with the procedures they follow for using personal data. Ultimately, regardless of their privacy concerns, users are often made oblivious to when products are actually active, therefore, even those users who admittedly value their privacy can do little when they are unaware to pervasive monitoring.

Secondly, due to the smaller size and mobility of some IoT devices, such as smartwatches, there is little space for extensive storage and operations are constrained. Subsequently, together with 5G architecture, IoT applications demand response-latency beyond centralised computations. Instead, a complementary paradigm to the cloud used by IoT devices is edge/fog computing and the decentralisation of the cloud into multiple smaller scale computing devices, or cloudlets. However, with this decentralised approach, computing infrastructure can be distributed to billions of storage and computation spots, operated by anyone who can innovate on it (Psaras, 2018). Consequently, this distributed computing between trust-less nodes is an enabler for ubiquitous computing and removing the trust from the infrastructure provider. Similarly, some IoT devices' little space for extensive storage and limited battery power restricts the complex operations required by cryptographic algorithms, thus risking confidentiality (Ukil, Sen and Koilakonda, 2011). Subsequently, a study by HP (2014) reveals that 70% of the most popular IoT devices contain serious vulnerabilities. Given that IoT has entering a phase of mass usage, this level of vulnerability is worrying in terms in privacy and security.

Overall, given the privacy challenges in the IoT, it requires a privacy awareness and control mechanism more advanced compared to typical privacy mechanisms. For instance, current smartphone operating systems do have centralised permission managers that provide users with control over the permissions requested by their smartphone apps. Whereas, the IoT currently does not offer any equivalent functionality. Instead, users are often unaware of the presence of IoT technologies, as there is no consistent mechanism for discovering them, let alone understanding the particular context under which personal data is collected or opting in or opt out of data collection practices. This is more pertinent for facial recognition based technology in particular, as there is no standardised way of determining whether an area is under video surveillance and what analytics might be applied to the footage captured by cameras.

2.2 Facial Recognition Technology

Facial recognition is defined as automated biometric technology that identifies individuals, from a digital image or video frame, based on their distinctive and measurable facial patterns (Gates, 2011). Conventionally, facial recognition technology has been utilised by government and law enforcement to support assorted security and safety tasks (Met.police.uk., 2020), however, in recent years many commercial applications have started using facial recognition technology.

A report by Allied Market Research finds that the global market of facial recognition technology is likely to grow to $9.6 billion dollars by 2022 (Allied Market Research, 2016). The rise in proliferation of the IoT is partly responsible for this growth as the decreasing cost of cameras and internet-connected computation devices has enabled large-scale deployments of IoT cameras in places such as offices, shopping centres, colleges, and public streets (Rajput, 2016). Consequently, there are widespread examples of real commercial implementations of facial recognition technology. For instance, by installing IoT cameras at shop entrances, the system 'Facedeals' (Sennaar, 2018) would recognise customers based on their Facebook profiles and deliver relevant ads to them based on their demographic information. In another example, a high school in Sweden introduced facial recognition trials in order to monitor its students' attendance in class, it was subsequently fined circa EUR20,000 for a GDPR breach (EDPB, 2019). Further, advertising companies are looking into analysing consumers' facial expression towards different advertisements to increase engagement of consumers (Doerrfeld, 2015).

Widespread implementation of facial recognition technology presents an increasing threat to personal privacy. It can be used to not only identify and recognise individuals but it can also be used to determine our social activities (US GAO., 2015), including who we socialise with and our psychological state (Dormehl, 2014), including whether we look happy or depressed. Moreover, this biometric data can be combined with auxiliary data, such as social media profiles, to gain even deeper insight into our lives. Ultimately, advocates of privacy highly criticise the obscure nature of facial recognition technology due to its lack of transparency and how video streams captured by IoT cameras, at time concealed, are used for the collection and processing of personal data (Introna and Wood, 2004).

2.3 Regulations

As a hopeful movement for better privacy policy in the IoT, the new European General Data Protection Regulation (GDPR), which came into effect on 25 May 2018 (Regulation, G.D.P., 2016), signifies the largest overhaul of modern data protection regulation in more than twenty years. The purpose of the GDPR is to give EU citizens more control over their personal data and it aims to influence the way in which organisations approach data collection and protection.

The GDPR (Regulation, G.D.P., 2016) defines personal data as "any information relating to an identified or identifiable natural person ('data subject')". In terms of biometric data, GDPR (Regulation, G.D.P., 2016) defines it as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". Given biometric data can be processed for the purpose of uniquely identifying a natural person, all biometric data is classed as sensitive 'special category' data and requires a higher level of protection. In other words, we (as individuals) own our facial images, and we have a right to its use, its ownership and its recognition (LaFrance, 2017). As specified in Article 9 of the GDPR, when personal data, such as biometrics, are collected from the data subject, then the data controller must ensure that their data processing is lawful, fair, transparent and, at the time when personal data is obtained, provide the data subject with information regarding the existence of automated decision-making and 'meaningful information about the logic involved'.

As defined in GDPR, consent must be communicated by a statement or a "clear affirmative action" that has to be unambiguous. Therefore, consent cannot be expressed by silence, inactivity or pre-ticked boxes. Most significantly, the consent should be specific and informed where the data subject understands exactly what they are consenting to. A practical application of facilitating consent can be found in many smartphones, which give access to some features of the device, such as Apple Pay, through facial recognition. The consent is given freely, can be withdrawn by deleting the face scan, and the functionality of the phone can be accessed by alternative means, like a passcode.

Nevertheless, given the challenges of ensuring privacy in the IoT and the trend of IoT technology companies, the standards of the GDPR are likely undermined. This is because of the underlying functionality and business models many IoT vendors rely on. For instance, IoT devices may be configured to persuade disclosure of personal data in order to offer seamlessly linked and personalised services for users (Wachter, 2018) and/or monetise the data collected by selling it to third parties. This leads to a fundamental, challenging tension between two forces for IoT technology: operating within the GDPR regulations and privacy standards on the one hand, and using identification technologies to personalise services and capture revenue on the other. The GDPR is therefore expected to have an interesting impact on the IoT industry and this project aims to offer some insight into how the challenges of meeting the GDRP and ensuring privacy in the IoT can be addressed.

2.4 Informed Consent

Given the challenges of ensuring privacy in the IoT and the tension between IoT technology and GDPR compliance, it is no surprise that free and well-informed consent in the IoT is even-the-more challenging. Informed consent can be defined as ‘the process by which a fully informed user participates in decisions about his or her personal data’ (Van Der Geest, Pieterson and De Vries, 2005). To achieve informed consent, Friedman (2000) introduces the Information Systems Model of informed consent, the model comprises factors associated with 'being informed' (including disclosure and comprehension) and 'giving consent' (i.e., voluntariness, competence and agreement). The model been integrated in 'Value-Sensitive Design' frameworks supported by many scholars as an essential part (Jacko, 2012) of real-world software systems.

However, the Information Systems Model’s ethical underpinnings related to informed consent are considered insufficient and outdated (Rhodes, Bowie and Hergenrather, 2003) for today's modern technology world, namely the IoT. The very nature of facial recognition, makes it difficult to establish effective mechanisms for informing users of the collection, storage and processing of their personal data and enabling them to withdraw consent at any time. For instance, as found in the UK Metropolitan Police’s trial of facial recognition (Met.police.uk., 2020) between 2016-2019, displaying messages that facial recognition technology is in use, is unlikely to sufficiently satisfy the threshold of explicit consent. Namely because data subjects are likely to already be in the vicinity of the facial recognition-enabled cameras by the time they are aware of it. Group consent also poses a challenge in informed consent. As demonstrated by Facebook's use of facial recognition in their photo-tagging tool, while one data subject may explicitly consent to the use of facial recognition to identify them in images, others who are affected by the technology may not have. The facial recognition service would be required to compare the consenting data subject’s face against many images of potentially non-consenting individuals to make an accurate tag.

Overall, this background section covers why the compliance of IoT technology with principles of data minimisation, data protection and consent by design is doubtful. Existing research finds that individual privacy expectations (Lin et al. 2012), social norms (Nissenbaum, 2009), the purpose of data sharing, whom data is shared with (Lederer, Mankoff and Dey, 2003), how long the data will be accessible and how it will be processed, are all factors that influence whether one will approve of disclosing their personal information. However, given that IoT sensors can be obscured, there are currently no mechanisms for discovering IoT device's, let alone providing users with sufficient privacy awareness and control. To enable better informed decisions, this project serves to communicate the privacy risk of IoT devices in a meaningful way and provide control in a way that enables users to make an informed decision as to whether or not they want to disclose sensitive personal data (Pollach, 2005). It is envisioned this will improve user's awareness and control of IoT systems, and allow users to achieve meaningful notice and consent to privacy agreements and ease the privacy paradox (Bashir et al. 2015).

3 Related Work

3.1 Methodology

Multiple stakeholders including regulatory bodies, trade organisation and privacy advocates have proposed better practices in using facial recognition technology commercially. Almost all of these guidelines include the practice of explicitly notifying individuals when facial recognition is being used and obtaining affirmative consent before using facial recognition to identify an individual. However, existing mechanisms which inform users about what data is collected and what choices they have with respect to how the data is used are not easily or effectively implemented in the IoT. With this gap in mind, to identify the requirements of an effective solution, this paper presents a systematic literature review of all the previous/current academic or commercial work on designing interfaces that provide privacy warnings and user-driven control.

The initial stage of the literature search involved identifying papers relevant to the design of interfaces providing privacy awareness and control in the electronic databases of Google Scholar, Scopus, IEEE, Web of Science and ACM. The initial search found a large form of evidence, including articles, published journals and patents. Using the keywords "IoT privacy nudges", "IoT privacy control" and "IoT privacy alerts", seventeen studies were found, however, eight of these studies were selected, this is because the following criteria excluded studies that:

a) Were anonymous, erratum notifications and editorials.
b) Concerned privacy warning and control interfaces which were only relevant to general online contexts, websites and e-commerce platforms.
c) Concerned privacy protection tools which do not have an interactable user awareness and control interface. For instance, a Policy Enforcement Fog Module (PEFM) can be implemented within the fog computing infrastructure to self-enforce privacy policies (Al-Hasnawi and Lilien, 2017).

The second stage of the literature search followed the research trail based on the references lists of papers found in the first stage. Using the same exclusion criteria, three additional relevant papers were found. In total, eleven papers were found to be most relevant for the design of interfaces which provide privacy warnings and user-driven control in both smartphone application and IoT contexts. How a user's personal data is collected, processed and used by smartphone apps is notably different to personal data practices in the IoT, and this is considered in the literature review. However, how the interfaces in both contexts approach providing privacy awareness and control, is central to how this project realises the design of its own prototype interface. Overall, it is believed that this review covers the most relevant literature pertaining to designing interfaces providing privacy warnings and user-driven control in the context of the IoT.

3.2 Literature Review

An overview of the relevant work identified can be found in Table 1. This table was realised through detecting areas of interest for the design of privacy awareness and control interfaces. Subsequently, the table summarises the system's name, the context of the system (i.e., what technology the interface is providing privacy awareness and control for) and whether its privacy nudges are personalised or non-personalised.

Table 1. Review of previous/current academic or commercial work on interfaces providing privacy warnings and user-driven control.

Study	**System name (**if applicable)	**Context**	**Privacy Nudges (personalised or non-personalised)**
Almuhimed et al. (2014)	AppOps	Smartphone apps	Non-personalised
Kelley, Cranor and Sadeh (2013)	Privacy Facts	Smartphone apps	Non-personalised
Lin et al. (2012)	-	Smartphone apps	Non-personalised
Ukil, Bandyopadhyay and Pal (2015)	Dynamic Privacy Analyzer	IoT (Smart Energy Systems)	Non-personalised
Bosua, (2014)	IWA (Intelligent Warning Application) 'Data Mind'	IoT devices	Personalised
Liu, Lin and Sadeh, (2014)	Privacy Guard	Smartphone apps	Personalised
Ferreira et al. (2015)	Securacy	Smartphone apps	Personalised
Harbach et al. (2014)	-	Smartphone apps	Personalised
Tsai et al, (2017)	TurtleGuard	Smartphone apps	Personalised
Jackson and Wang (2018)	-	Smartphone apps	Personalised
Liu et al. (2016)	Personalised Privacy Assistant (PPA)	Smartphone apps	Personalised

3.2.1 Privacy Nudges

Over past years, ‘nudges’ have emerged within the privacy literature as an effective technique for influencing user behaviour (Acquisti et al., 2017; Kozlov, Veijalainen and Ali, 2012; Yang et al., 2019). In this sense, nudges can act as a soft warning or intervention that can guide users toward making better decisions to control how much their personal data is disclosed. When detecting areas of interest for the design of privacy nudges, a pattern emerged in making a difference between personalised and non-personalised privacy nudges. Personalised nudges are nudges which are tailored based on individual traits (Egelman and Peer, 2015) and demographics (Knijnenburg and Alfred Kobsa, 2013), whereas, non-personalsied nudges are general privacy notifications that aren’t tailored to each individual. Four (36%) of the eleven applications of nudges within the literature have focused on a non-personalsied, ‘one-size-fits-all’ approach. Prior work in this category aims to increase users’ knowledge about the purpose of permission requests by applying a general privacy notification to a diverse set of users. For instance, **AppOps** (Almuhimed et al., 2014) informs users about the data collection practices of apps installed on their devices and users are periodically nudged to review and adjust their permission settings. **Privacy Facts** (Kelley, Cranor and Sadeh, 2013) provides a “just-in-time” privacy display, warning users when sensitive information, such as their geolocation, is being requested. Alternatively, **Lin et al. (2012)** provide the privacy rating of the mobile applications a user installs. Meanwhile, the **Dynamic Privacy Analyzer** (Ukil, Bandyopadhyay and Pal, 2015) ensures that user’s privacy is protected by accurate estimation of privacy disclosure risk though a robust analytical framework.

In summary, these non-personalised nudges assume that the ‘true cost’ (John, Acquisti, and Loewenstein, 2011) of disclosing personal data is about the same for every user, for every type of smartphone app or IoT device, for every type of personal data, in every situation. Even when disregarding potentially unique privacy configurations, different individuals are likely to have different preferences, and these preferences may depend on the specific situation and environment of IoT devices. Conversely, seven (64%) of the eleven studies have focused on making privacy nudges more effective by tailoring them based on the individual. For instance, **Data Mind** gives users more personalised control over the collection, storage and processing of their personal data collected by IoT and social media. **Liu, Lin and Sadeh, (2014)**, **Tsai et al. (2017)** and **Liu et al. (2016)** all use machine learning and data mining to identify groups of users with similar privacy preferences and use this to automatically predict the privacy decisions on behalf of the user. Meanwhile, **Securacy** (Ferreira et al., 2015), has a reactive, personalised approach, providing feedback on app permission settings that the user has previously stated as concerning. Alternatively, **Harbach et al. (2014)** leverage the rich set of personal data available on smartphones to communicate risks using personalised and contextualised examples. Meanwhile, **Jackson and Wang (2018)** propose a personalised privacy notification approach to nudge users towards privacy actions and decisions that reflect their privacy attitudes.

Overall, personalising privacy nudges is in accord with research which recognises the substantial diversity in the privacy attitudes and behaviours throughout cultures among different individuals within the same culture (Moore, 2017; Duby, 1992; Westin, 1966). Further work has also studied the psychometric differences of individuals and found them to be predicators of differences in privacy attitudes and behaviours (Egelman and Peer, 2015). This suggests that differences in individual traits plays a significant role in terms of privacy decision making. Therefore, in respect of the project's objectives, to effectively influence informed decision making, this project will focus on providing personalised privacy nudges.

Analysis. Other than Data Mind, the eleven studies do not innovate toward providing personalsied privacy nudges in the IoT. To personalise nudges, users of Data Mind must set up their preferred data protection levels. Alternatively, Jackson and Wang (2018) highlight the importance of personalising privacy nudges based on user's underlying privacy attitudes and decision processes, and demonstrate their approach's effectiveness in nudging users toward privacy actions. Subsequently, this project seeks to go beyond the work of Data Mind and Jackson and Wang (2018), and will personalise privacy nudges by capturing the underlying privacy attitudes and decision process of users in the IoT**.** It is envisioned this will enable the project to influence informed decision making by highlighting any discrepancy between the user's privacy attitudes and the privacy riskiness of an IoT device.

3.2.2 Measuring Users' Privacy Attitudes Towards IoT Technologies

For the seven studies that personalise privacy nudges, there are different approaches among them for measuring the privacy boundaries and privacy attitudes of individual users, a summary can be found in table 2. The table summarises how privacy boundaries and attitudes of individual users are measured and whether the measurement is conducted once by the system or continuously. This table was realised through focusing on the seven studies which personalsied privacy nudges and investigating how they measured privacy boundaries and users' privacy attitudes in order to personalise their nudges.

Table 2. Review of how interfaces providing personalised privacy nudges measure privacy boundaries and attitudes of individual users.

Study	**Method** (How privacy boundaries and attitudes are measured)	**One time or continuous measurement?**
Bosua, (2014)	User settings of required risk levels	One time
Liu, Lin and Sadeh, (2014)	Machine learning to predict privacy preferences	Continuous
Ferreira et al. (2015)	User settings of required risk levels	One time
Harbach et al. (2014)	Personalised examples of risk using user's current personal data	Continuous
Tsai et al, (2017)	Machine learning to automatically predict privacy preferences.	Continuous
Jackson and Wang (2018)	9-item Mobile Users Information Privacy Concerns (MUIPC) survey	Continuous
Liu et al. (2016)	Machine learning to predict privacy preferences	Continuous

3.2.2.1 The Privacy Preferences Approach

Of the seven studies that personalise their privacy nudges, two of the systems (Bosua, 2014; Ferreira et al., 2015) record individual user's attitudes by explicitly asking for the permissions, for categories accessed by apps, that the user is most comfortable with (i.e. privacy preferences). These privacy managers follow the typical Identity Based Access Control model (IBAC), where individual permissions can be set for each app or IoT device. However, this model and relying on individual's prespecified privacy preferences has a number of significant limitations. Firstly, users may be overwhelmed by the amount of privacy settings available to them, some of which are only vaguely pertinent to privacy. Secondly, IoT device users might not understand the repercussions of privacy permissions, especially when users aren't tech savvy nor privacy aware. And finally, users are often unsure about their privacy preferences (Acquisti, Brandimarte and Loewenstein, 2015) and their preferences may change as time goes on.

3.2.2.2 The Socio-technic Approach

Alternatively, the remaining five studies aim toward a socio-technic approach and capture individual users' privacy attitudes by measuring their underlying decision processes rather than their preferences (Liu, Lin and Sadeh, 2014; Harbach et al., 2014; Liu et al., 2016; Tsai et al., 2017; Jackson and Wang, 2018). This approach aims to establish individual's underlying decision processes that cause their privacy attitudes and use this information to more effectively tailor decision support mechanisms, such as nudges, and aid informed privacy decision making. For instance, DePaula et al. (2005) acknowledge a constant struggle for individuals to predict and stipulate their privacy preferences before using a system as privacy needs are context-dependent and thus hard to stipulate a priori. Therefore, rather than utilising individual users' privacy preferences, it is also argued that obtaining general privacy attitudes is more stable and easier to obtain. Practical solutions to operationalise and measure the privacy attitudes and underlying decision processes of individual users are presented in the current work.

Liu, Lin and Sadeh, (2014), Tsai et al. (2017) and Liu et al. (2016), use machine learning and data mining to identify groups of users with similar privacy preferences and use this to automatically predict the privacy decisions and adjust permission settings on behalf of the user. Given privacy permission settings can be set automatically, all three systems also provide a feedback mechanism to encourage users to audit decisions and adjust any errors. However, the three studies use data sets comprising the permission settings of millions of smartphone users. There are currently no data sets of a similar scale available for the permissions settings of IoT device users. To gather such data would require substantial research to study IoT users' privacy decisions in both controlled and real-world environments.

Alternatively, Harbach et al., 2014 access a user's actual personal data (e.g. location, images, phone state etc.) stored on their smartphone to personalise and contextualise examples of how an application can also access such data. However, unlike smartphone applications, the personal data collected, processed and used by IoT devices tends to be analysed and stored outside of the IoT user's immediate control. Therefore, it is difficult to communicate privacy risks with a concrete piece of existing personal data as an example, while listing a known cause as well as concrete consequences.

A final solution to operationalise and measure the privacy boundaries and attitudes is using a validated scale of privacy concerns. To measure individuals' general privacy attitudes towards mobile apps, Jackson and Wang (2018) use the Mobile Users Information Privacy Concerns (MUIPC) survey (Xu et al., 2012). The survey is proposed and validated by Xu et al. (2012) and captures the high-level privacy values that an individual supports. When compared to the alternative methods of measuring individual user's privacy attitudes via machine learning and data mining of a user's existing personal data, measuring privacy attitudes via an established and validated privacy scale has a number of advantages.

First, the survey is reliable as users are not required to be privacy aware nor technically savvy to have general privacy attitudes and behaviours. Second, unlike machine learning and data mining, using a Likert scale and measuring across specific constructs (user concerns about perceived intrusion, secondary use of information, and perceived surveillance), an individual's MUIPC score can be operationalised into discrete levels of privacy concern. Using this measure, the score can be compared with a score measuring the privacy riskiness of an app or IoT device on a similar scale. The two scores can then be used to juxtapose users' general privacy attitudes towards IoT devices compared to the riskiness of a particular app or IoT device. Importantly, this allows an interface to bring the constituents of the juxtaposition to the forefront of the interface to trigger user behavioural changes.

The MUIPC is a version of the original Concern for Information Privacy (CFIP) survey, adapted for measuring privacy in the smartphone context. Smith et al. (1996) first introduced the CFIP recognised four dimensions (see Appendix item A) of privacy concerns regarding in response to organizations' information privacy practices: collection, unauthorized secondary use, improper access and errors. Stewart and Segars (2002) enhance understanding behind the dimensionality of the CFIP construct and state, users may be exposed to high levels of CFIP if (1) users view the service as collecting too much personal data, (2) unauthorized third parties are given use of personal information for undisclosed purposes, (3) personal data can be accessed by unauthorized third parties and (4) personal data is erroneous.

Analysis. Stewart and Segars (2002) empirically examined the CFIP framework and validated the measurement model as a multidimensional construct. Their results suggest that CFIP may be better characterised as a reflective, second-order factor structure rather than a correlated set of first order factors (Korzaan and Boswell, 2008). In other words, the assumptions underlying the structure of the CFIP can be reinvented in light of emerging technology. However, although the CFIP has been adapted to measure privacy concerns in the smartphone context, few systematic attempts have been made to provide a theory-driven framework on the specific nature of privacy concerns among IoT users. This is important given the shifting dimensions of information privacy concern, for instance, the privacy concerns and how users perceive privacy threats is likely to differ in the context of smart phones compared to IoT. To fill the gap in this literature, this paper proposes a CFIP survey

(Smith et al., 1996) modified to measure the underlying privacy attitudes and decision processes of users in the context of IoT.

The modified survey (see Appendix item B) measures privacy attitudes across the same four dimensions as the original CFIP survey (collection, unauthorized secondary use, improper access and errors). Namely, data collection concerns the collection of extensive amounts of personal data by IoT service providers. Unauthorised secondary use is defined as the concern that information collected for one purpose may ultimately be used for other unauthorized purposes. Improper access is the concern that personal data collected by IoT service providers may be accessible by unauthorised parties. Finally, errors entail the concern that inadequate procedures are used to protect against accidental or deliberate errors in storing personal data.

4 Requirements: IoTAware

In terms of the original research question: *How to ensure users have awareness and control of the collection, storage and processing of personal data within IoT systems?* Based on the findings of the literature review, this paper argues that, by measuring a user's underlying privacy attitudes and decision processes, privacy nudges can be tailored to the user. Highlighting any privacy discrepancy to the user can then trigger behaviour changes by giving the user the option to change the IoT device's permission requests in alignment with their privacy attitudes (e.g., enabling users to obfuscate their faces on live video feed captured by an IoT camera). In response, this paper proposes a conceptual architectural model and mock-up prototype design for a personalised IoT privacy warning and control application named 'IoTAware'.

To understand how this paper's solution will provide value to users, the following user stories were created. The user stories were created based on the findings of the literature review and examining how the techniques and approaches could be incorporated in a hypothetical IoT scenario. Each user story creates a high level requirement to achieve the aim of this research. In summary, to realise an effective solution and meet the project's aim and objectives, the solution must:

1. Accurately and efficiently measure the privacy risk of IoT devices.
2. Precisely measure individual user's underlying privacy attitudes in the IoT context.
3. influence informed decision making highlight any discrepancy between a user's privacy attitudes and the privacy risk of an IoT device.
4. Allow users to control their privacy in IoT systems.

Title: Accurate and efficient measuring of the privacy riskiness of IoT devices

User Story:
As a non tech savvy nor privacy aware user,
I want the risk of the IoT device to be accurately measured,
So that I know how risky the device is.

Acceptance Criteria:
Given the device is registered in the IPRR,
And I enter the vicinity of an IoT device,
When the IoT device has a higher-than-average number of data flow paths,
And I have a higher-than-average collection privacy-concern score
Then the IoT device has high collection risk and the collection privacy icon is coloured red.

Title: Precise measurement of individual user's underlying privacy attitudes and decision process in the IoT context

User Story:
As a non tech savvy nor privacy aware user,
I want my privacy concern score to accurately reflect my privacy attitudes and underlying decision process in the IoT context,
So that I know how if an IoT device is within or outside my comfort zone.

Acceptance Criteria:
Given I have completed the CFIP survey,
And I enter the vicinity of an IoT device,
When I have low privacy concern for collection of my personal data by IoT systems,
And the IoT device has a low privacy-risk score for collection,
Then then the IoT device has high low privacy risk and the collection privacy icon is coloured green.

Title: Providing a privacy nudge when the user enters the immediate vicinity of the IoT device.

User Story:
As a non tech savvy nor privacy aware user,
I want to be notified when I enter the vicinity of an IoT device,
So that I know the device is there.

Acceptance Criteria:
Given a Bluetooth low energy (BLE) beacon resides within an IoT device,
When I enter the immediate vicinity of the IoT device,
Then I receive a privacy nudge from IoTAware.

Title: Correctly highlighting the privacy discrepancy to the user

User Story:
As a non tech savvy nor privacy aware user,
I want to be see if there is any discrepancy between my level of privacy-concern and the privacy-risk of the IoT device,
So that I know whether an IoT device is not in my best interests.

Acceptance Criteria:
Given an IoT device has a high unauthorised secondary use privacy-risk score
And I have a low unauthorised secondary use privacy-concern score
When I enter the immediate vicinity of the IoT device,
Then the unauthorised secondary use privacy icon is coloured yellow.

Title: Allowing the user to control their privacy

User Story:
As a non tech savvy nor privacy aware user,
I want to control my privacy,
So that my privacy reflects my privacy attitudes.

Acceptance Criteria:
Given I have received a privacy nudge,
And I have chosen to change my settings,
When I select "obscure my face",
Then the user's face is blurred on the camera's real-time video recording.

5 Project Management

The Gantt chart (see appendix item H) of this project's actual progress, compared to the forecasted Gantt chart (see appendix item I), reveals how this project's activities have deviated over time. This project's literature review of existing work revealed design approaches and techniques which were important for the design of an effective privacy awareness and control interface. The approaches and techniques which were not considered in the initial project definition, include (1) realising the benefit of personalising privacy nudges via a privacy discrepancy approach (2) addressing a gap in the literature with a technique to measure the underlying privacy attitudes and decision processes of users in the context of IoT, and (3) addressing another gap in the literature with a technique to measure the privacy risk of IoT devices. Subsequently, including these approaches and techniques in the project's work was significant for effectively meeting the project's aim and objectives.

Therefore, the project's focus shifted from development of a fully-working un-personalised IoT awareness and control interface to developing and evaluating a conceptual architectural model and mock-up prototype design of a personalised IoT privacy warning and control application. To allow time for in-depth exploration and investigation, the following features of the IoTAware interface weren't included in the project's scope as they were not feasible to include, this includes:

- Encryption between the IoTAware mobile application's communication with the Information Privacy Risk Repository (IPRR), Privacy Settings Implementation Point (PSIP) and Face Trainer (vice versa).
- Security in terms of accessing the IoT device from a third-party device.
- Security in terms of communication between the IoT device and mobile application.
- Detailed mathematical explanation of facial recognition algorithms.
- Moderation of privacy risk information inputted into the system and anti-spam mechanisms.

A diary of the project's activities, including issues and risks encountered during the course of the project, can be found in appendix item K.

To suit the more exploratory and investigational direction of the project, actual development of the project shifted toward being iterative as opposed to linear.

In particular, the IoTAware prototype interface was developed with a focus on User-Centred Design (UCD). According to ISO 13407 (ISO, 1999), the human-centred design process for interactive systems entails four principles: active involvement of users; appropriate allocation of function between users and technology; iteration of design solutions; and multi-disciplinary design. Pictured as a cycle of 'design, test, measure, redesign', a focus on UCD throughout the development of IoTAware enabled solutions to evolve and constantly move forward during development. Subsequently, methods of UCD were rigorously applied to the development of the IoTAware interface by instilling an iterative design process. This consisted of multiple online experiments with users and, depending on an experiment's feedback, adaptations were continually made to the interface and validated in the next experiment. The feedback of the first user study helped identify a number of areas for improvement, the feedback in question and the subsequent improvements to the interface are covered in the evaluation section (see section 10).

6 System Design

Figure 1 illustrates the system's architecture working in a particular scenario with an IoT device using facial recognition technology. This proposed infrastructure is intended to be applicable to a wide range of IoT scenarios that involve notifying users of nearby IoT sensors. The following steps describe a typical work flow of how a user interacts with the IoTAware system.

1. The user installs the IoTAware app on their smartphone and agrees to upload an image of their face and register their identity by signing-in using Google's OAuth 2.0.
2. After authenticating their identity, the user completes the CFIP survey, this measures measure the underlying privacy attitudes and decision processes of the user in the context of IoT.
3. When the user enters the immediate proximity of the IoT camera, IoTAware picks up the signal of the Bluetooth low energy (BLE) beacon attached to the camera. The beacon also broadcasts the URL to the Information Privacy Risk Repository (IPRR) responsible for the particular camera network.
4. A privacy nudges is sent to the user, highlighting any discrepancy between the user's privacy-concern scores and the privacy-risk scores of the IoT resource. The user then reviews the information and decides whether to control the device's permission requests. Once the user makes their choice, the corresponding setting is sent to the Privacy Settings Implementation Point (PSIP) for update.
5. The PSIP upon verifying (checking OAuth token) the request sent by the user, first updates the local database with the user's current setting and then forwards the request to the Privacy Mediator for appropriate action.
6. The Privacy Mediator, upon receiving the request from the PSIP, first retrieves the user's facial embedding from the training server and then starts performing facial recognition to detect the user's face in the video stream. Depending on the privacy setting selected by the user the Privacy Mediator either denatures the user's face or retains unaltered video frames.

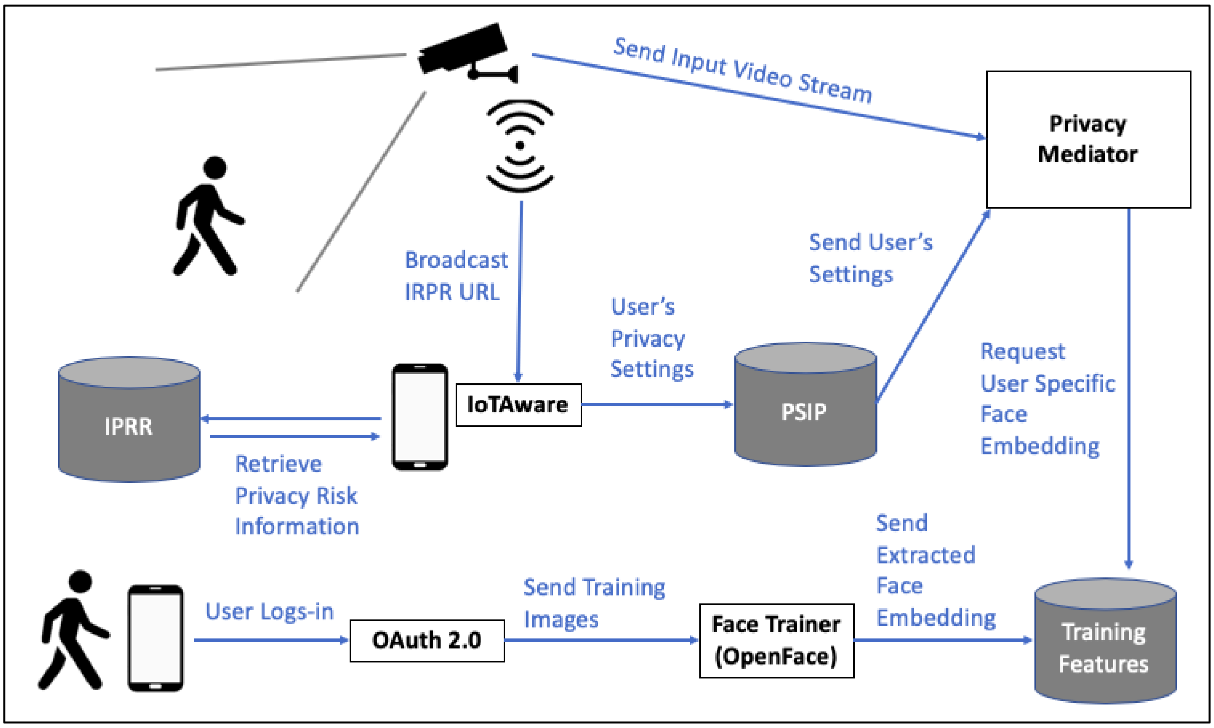
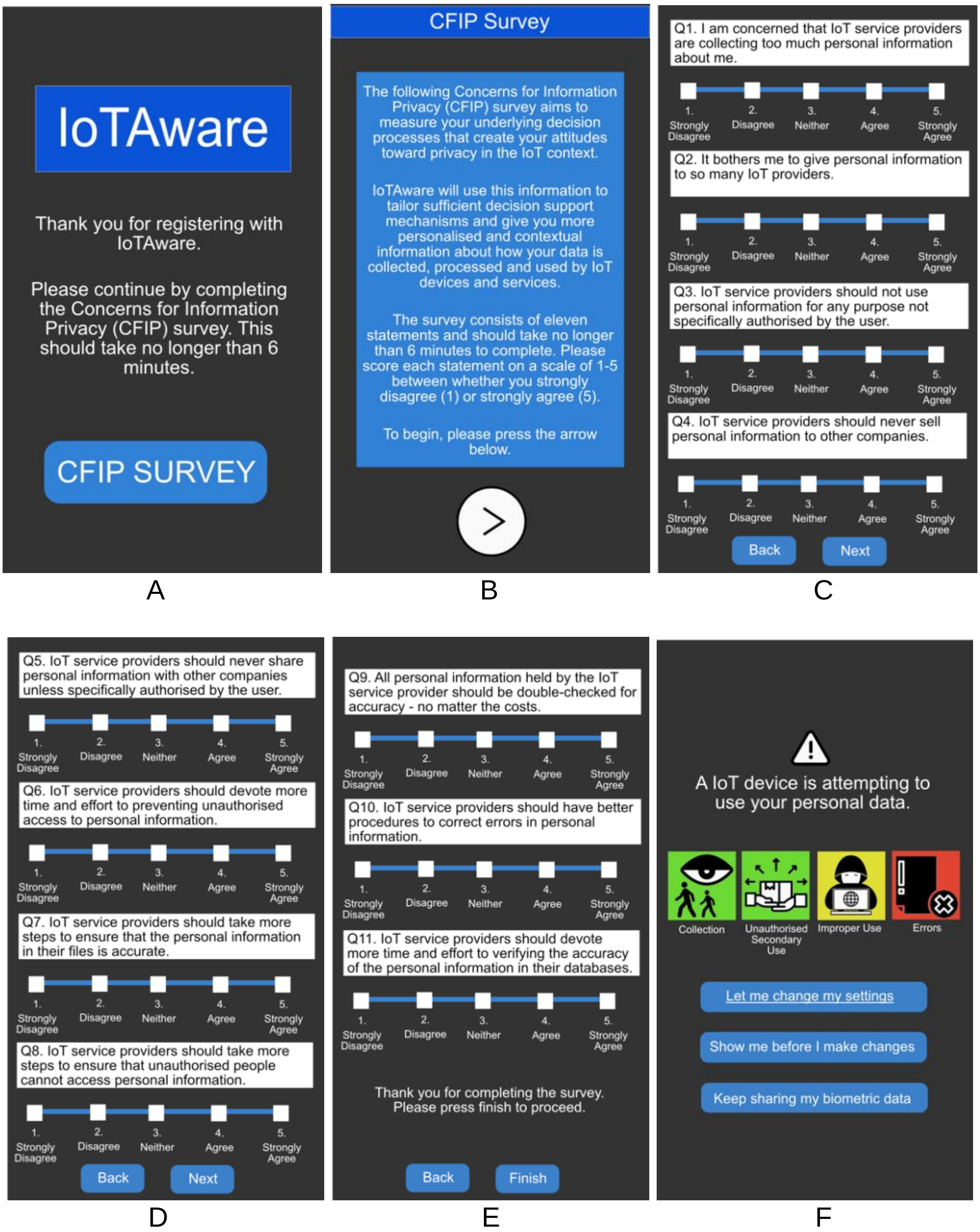


Figure 1. Illustration of IoTAware's System Architecture. (IPRR = IoT Privacy Risk Repository, PSIP = Privacy Settings Implementation Point).

Unlike within our homes, in public spaces, people generally do not know what IoT devices are around them, what data they collect, and what happens to that data. Alternatively, homeowners are aware of their IoT resources and can review and control the permissions granted to the IoT resource through the associated smartphone app. In this context, IoTAware could have a more centralised infrastructure, namely IoTAware could enforce permissions settings directly through the homeowner's smartphone. However, IoT resources in public spaces, such those using facial recognition technology, can collect and process personal data discretely and in real-time. To remedy this situation, it requires an infrastructure that supports the discovery of nearby IoT resources, their privacy risk information and the permission settings supported by the underlying system. In this context, this proposed infrastructure can relieve privacy fears by providing users with in situ notification of nearby IoT cameras, highlight any privacy discrepancy and present users with privacy control. This infrastructure can be generalised to many other IoT scenarios that involve data collection with sensors.

6.1 IoTAware

The IoTAware interface is intended to be deployable as a smartphone app. Figure 2 illustrates the designs of the interface after the user has been authenticated using Google's OAuth and uploaded images of their face to the training server. Figure 2.A shows the landing page of the IoTAware application. Figures 2.B – 2.E are designs for completing the CFIP survey. Once the user enters the proximity of an IoT device, a privacy nudge, as shown in Figure 2.F, is sent to the user. The privacy icons are based on the four constructs of the CFIP survey and are coloured based on any juxtaposition between a user's privacy-concern score and the IoT device's privacy-risk score. When selecting “Show me before I make changes”, Figure 2.G will give users a detailed report with detailed privacy information. Finally, when selecting “Let me change my settings”, Figure 2.H will give users the option to adjust their permission settings.



A

IoTAware

Thank you for registering with IoTAware.

Please continue by completing the Concerns for Information Privacy (CFIP) survey. This should take no longer than 6 minutes.

CFIP SURVEY

B

CFIP Survey

The following Concerns for Information Privacy (CFIP) survey aims to measure your underlying decision processes that create your attitudes toward privacy in the IoT context.

IoTAware will use this information to tailor sufficient decision support mechanisms and give you more personalised and contextual information about how your data is collected, processed and used by IoT devices and services.

The survey consists of eleven statements and should take no longer than 6 minutes to complete. Please score each statement on a scale of 1-5 between whether you strongly disagree (1) or strongly agree (5).

To begin, please press the arrow below.

C

Q1. I am concerned that IoT service providers are collecting too much personal information about me.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q2. It bothers me to give personal information to so many IoT providers.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q3. IoT service providers should not use personal information for any purpose not specifically authorised by the user.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q4. IoT service providers should never sell personal information to other companies.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Back Next

D

Q5. IoT service providers should never share personal information with other companies unless specifically authorised by the user.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q6. IoT service providers should devote more time and effort to preventing unauthorised access to personal information.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q7. IoT service providers should take more steps to ensure that the personal information in their files is accurate.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q8. IoT service providers should take more steps to ensure that unauthorised people cannot access personal information.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Back Next

E

Q9. All personal information held by the IoT service provider should be double-checked for accuracy - no matter the costs.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q10. IoT service providers should have better procedures to correct errors in personal information.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Q11. IoT service providers should devote more time and effort to verifying the accuracy of the personal information in their databases.

□ 1. Strongly Disagree □ 2. Disagree □ 3. Neither □ 4. Agree □ 5. Strongly Agree

Thank you for completing the survey. Please press finish to proceed.

Back Finish

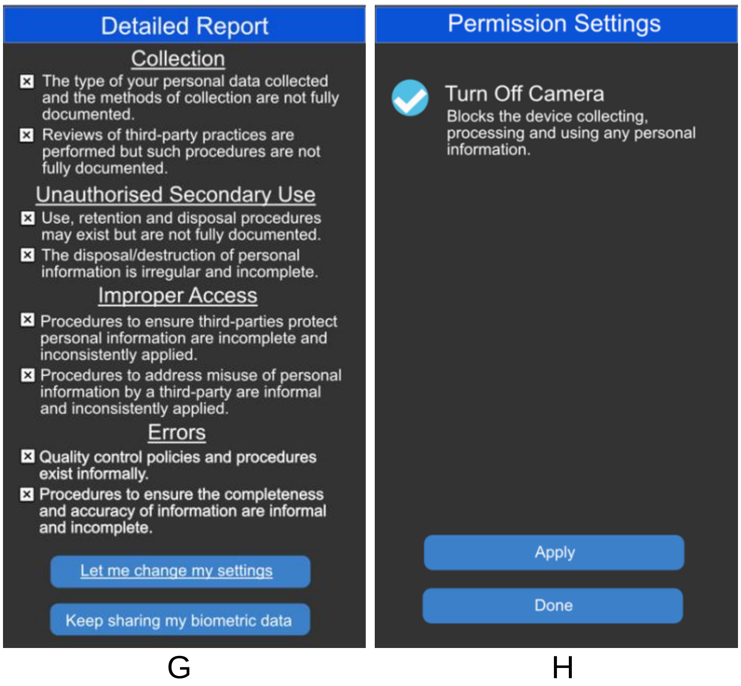
F

⚠ A IoT device is attempting to use your personal data.

Let me change my settings

Show me before I make changes

Keep sharing my biometric data



Detailed Report

Collection

☒ The type of your personal data collected and the methods of collection are not fully documented.

☒ Reviews of third-party practices are performed but such procedures are not fully documented.

Unauthorised Secondary Use

☒ Use, retention and disposal procedures may exist but are not fully documented.

☒ The disposal/destruction of personal information is irregular and incomplete.

Improper Access

☒ Procedures to ensure third-parties protect personal information are incomplete and inconsistently applied.

☒ Procedures to address misuse of personal information by a third-party are informal and inconsistently applied.

Errors

☒ Quality control policies and procedures exist informally.

☒ Procedures to ensure the completeness and accuracy of information are informal and incomplete.

Permission Settings

☑ Turn Off Camera

Blocks the device collecting, processing and using any personal information.

Figure 2. Design of post-registration sections of the IoTAware interface.

6.1.1 Measuring Individual User’s Privacy Attitudes towards IoT Technologies

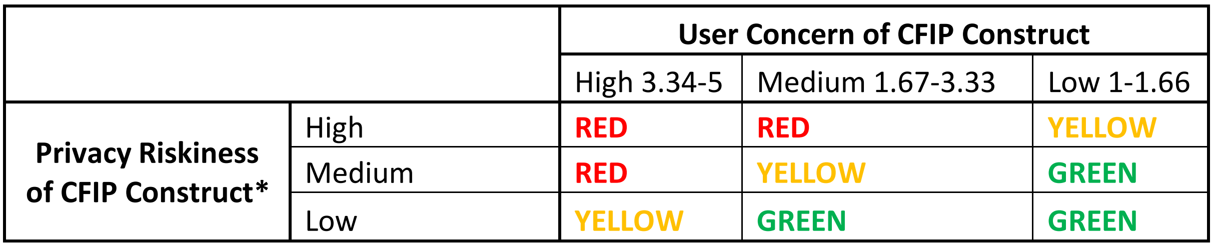
To measure users’ underlying privacy attitudes and decision processes in the context of IoT, IoTAware presents a modified version of the CFIP survey (see Appendix item B). The survey contains eleven statements across four dimensions (collection, unauthorised secondary use, improper access and errors) and users are asked to answer each statement with a response from a 5-point Likert-scale ranging from Strongly Disagree to Strongly Agree. After users complete the survey, IoTAware will then develop a single ‘privacy-concern’ score for each of the four constructs by averaging the responses of each construct. In order to operationalise the score into distinct levels for visualising privacy warnings (using a three-colour traffic light metaphor), the average 5-point score of each construct is divided into three categories and will either be: 1-1.66 to indicating low privacy concern, 1.67-3.33 as medium concern or 3.34-5 indicating high concern.

6.1.2 Design of Privacy Warning Icons

A major component of the system is sending privacy nudges to alert users of any discrepancy between their privacy concern-score and privacy risk-score of the IoT device in their proximity. In order to represent any discrepancy on a meaningful scale, warning icons for all four constructs of privacy concerns (collection, unauthorised secondary use, improper access and errors) are displayed in the centre of the nudge. Figure 2.F shows the current design of these three icons, these icons were inspired by images of privacy icon designs by the Noun Project (https://thenounproject.com). The Noun Project is a website that aggregates and catalogues symbols that are created and submitted by graphic designers around the world. The site has four guidelines for summitted icons: include only the important characteristics of the idea conveyed, maintain a consistent design style, favour an industrial look over a hand-drawn one, and avoid conveying personal beliefs, feelings and opinions (The Noun Project, 2020).This makes the noun project’s icons a visual language that can be trusted to allow quick and easy communication of the privacy icons, no matter the culture of the user.

6.1.3 Colour of Privacy Warning Icons

To reflect the degree of discrepancy between a user’s privacy concern-score and the privacy risk-score of an IoT device, the privacy icons (see Figure 2.F) are coloured using a three-color approach, such as the one used by Jackson and Wang (2018). Leveraging a familiar metaphor of traffic lights, green represents low risk, yellow represents medium and red represents high risk. The colour of icons is determined using two variables – the user’s privacy concern-score and the privacy risk-score of the IoT device. Subconsciously, if users are concerned about unauthorised secondary use of their personal data processed by an IoT device and the IoT device under consideration has a high level of riskiness in unauthorised secondary use, the user’s decision to accept all permission requests would contradict their privacy attitudes towards unauthorised secondary use of their personal data. Therefore, in this case, the colour of the unauthorised secondary use icon would be red, signalling a high degree of discrepancy between users’ privacy attitudes and the privacy riskiness of the IoT device. Figure 3 shows the risk calculation table to determine the colour of privacy icons based on users’ general privacy concerns and the privacy riskiness of specific IoT devices. In summary, the increasing levels of discrepancy would map to the icon colours of green, yellow, and red.



		User Concern of CFIP Construct		
		High 3.34-5	Medium 1.67-3.33	Low 1-1.66
Privacy Riskiness of CFIP Construct*	High	**RED**	**RED**	**YELLOW**
	Medium	**RED**	**YELLOW**	**GREEN**
	Low	**YELLOW**	**GREEN**	**GREEN**

*precisely how the privacy riskiness of devices is calculated will be covered in the implementation section of this paper. (see section 8.1)

Figure 3. Risk calculation table to determine the colour of privacy warning icons based on user’s general privacy concerns and the privacy riskiness of specific IoT devices.

6.1.4 Nudge Response Options

To target users into making decisions to change the IoT device’s permission requests, user responses to the privacy nudge are designed using a three-option approach, similar to the one used by Almuhimed et al. (2014). At the bottom of the nudge there are three options for users to respond to the privacy nudge they receive, these include “Let me change my settings”, “Show me more before I make changes or “Keep sharing my [data]”.

The “Let me change my settings” option opens the privacy permission settings page directly. Theoretically, by facilitating access to the permission settings it may lead users to review and adjust additional permissions as they switch their focus to privacy control. Given this prototype encourages users to make privacy decisions in alignment with their privacy attitudes, this option is highlighted in the nudge. The second option, “Show me more before I make changes”, opens a detailed report in IoTAware, shown in Figure 2.G. The detailed report will list the IoT device’s data practices across the four areas of privacy concern as follows:

- Collection: detail how much and how frequent personal data is collected by the IoT service provider.
- Unauthorised secondary use: detail the purpose of personal data use, whether personal data is shared and/or sold to other companies and if there is a risk information may be used for unauthorised purposes.
- Improper access: detail the time and effort to prevent unauthorised access to personal data.
- Errors: detail how the accuracy of personal data is checked and verified and the procedures to correct errors in personal information.

The details for each of the four areas will be summarised based on the IoT device’s privacy risk information retrieved from the IPRR. The goal of the detailed report is to allow users to evaluate how personal data is collected, processed and used by the IoT device and for users to compare the practices with their expectations. As opposed to naming the second option “show me more information”, this option purposefully indicates that users will be able to make changes and implies that the additional information may help their decision. At the bottom of the detailed report, the remaining two options from the nudge (“Let me change my settings” and “Keep sharing my data”) are replicated in order to make the information of the detailed report actionable.

The third option (“Keep sharing my [data]”) gives the user the option to follow the status-quo. Keller et al. (2011) advocate employing ‘enhanced active choice’ in order to emphasise the favoured option (“Let me change my settings”). This involves highlighting the damages present in the non-favoured alternative (“Keep sharing my [data]”), therefore, the third option is to be adapted to the specific personal data to be shared (e.g., [data] is replaced with “biometric data”). Finally, users can also opt to not respond to the nudge by leaving the notification.

6.1.5 PSIP (Privacy Settings Implementation Point) - Permission Settings

The permission settings page (see Figure 2.H) provides a checklist of permissions requested by a particular IoT device and gives users the option to ‘check’ or ‘un-check’ permissions to grant or deny the device’s requests. Adjustments to settings in IoTAware are sent to the privacy settings implementation point (PSIP) that ensures that the privacy settings are systematically captured and enforced. The selection of privacy settings available to the user depends on the fundamental services that offer simple REST APIs to enforce privacy settings. While this has the potential to provide flexible privacy settings to users, for the purpose of this study, simple options to ‘check’ and ‘un-check’ permissions are provided. To support repeat-visits to trusted IoT devices, there is a ‘save for this device’ option. Here it is envisioned that the

PSIP will maintain a database for storing each user's privacy settings, therefore, when pressing 'save for this device', the user's permission settings are saved for the next time the user enters the proximity of the same device.

6.1.6 IPRR (Internet of Things Privacy Risk Repository) - Measuring the Privacy Riskiness of IoT devices

Many forms of privacy risk management analysis are available. For instance, Privacy Impact Assessments (PIAs), such as the AICPA/CICA Privacy Impact Assessment Tool (2011), provide a measurable criterion for comparing an IoT vendor's compliance with international privacy regulations. However, the content and risk measuring of PIA's is subjective. This makes automated privacy risk analysis difficult and requires extensive moderation and anti-spam mechanisms to ensure validity. Alternatively, a more accurate, interesting and semi-automated form of privacy risk analysis can be found in program-analysis. Program-analysis techniques are used to design and build algorithms that identify security and privacy issues and vulnerabilities within the targeted IoT device's programming platform. These techniques operate on IoT app source code to achieve a variety of goals, these goals of analyses include sensitive data leaks, abuse prevention, permission misuse, data provenance and more.

Program analysis can be applied either statically or dynamically. In static analysis, there is a focus on issues of sensitivity analysis and code representation and the source code of an app is analysed without running it, whereas, in dynamic analysis, there is a focus on inspection-level and input generation and the code is run, on possibly under-instrumented conditions. Overall, static analysis tools are more efficient, easier to automate (Lin et al., 2014) and focus on analysing complete source code. Subsequently, static program-analysis is used to support the development of this paper's solution, where it is envisioned that the source code of each IoT device will be analysed to score the device's privacy risks vis-à-vis their relevance to the four CFIP constructs. Each device's privacy risk-scoring will then be stored in the IPRR (Internet of Things Privacy Risk Repository), a web interface, compliant with a machine readable JSON schema.

The IPRR is designed as a distributed platform that can be arranged around buildings or cities. While the building platform may be controlled and managed by the organisations that own the building, a cities platform may be open to input from services that have created or know of the data collecting processes of IoT devices. The open scenario requires moderation of inputs and anti-spam mechanisms in place; however, this is not included in the scope of this paper's prototype. In terms of availability, the IPRR can be discovered by the user through a directory based on geo-location or advertised with Bluetooth low energy (BLE) beacons.

As IoT apps are exposed to a myriad of sensitive data from interconnected sensors and devices, one of the chief criticisms of modern IoT systems is that the existing commercial frameworks lack basic tools and services for analysing what they do with personal information (Zeng, Mare and Roesner, 2017). SmartThings (2020), OpenHAB (2020), Apple's HomeKit (2020) provide guidelines and policies for regulating security and these related markets provide a degree of internal (hand) vetting of the applications prior to distribution. However, tools for evaluating privacy risks in IoT implementations is, at this time, largely non-existent. What is needed for measuring the privacy risk of IoT devices is a suite of analysis tools and techniques targeted to IoT platforms that can identify privacy concerns in IoT apps. To fill this gap, this paper uses SaINT (Celik et al., 2018), a static taint analysis tool, specialising in Information Flow Analysis (IFA) for IoT applications. It provides a rigorously grounded framework for evaluating the use of sensitive information in IoT apps - and therein provides developers, markets, and consumers a means of identifying potential threats to security and privacy.

SaINT analyses the source code of an IoT app, identifies sensitive data from a taint source, and attaches taint labels that describe sensitive data's sources and types. It then performs static taint analysis that tracks how labelled data (source data, e.g., camera image) propagates in the app (sink, e.g., network interface). Finally, it reports cases where sensitive data transmits out of the app at a taint sink such as through the Internet or some messaging service. In a warning report, SaINT states the source in the taint label and the details about the sink, such as the external URL or the phone number. The implementation section of this paper will present evidence of using SaINT for the purpose of measuring the privacy riskiness of IoT devices and storing this information in the IPRR.

6.2 Privacy Mediator VM

The IoTAware system includes a privacy mediator VM (Virtual Machine) associated with each camera feed. This VM's architecture is shown in Figure 4, and its principal task is to carry out selective denaturing of the video before it is stored or made available for analytics. Privacy mediator VMs run on cloudlets located near the cameras, typically connected by wired networks with high-bandwidth. A cloudlet may host multiple privacy mediator VMs. Further, depending on the size of the implementation, there can be multiple cloudlets each serving multiple cameras in an area.

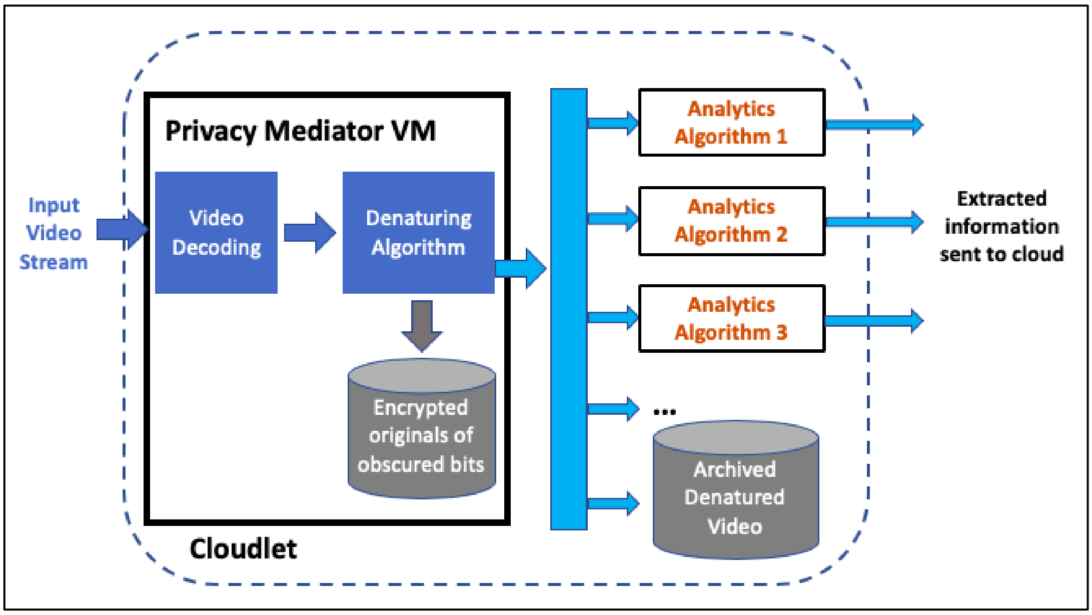


Figure 4. Architecture for the Privacy Mediator and Live Video Analytics.

6.2.1 RTFace and Denaturing

Denaturing involves content-based modification of images or video frames which, in this case, administers a privacy policy. Given the IoT facial recognition scenario focuses on a service using live video analytics, this paper's solution must denature real-time video at full frame rate. RTFace is one such denaturing framework available (https://github.com/cmusatyalab/rtface) that selectively blurs a user's face based on their identity in real-time to protect the user's privacy. The framework leverages object tracking to achieve real-time while running face detection using dlib, and face recognition using OpenFace. OpenFace (https://cmusatyalab.github.io/openface/#openface) is a Python and Torch implementation of face recognition with deep neural networks and is based on the CVPR 2015 paper FaceNet: A Unified Embedding for Face Recognition and Clustering (Schroff, Kalenichenko and Philbin, 2015).

Wang et al. (2017) compare OpenFace to Eigenfaces (Turk and Pentland, 1991), Fisherfaces (Belhumeur, Hespanha and Kriegman, 1997) and LBPH (Ahonen, Hadid and Pietikainen, 2006) and find that OpenFace has the highest face identification accuracy by a large margin, and its accuracy falls off slowly as the number of faces increases from 10 to 100. Further, Wang et al. (2017) also find that the recognition speed for a single face with OpenFace is roughly 80 Ms without a GPU, dropping to roughly 20 Ms with a high-end GPU, thus making it competitive compared to alternative frameworks.

6.3 IoT Camera Setup

IoT cameras recognised in the IoTAware system are assumed to connect through a high-bandwidth, wired network. In collaboration with IoT technology providers, each IoT camera is to be configured to continuously generate and send a compressed video stream to only its accompanying privacy mediator VM. A Bluetooth low energy (BLE) beacon residing with each camera will also broadcast camera-specific information. This fulfils a number of purposes. First, the electronic signal can trigger nudges to inform individuals in the vicinity that their biometrics are being captured. This beacon can be received by any modern smartphone or wearable device that supports BLE. Secondly, the beacon includes information about the camera and a URL to the IPRR responsible for the particular camera network. This acts as a discovery mechanism for each unique IoT device, thus allowing many different camera networks to function in overlapping areas. Finally, the range of the BLE beacon is approximately a dozen of meters, this radius is similar to the typical viewing range of surveillance cameras, therefore, this can act as a means to determine which camera(s) are observing the user.

6.4 Face Trainer

For a user's privacy settings to be enforced, the user's face needs to be recognisable by the system. In other words, if a user opts-out of all permissions requested by the IoT facial recognition device, the system needs to know whose face to obfuscate. OpenFace can achieve accurate recognition by using just 20 training images per person (Wang et al., 2017). After downloading IoTAware, users are asked to send 20 images of their face for training, as shown in Figure 6. The captured images are transmitted to the web training sever via the secure WebSocket protocol. For each face detected in training images, the training web server then extracts a 128-dimensional feature vector using OpenFace and stores it into a global database. At runtime, these feature vectors are retrieved by the privacy mediator VM when a user enters into the range of a camera.

A complete deployed system for training and storing feature vectors will need to address a few additional security concerns. Most importantly, requests for a feature vector from the IoTAware application need to be properly authenticated and authorised. This can be implemented using OAuth 2.0 user authentication (see Figure 5). OAuth 2.0 is the industry standard-standard protocol for authentication (OAuth.net, 2020) and allows a user of IoTAware to authenticate themselves using their Facebook, Google or other supporting company's log-ins. Subsequently, before using the IoTAware application, and uploading their biometric data, users are asked to sign-in (see Figure 6.A) using their Gmail account. The user's email address is then used as an identifier to process setting requests made by IoTAware.

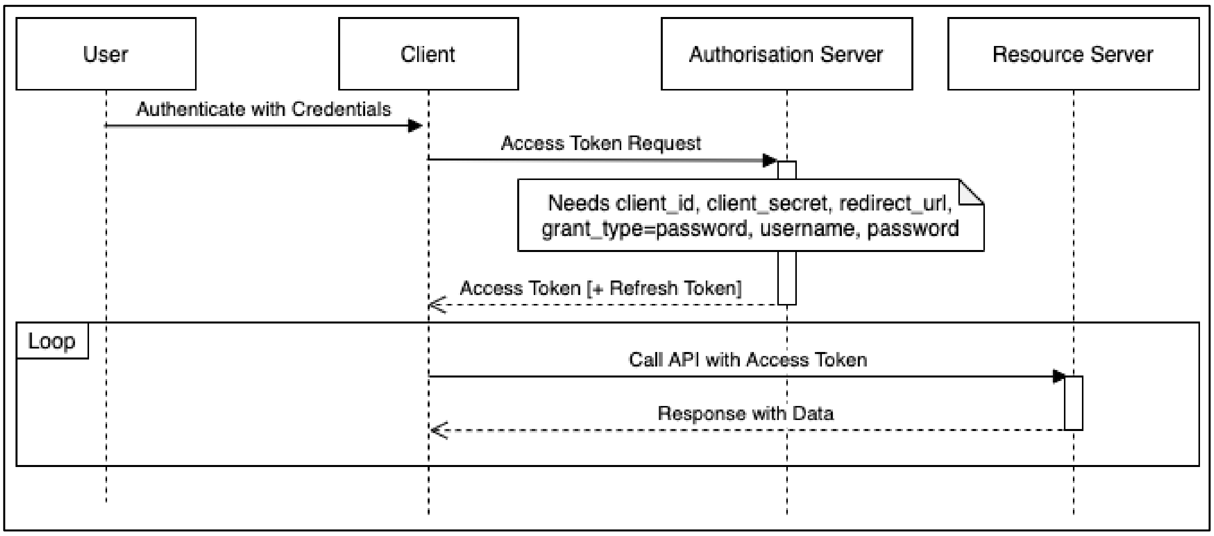
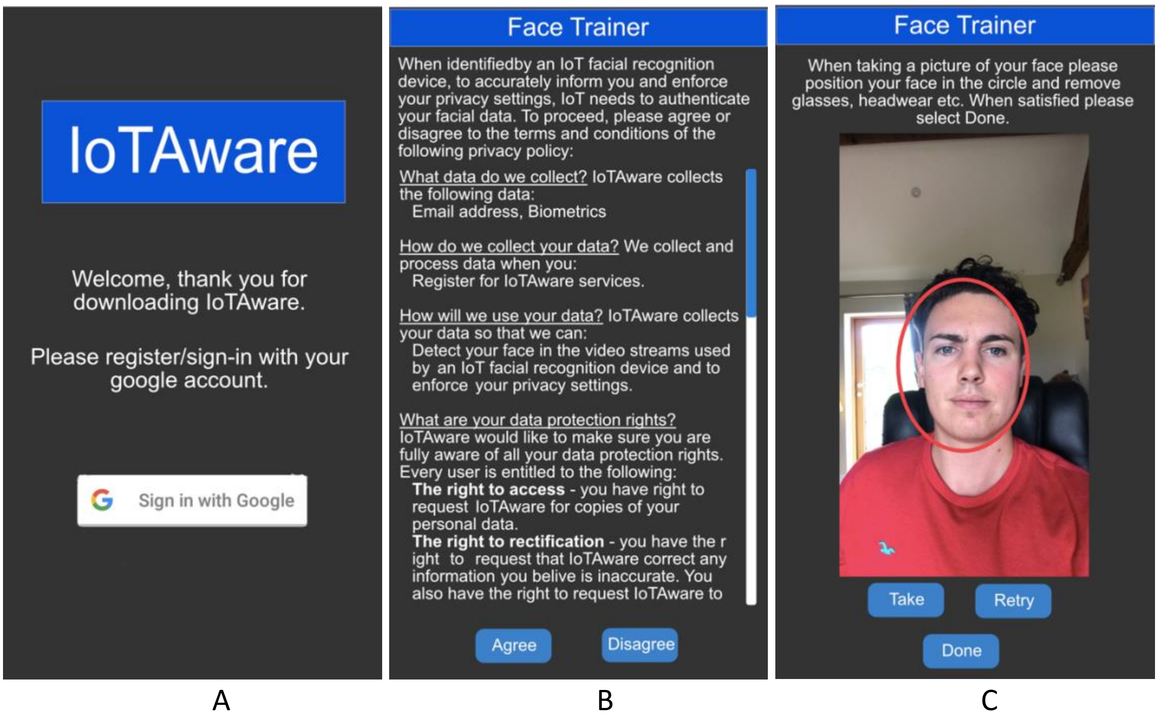

User
Client
Authorisation Server
Resource Server
Authenticate with Credentials
Access Token Request
Needs client_id, client_secret, redirect_url, grant_type=password, username, password
Access Token [+ Refresh Token]
Loop
Call API with Access Token
Response with Data

Figure 5. Sequence diagram illustrating the flow of user authentication.



Welcome, thank you for downloading IoTAware.

Please register/sign-in with your google account.

When identifiedby an IoT facial recognition device, to accurately inform you and enforce your privacy settings, IoT needs to authenticate your facial data. To proceed, please agree or disagree to the terms and conditions of the following privacy policy:

What data do we collect? IoTAware collects the following data:
Email address, Biometrics

How do we collect your data? We collect and process data when you:
Register for IoTAware services.

How will we use your data? IoTAware collects your data so that we can:
Detect your face in the video streams used by an IoT facial recognition device and to enforce your privacy settings.

What are your data protection rights? IoTAware would like to make sure you are fully aware of all your data protection rights. Every user is entitled to the following:
The right to access - you have right to request IoTAware for copies of your personal data.
The right to rectification - you have the r ight to request that IoTAware correct any information you belive is inaccurate. You also have the right to request IoTAware to

When taking a picture of your face please position your face in the circle and remove glasses, headwear etc. When satisfied please select Done.

Figure 6. Design of user authentication and Face Trainer sections of the IoTAware interface.

7 Performance Analysis

In terms of performance, the Privacy Mediator and PSIP are the most critical two components in the system's infrastructure. Therefore, this section focuses on analysing the potential performance of these two components and serves to inform the design and build of the solution.

7.1 Accuracy and Scalability of Privacy Mediator

Denaturing faces from a large collection of users will be challenging to both the scalability and accuracy of the Privacy Mediator. In the context of a large-scale, such as city-wide, deployment, the total number of individuals to be recognised will be significantly higher. However, even though the total user population may be large, the number of people captured by a camera at any given time is limited. Therefore, by sending beacons to IoTAware when a user enters the proximity of the IoT device, it reduces the number of potential candidates that the Privacy Mediator has to identify.

The Privacy Mediator can be evaluated by calculating the time it takes to recognise users when the number of users ranges from 10 to 100. In their performance analysis of OpenFace, Wang et al. (2017) find that increases in recognition time from 10 to 100 individuals is minimal relative to the execution time of the neural network. Further, the training time for up to 100 new faces only requires a few tenths of a second.

Wang et al. (2017) also analyse the maximum processing speed of RTFace when allocating one core per camera. The analysis used 2300 frames from a 1920x1080 (HD) video that contains multiple faces, with twenty individuals in the system and almost five people present in a single frame. When running on a 1-core 3GB RAM VM, RTFace ran at five-times the speed of a second alternative – Downsample, and eight-time that of a third alternative – Baseline. Overall, the 48.7 Ms processing time for RTFace indicates it can withstand a speed of just over 20 FPS at HD resolution.

7.2 Scalability of PSIP

Considering that the PSIP (privacy settings implementation point) entity may be supporting a large number of users and a wide variety of settings, for successful future implementation of IoTAware, it's important to consider how well the PSIP performs as the number of users increases. Currently, the PSIP is designed to support three essential operations: (1) status request: returns the current status of a user's privacy setting; (2) opt in request: change a user's current permission setting to accept; (3) opt out request: change a user's current permission setting to decline.

Whenever a request is forwarded to the PSIP, it first verifies if the right user has sent the request. This verification step is done through OAuth tokens where the IoTAware app sends the user's Gmail address along an OAuth token to the PSIP. The PSIP then forwards the OAuth token to Google's authentication sever. Google's authentication sever responds back with either a valid or invalid response. Depending on the response received from the Google authentication sever the PSIP finally responds with either a 'Successful' or 'Un-successful' message back to IoTAware.

For each request, the total service time can be separated into two parts: (1) Google authentication time and, (2) database query and update time. It is envisioned that IoTAware will use an SQLite database to store users' settings. To assess the scalability of the PSIP, future work should analyse the amount of time spent in each of these phases using mock users, valid OAuth tokens and three particular timestamps. At the beginning of processing the request, time t1 should be noted. Following authentication, time t2 is recorded, and finally time t3 is recorded before sending the response back IoTAware. With these times recorded, the operational time can be computed as follows:

- Time to authenticate Google token = t2 – t1
- Time to query and update database = t3 – t2
- Total time to process a request = t3 – t1

To perform this measurement, parallel status, and opt_in and opt_out requests need to be sent to the PSIP. To mimic a large number of users, the test should associate a random user id with each incoming request to the PSIP. Each user id should then generate a separate entry in the local database residing in the PSIP. For adequate scalability testing, user ids should be randomly generated. Further, for generating valid OAuth tokens, each outgoing request from PSIP should be randomly associated with a valid Gmail account. The results of this scalability test should aid future development of IoTAware by indicating how the average authentication time will change as the number of concurrent requests increases. However, it is important to note that this analysis would ignore the time it takes for a request to go from IoTAware to PSIP and vice versa as this latency various across Wi-Fi or 4G connections.

8 Implementation

This section will provide a high-level overview of this paper's realisation of the IoTAware and system design.

8.1 IPRR Measuring the Privacy Riskiness of IoT devices with SaINT

Celik et al. (2018) introduce IoTBench (https://github.com/IoTBench), a publicly available repository for testing their static taint analysis tool SaINT. Using IoTBench and the SaINT Analysis Console (http://saint-project.appspot.com/) this paper will use SaINT to carry out static analysis on some example IoT applications. This will demonstrate how SaINT will be used to measure the privacy riskiness of IoT devices stored in the IPRR, while also assessing the accuracy and effectiveness of SaINT.

Currently, SaINT is designed to analyse SmartThings IoT apps written in the Groovy programming language. Evaluating the SmartThings platform is relevant for this demonstration for two reasons. First, it supports the largest number of devices (142) among all IoT platforms and provides apps of various functionalities (SmartThings, 2020). Second, it provides thorough, publicly available guidance and documentation that helps validate findings. Nevertheless, with the highly-structured nature of the IoT programming platforms, the algorithms developed in SaINT can be integrated into a wide range of programming platforms written in different programming or domain-specific languages. The experiment started by obtained 40 official apps from the SmartThings GitHub repository (https://github.com/SmartThingsCommunity). Each app was then studied by downloading the source code and running an analysis with SaINT. In terms of performance, it took less than 3 minutes to analyse all 40 apps. The experiment was performed on a laptop computer with a 2.6GHz 2-core Intel i5 processor and 8GB RAM, using Oracle's Java Runtime 1.8 (64 bit) in its default settings. The average run-time for an app was 23±5 seconds.

8.1.1 Taint Tracking

Figure 8 is the analysis report from SaINT. These particular analysis results are from the source code (see Appendix item F) of sample IoT app 17 from the SmartThings GitHub repository.

```
Data Flow Path 1: send --> sendSms -->  phoneNumber -->  message
Data Flow Path 2: send --> sendSms -->  $onSwitches.size    -->
message
Data Flow Path 3: send --> sendSms -->  phoneNumber2 -->  message
…
Data Flow Path 37: send --> sendPush -->  msg  -->  message  -->
something
```

```
Finding #1: Potential leaking of User Input source through variable:
phoneNumber
Finding #2: Potential leaking of User Input source through variable:
message
Finding #3: Potential leaking of User Input source through variable:
phoneNumber2
Finding #4: Potential leaking of User Input source through variable:
phonenumber
Finding #5: Potential leaking of User Input source through variable:
recipients
Finding #6: Potential leaking of User Input source through variable:
7865014232
Finding #7: Potential leaking of User Input source through variable:
more
Finding #8: Potential leaking of User Input source through variable:
something
Finding #9: Potential leaking of Async API source 'head' through
variable: headers:
Finding #10: Potential leaking of Async API source 'head' through
variable: resp.headers.collect{
Finding #11: Potential malicious flow of sensitive data to the
following server: [uri:https://automated-lore-135923.appspot.com,
Finding #12: Potential malicious flow of sensitive data to the
following hard-coded number: 222-222-2222
Finding #13: Potential malicious flow of sensitive data to the
following hard-coded number: 111-111-1111
Finding #14: Potential malicious flow of sensitive data to the
following hard-coded number: 7865014232
Finding #15: Potential malicious flow of data through dynamic call
during runtime: '$newMode'
Finding #16: Potential malicious flow of data through dynamic call
during runtime:  $onSwitches.size

Summary of sinks found in this app:
Total times sending SMSs or messages: 4
Total times sending notifications: 2
Total times using internet: 2
```

Figure 8. Analysis Results of IoT app 17.

This analysis report by SaINT contains the following information: (1) full data flow paths between taint sources and sinks, (2) the taint labels of potential sensitive data leaks, (3) the potential malicious flows of data or sensitive data, and (4) a summary of taint sink information. This particular analysis reveals different parameters are obtained from device objects and user inputs are leaked via several sinks. In line 123 of the source code (see Appendix item F) a state variable is declared with the information of device status. In line 124, a local variable is declared with the number of on active switches. In line 175 and line 177, two variables are declared consisting device ID and Hub ID respectively. All these variables consist sensitive information and are leaked via SendSms and SendNotification from line 181 to 200.

8.1.2 Data Flow Analysis (Taint Source Analysis)

Using SaINT to analyse 40 example IoT apps, SaINT flagged all 40 apps to have explicit “sensitive” data flow paths from taint sources to taint sinks. SaINT automatically classifies each data flow into a set of sensitive data taint labels, which precisely describe what sources the data comes from. These are:

1. Device States: are the attributes of a device. An IoT app can acquire a variety of privacy-sensitive information through device state interfaces.
2. Device Information: IoT apps grants access to IoT devices at install time. Our investigations reveal the platforms often define interfaces to access device information such as its manufacturer name, id, and model. This allows a developer to write device-specific apps.
3. Location: In the IoT domain, location information refers to a user’s geolocation or geographical location. SaINT refers location information to a user’s geolocation or geographical location. Geolocation defines a virtual property such as a garage or an office defined by a user to control devices in that location. Geographical location is used to control app logic through time zones, longitudes, and latitudes.
4. User Inputs: IoT apps often require user inputs of personal information to enable certain functionality, manage app logic or to control devices, such inputs are sensitive since they contain personally identifiable data and may be used to profile user behaviour.
5. State Variables: IoT apps do not store data about their previous executions. To retrieve data across executions, platforms allows apps to persist data to some propriety external storage and retrieve this data in later executions.

(Celik et al., 2018)

IoT app	1	2	3	4	5
1	■		🟦		
2		■	🟦		
3		■	🟦		
4		■	🟦		
5		■	🟦		
6		■	🟦		
7		■	🟦		
8		■	🟦		
9			🟦		
10	■	■	🟦		■
11	■	■	🟦		■
12	■	■	🟦		■
13	■	■	🟦		■
14	■	■	🟦		
15	■	■	🟦		
16	■	■	🟦		
17	■	■	🟦		
18			🟦	■	■
19			🟦	■	■
20				■	
21	■	■			
22	■	■			
23	■	■			
24	■	■			
25	■				
26	■				
27	■				
28				■	
29	■	■			
30	■	■			
31	■	■			
32	■	■			■
33	■				■
34	■				■
35	■				■
36	■	■			
37	■	■			
38	■	■			
39	■	■			■
40	■	■			

1 = Device State
2 = Device Information
3 = User Input
4 = Location
5 = State Variable

Table 3. Data flow behaviour of the 40 IoT apps.

From SaINT’s analysis results of 40 example IoT apps, Table 3 characterises sensitive data flows by the type of taint source. This shows that 19 out of the 40 apps have user input information flows, the other 21 apps have flows sourcing from a combination of device state, device information, device location and state variables. Given IoTAware’s focus on ensuring users have better awareness and control of the collection, storage and processing of their personal data, user input is the only real taint source that is representative of personal data. Therefore, IoTAware will classify IoT devices with user input data flows as a potential risk to users and register them in the IPRR.

8.1.3 Calculating the Privacy-risk Score

Of the IoT devices that have user input data flows, their privacy riskiness will be scored across the four CFIP constructs (collection, unauthorised secondary use, improper use and errors). The information from SaINT analysis reports of these IoT apps (e.g. Figure 8), will be fed into a database table (see Table 4) in the IPRR and the IoT device's (app's) privacy risk score for the relevant CFIP construct will be calculated as follows:

1. Collection. The privacy risk score of personal data collection will be scored based on the number of data flow paths. This represents the number of data flows between taint sources and sinks and represents the extent, beyond the point of collection, to which an individual's personal information is used by an IoT vendor. Therefore, the more data flows than average, the greater the risk of a user allowing personal data collection.
2. Unauthorised Secondary Use. The privacy risk score of unauthorised secondary use will be calculated based on the number of potential leaks of user input sources. The higher the number of potential leaks, the greater the risk of personal data being disclosed to unauthorised parties.
3. Improper Use. The privacy risk score of improper use will be calculated based on the number of potential malicious flows of data. If the number of potential malicious data flows is higher than average, this increases the risk of personal data being wrongfully used.
4. Errors. Designed as a taint analysis tool, SaINT analysis reports cannot measure errors in personal data. Instead, other tools integrity checking tools, version checks provide a more accurate measure of accuracy in personal data. However, this is a scope for future work, and for demonstrative purposes, the privacy risk score of errors will be calculated based on the average privacy risk score of potential leaks and potential malicious flows of data combined. This is based on the principle that primary IoT vendors cannot ensure unauthorised third-party's abidance of data accuracy practices and malicious data flows make data vulnerable to wrongful modification or loss.

Device			
id	**Flow_paths**	**Potential_leaks**	**Malicious_flows**
1	7	6	3
2	5	3	4
3	5	3	1
4	5	3	3
5	10	0	3
6	3	0	2
7	7	6	1
8	7	4	1
9	7	4	2
10	5	3	2
11	5	1	3
12	6	1	3
13	5	1	2
14	6	4	4
15	9	3	3
16	11	5	4

17	37	8	6
18	0	0	0
19	6	0	2

Table 4. Database table containing analysis for 19 IoT apps with user input data flows.

Using the data within table 4, the following algorithm, written in Java, will be used to calculate the privacy risk score for each CFIP construct. After finding the minimum and maximum values of each construct data (flow_paths, potential_leaks, malicious_flows), the range can be established. To set the boundaries for low, medium and high privacy risk, each construct's range of data is divided by three. Each device's is classified as low, medium and high risk as follows: (1) a device with a value below 1/3 of the construct's range is low risk, (2) a value below 2/3 of the construct's range is medium risk, and (3) a value above 2/3 of the construct's range is high risk.

```
private int flow_paths;
private int potential_leaks;
private int malicious_flows;


//Finding the highest and lowest number of flow paths
for (int i = 1; i < device.size(); i++) {
    Device d = device.get(i);
    if (d.getFlow_paths() > dMax.getFlow_paths()) {
        dMax = d;
        maxFlow_paths = dMax.getFlow_paths();
    }
}
for (int i = 1; i < device.size(); i++) {
    Device d = device.get(i);
    if (d.getFlow_paths() < dMin.getFlow_paths()) {
        dMin = d;
        minFlow_paths = dMin.getFlow_paths();
    }
}


//Finding low, medium and high risk boundaries
int lowerFlow_Paths = (dMax.getFlow_paths() - dMin.getFlow_paths()) / 3;
int medFlow_Paths = lowerFlow_Paths * 2;
```

```
//Calculates collection risk for device 1
int flow_paths1 = device.get(0).getFlow_paths();
if (flow_paths1 <= lowerFlow_Paths) {
   System.out.println("Device 1 has low Collection risk");
}
if (flow_paths1 > lowerFlow_Paths && flow_paths1 < medFlow_Paths){
   System.out.println("Device 1 has medium collection risk");
}
if (flow_paths1 >= medFlow_Paths){
   System.out.println("Device 1 has high collection risk");
}
```

Algorithm 1. Algorithm to determine a device’s privacy scores for each CFIP construct.

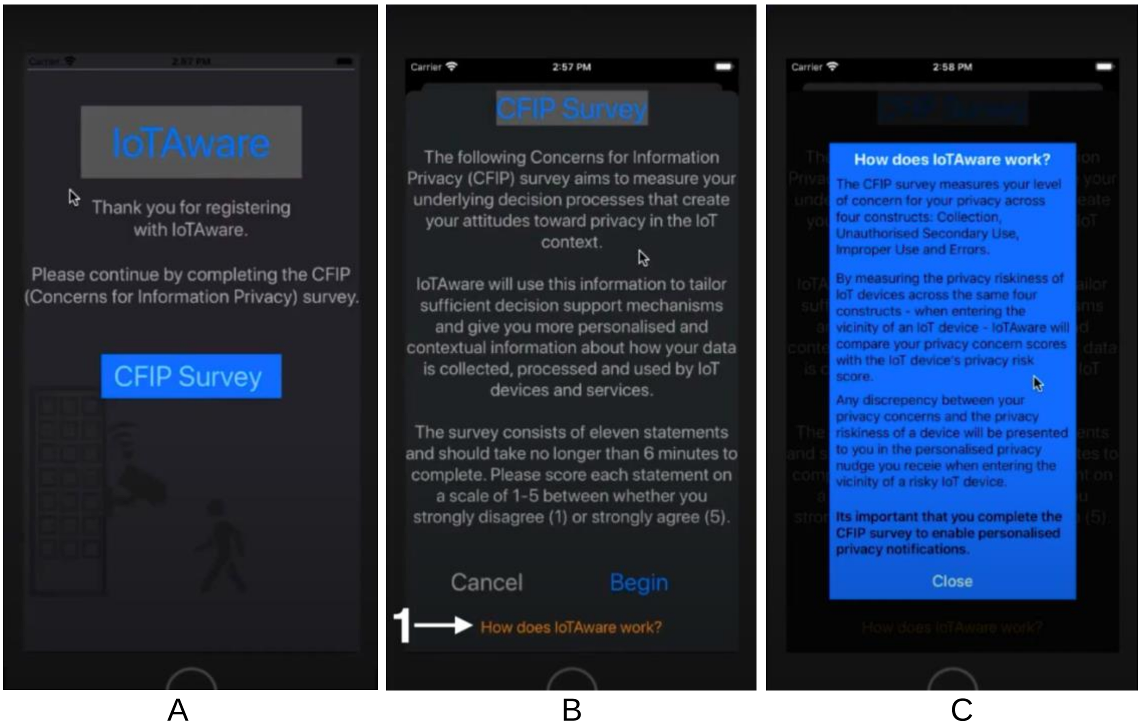
The algorithm is implemented as part of the code of the ‘Device’ Java class (see Appendix item G). The purpose for this class is to run the algorithm and calculating the privacy risks scores of each IoT device across three CFIP constructs (Collection, Unauthorised Secondary Use and Improper Use).

8.2 The Prototype IoTAware Interface

A prototype interface of IoTAware was developed to simulate IoTAware for the purpose of experimentation. The prototype was developed in the Swift programming language using Xcode as the Integrated Development Environment (IDE). Swift was chosen for the development of the prototype interface because it is fast and efficient language, it is 2.6x faster than Objective-C, 8.4x faster than Python 2.7 (Apple, 2020) and provides real-time feedback. Xcode was chosen as the IDE as it complements Swift in bringing user interface design, coding, testing, debugging, and submitting to the App Store all into a unified workflow.

The complete code for the prototype interface can be found within the project folder. The code is split between two projects, the first is of the pre-notification stages of using IoTAware, including completion of the CFIP survey, and the second project focuses on receiving a personalised privacy notification and facilitating user-driven privacy control. Screengrabs of the prototype interface are demonstrated below (see Figure 9). In the field of user experience, cognitive load (Paas et al. 2003) is the mental processing power needed to use an interface. If an interface provides too much information at once, it may exceed the user's ability to process it, the cognitive load is therefore too high and the overall performance suffers. To minimise cognitive load and improve comprehension, it is essential to reduce clutter by reducing any information that isn’t absolutely necessary. This was done through number of design choices. For instance, the content of the privacy report in the initial design (see Figure 2.G) is text based and approximately 150 words in length. Given a mobile UI has limited space, text content of this length is likely to appear cluttered. Instead, visual representations can help users understand data quicker than text. Therefore, to present the user with only what they need to know, bar graphs (see Figure 9.J-K) represent the juxtaposition of users' privacy attitudes toward IoT technologies and the privacy riskiness of such IoT devices.

To further minimise cognitive load, the options for the privacy control settings (see Figure 9.L) were kept simple. Through selecting "Obscure my face", users can blur their face on the IoT camera's real-time video feed and prevent their sensitive personal data being collected, processed or used, all by choosing this single option. By having simple control options which are supported by the underlying system, as opposed to being generic to all types of IoT sensors, it prevents presenting users with too many settings options or a 'wall of checkboxes' (Good, 2012), which overwhelm users. Further, as according to Apple's iOS Human Interface Guidelines (2020), switches were implemented as a visual toggle between opting-in or opting-out of privacy setting options, this allowed users to visualise which settings were active so that settings aren't mistakenly applied. In terms of testing the prototype interface, evidence of unit tests on the functionality of the Likert scale feature of the interface can be found in appendix item J.



IoTAware

Thank you for registering with IoTAware.

Please continue by completing the CFIP (Concerns for Information Privacy) survey.

CFIP Survey

CFIP Survey

The following Concerns for Information Privacy (CFIP) survey aims to measure your underlying decision processes that create your attitudes toward privacy in the IoT context.

IoTAware will use this information to tailor sufficient decision support mechanisms and give you more personalised and contextual information about how your data is collected, processed and used by IoT devices and services.

The survey consists of eleven statements and should take no longer than 6 minutes to complete. Please score each statement on a scale of 1-5 between whether you strongly disagree (1) or strongly agree (5).

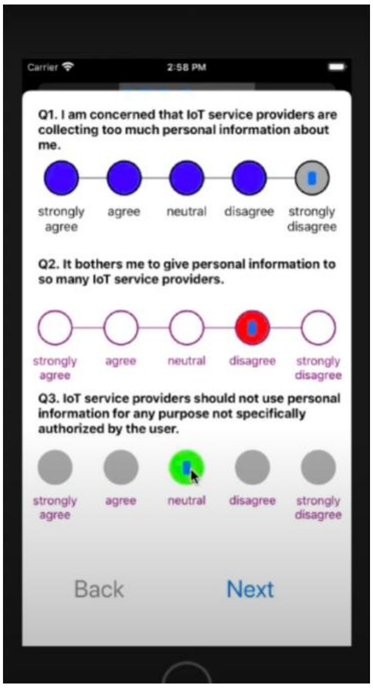
How does IoTAware work?

The CFIP survey measures your level of concern for your privacy across four constructs: Collection, Unauthorised Secondary Use, Improper Use and Errors.

By measuring the privacy riskiness of IoT devices across the same four constructs - when entering the vicinity of an IoT device - IoTAware will compare your privacy concern scores with the IoT device's privacy risk score.

Any discrepency between your privacy concerns and the privacy riskiness of a device will be presented to you in the personalised privacy nudge you receie when entering the vicinity of a risky IoT device.

Its important that you complete the CFIP survey to enable personalised privacy notifications.



Q1. I am concerned that IoT service providers are collecting too much personal information about me.

strongly agree · agree · neutral · disagree · [✓ strongly disagree]

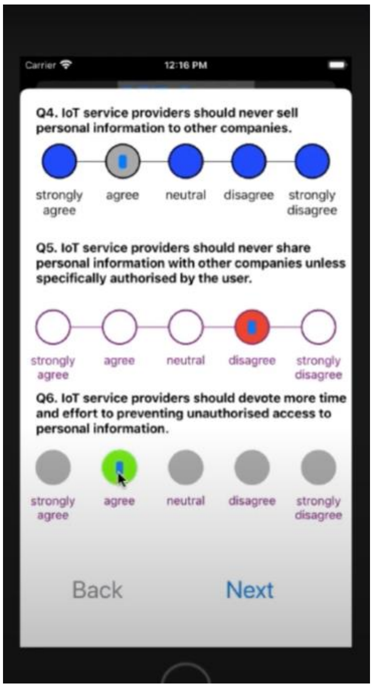
Q2. It bothers me to give personal information to so many IoT service providers.

strongly agree · agree · neutral · [✓ disagree] · strongly disagree

Q3. IoT service providers should not use personal information for any purpose not specifically authorized by the user.

strongly agree · agree · [✓ neutral] · disagree · strongly disagree

D



Q4. IoT service providers should never sell personal information to other companies.

strongly agree · [✓ agree] · neutral · disagree · strongly disagree

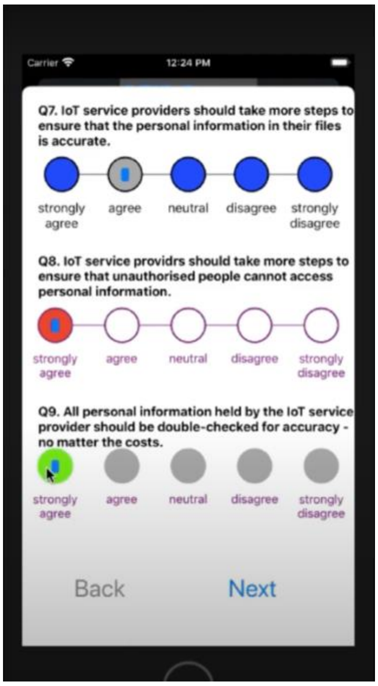
Q5. IoT service providers should never share personal information with other companies unless specifically authorised by the user.

strongly agree · agree · neutral · [✓ disagree] · strongly disagree

Q6. IoT service providers should devote more time and effort to preventing unauthorised access to personal information.

strongly agree · [✓ agree] · neutral · disagree · strongly disagree

E



Q7. IoT service providers should take more steps to ensure that the personal information in their files is accurate.

strongly agree · [✓ agree] · neutral · disagree · strongly disagree

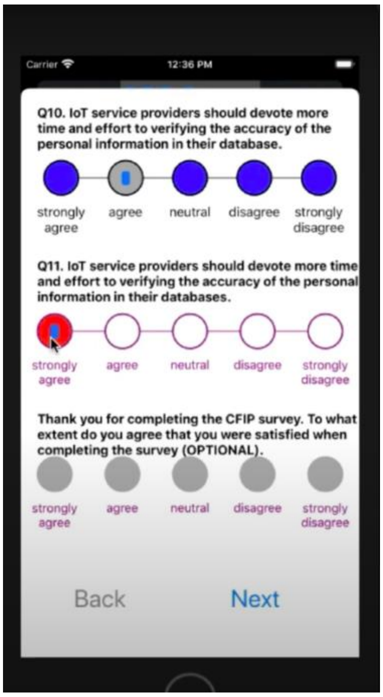
Q8. IoT service providrs should take more steps to ensure that unauthorised people cannot access personal information.

[✓ strongly agree] · agree · neutral · disagree · strongly disagree

Q9. All personal information held by the IoT service provider should be double-checked for accuracy - no matter the costs.

[✓ strongly agree] · agree · neutral · disagree · strongly disagree

F



Q10. IoT service providers should devote more time and effort to verifying the accuracy of the personal information in their database.

strongly agree · [✓ agree] · neutral · disagree · strongly disagree

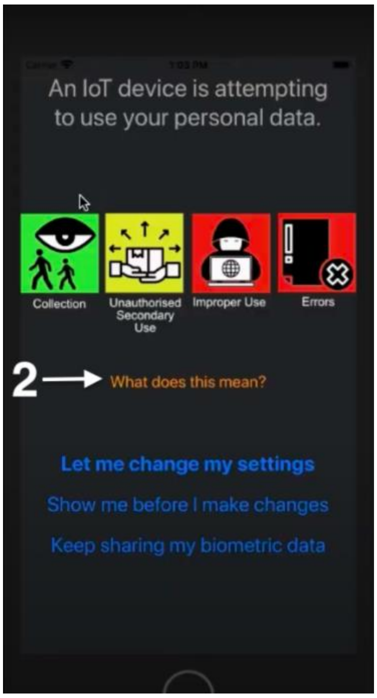
Q11. IoT service providers should devote more time and effort to verifying the accuracy of the personal information in their databases.

[✓ strongly agree] · agree · neutral · disagree · strongly disagree

Thank you for completing the CFIP survey. To what extent do you agree that you were satisfied when completing the survey (OPTIONAL).

strongly agree · agree · neutral · disagree · strongly disagree

G


An IoT device is attempting to use your personal data.

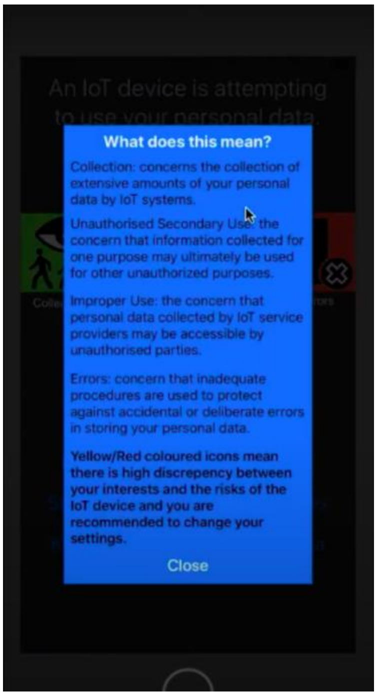
What does this mean?

Let me change my settings

Show me before I make changes

Keep sharing my biometric data

H


What does this mean?

Collection: concerns the collection of extensive amounts of your personal data by IoT systems.

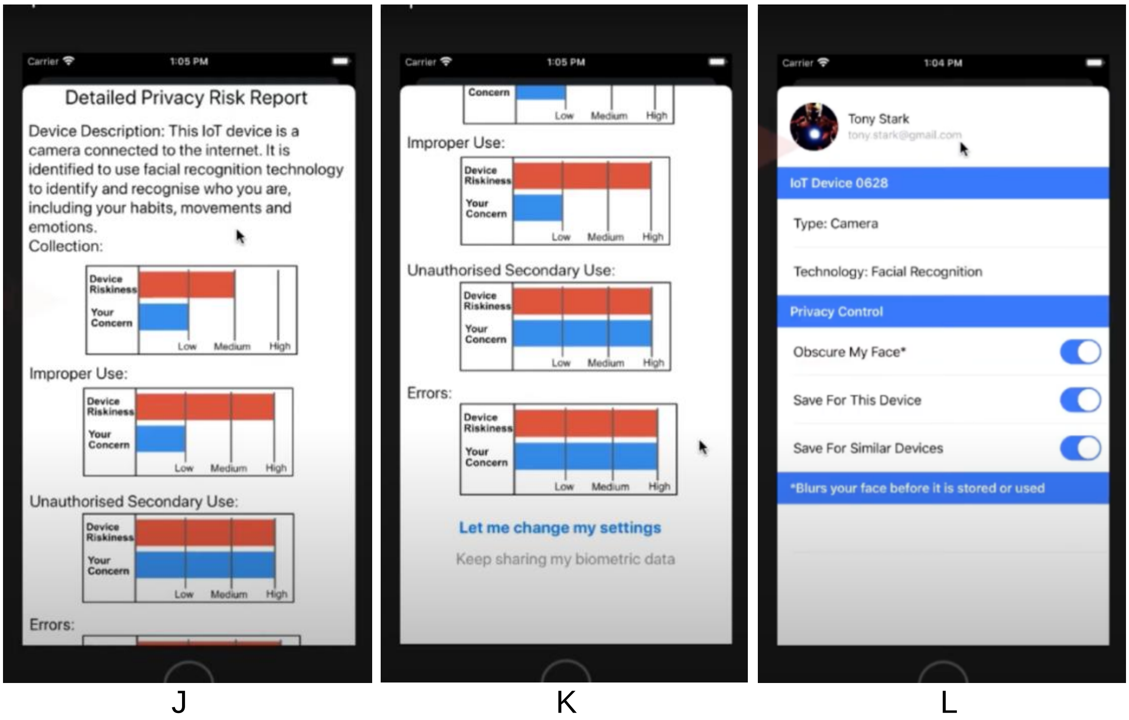
Unauthorised Secondary Use: the concern that information collected for one purpose may ultimately be used for other unauthorized purposes.

Improper Use: the concern that personal data collected by IoT service providers may be accessible by unauthorised parties.

Errors: concern that inadequate procedures are used to protect against accidental or deliberate errors in storing your personal data.

Yellow/Red coloured icons mean there is high discrepency between your interests and the risks of the IoT device and you are recommended to change your settings.

I



Detailed Privacy Risk Report

Device Description: This IoT device is a camera connected to the internet. It is identified to use facial recognition technology to identify and recognise who you are, including your habits, movements and emotions.

Collection:

Improper Use:

Unauthorised Secondary Use:

Errors:

Tony Stark
tony.stark@gmail.com

IoT Device 0628

Type: Camera

Technology: Facial Recognition

Privacy Control

Obscure My Face* ●

Save For This Device ●

Save For Similar Devices ●

*Blurs your face before it is stored or used

Figure 9. Screengrabs of the IoTAware interface.

9 Experimental Study

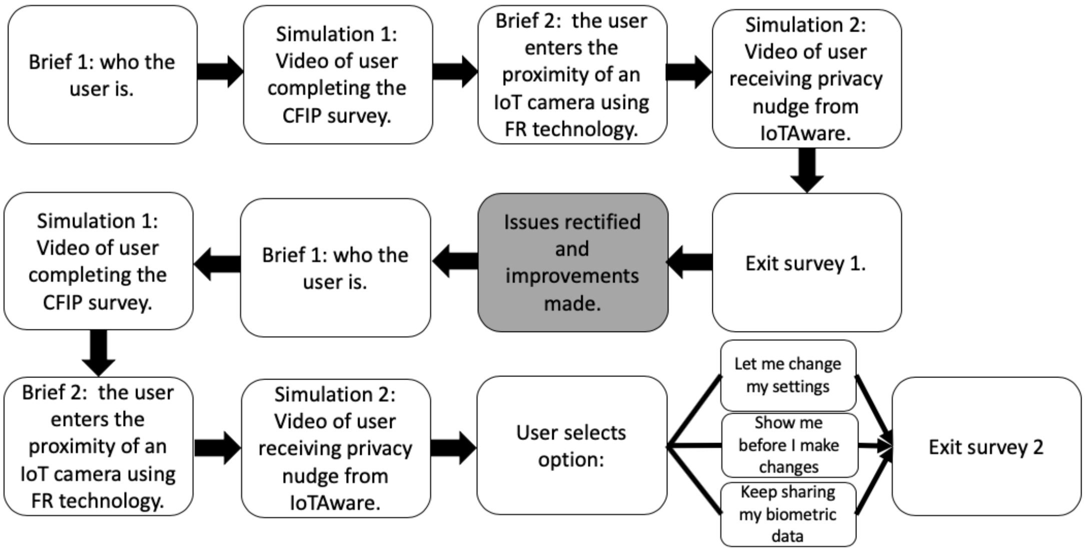
This evaluation assesses the effectiveness of the IoTAware privacy awareness and control interface in meeting its requirements (see section 4). The study was granted ethical approval by Aston University and conducted two online experiments beginning in July 2020. The study recruited fellow students and friends as participants and provided them with a hyperlink to the first experiment's Google form, followed by hyperlink to the second experiment's Google form a week later. No personal details were requested as responses were anonymised. A total of 10 participants completed the first online experiment and 11 participants completed the second online experiment.

9.1 Study Design

The user study comprised two online experiments. The aim of the first experiment was to evaluate how effectively IoTAware makes users aware of the collection, storage and processing of their personal data by an IoT device. It is believed that IoTAware can provide sufficient awareness, therefore, the first experiment will measure usability when completing the CFIP survey and the user comprehension and accuracy of the personalised privacy nudge. The aim of the second experiment is to evaluate how effectively IoTAware influences informed decision making and allows users to control the collection, storage and processing of their personal data by an IoT device. It is believed that IoTAware's privacy discrepancy approach is effective at nudging users to control their privacy in line with their privacy attitudes. Therefore, the second experiment will measure how IoTAware influences users to change their privacy settings and whether users can make the necessary changes to improve their privacy. The designs of both experiments were informed by social distancing. In an ideal environment, experiments would have involved users being given the IoTAware interface on a physical device in a physically-simulated environment. instead both experiments present video walkthroughs, showing a user interacting with the IoTAware system. When conducting the experiment, participants were instructed to reason about how they saw the user interact with IoTAware. After the simulations, participants were then asked to complete an exit survey, designed to investigate their reasoning during the experiment.

9.2 Experiment Procedure

Figure 10 outlines the sequence of tasks users were asked to complete in the first and second online experiment.



Brief 1: who the user is.
Simulation 1: Video of user completing the CFIP survey.
Brief 2: the user enters the proximity of an IoT camera using FR technology.
Simulation 2: Video of user receiving privacy nudge from IoTAware.
Exit survey 1.
Issues rectified and improvements made.
Brief 1: who the user is.
Simulation 1: Video of user completing the CFIP survey.
Brief 2: the user enters the proximity of an IoT camera using FR technology.
Simulation 2: Video of user receiving privacy nudge from IoTAware.
User selects option:
Let me change my settings
Show me before I make changes
Keep sharing my biometric data
Exit survey 2

Figure 10. Workflow of the study.

First Online Experiment: The first experiment's scenario's, video simulations and exit survey questions are shown in appendix item C. At the beginning of the first experiment, participants were briefed with a scenario explaining the role of the simulated user. Participants were then shown a video of the user filling in the CFIP survey on the IoTAware interface, the video includes captions describing the actions of the user and IoTAware. A second scenario then explained the user's role in triggering the privacy nudge and also some information about the IoT system (e.g., what data is being collected and for what purpose). Participants were then shown a second video simulation of the user receiving the privacy nudge along with captions explaining the meaning of the privacy icons and their colouring. Participants were finally directed to complete an exit survey in the Google form. Here, users were asked Likert-scale and open-ended questions about the interface, such as whether they understood the meaning of the privacy icons, and where also asked three questions from the Systems Usability Scale (SUS) (see Appendix item E), an instrument for measuring usability.

***Second Online experiment**:* After the results of the first experiment had been analysed and adjustments were made to IoTAware, participants were then provided with a hyperlink to the second experiment's Google form. The second experiment's video simulations used the improved interface and followed the same procedure and scenarios as the first experiment. However, additional steps were added to evaluate the effectiveness of the interface in influencing user-driven privacy control. This time, after being shown the video simulation receiving and opening the privacy nudge, users were instructed to make a decision on whether they thought the user should choose (a) "Let me change my settings" to change their settings, (b) "Show me before I make changes" to view a detailed privacy risk report or (c) "Keep sharing my biometric data" to keep sharing their data. Depending on which nudge response option the user chose, users were then shown a video of that option being followed-through. Upon completing the simulation, users were asked to complete a final exit survey (see Appendix item D). Here users were asked Likert-scale and open-ended questions about the interface, such as whether they adjusted some or all of the permission settings, and were also asked the same three SUS questions as in exit survey 1.

9.3 Limitations

As this paper explores a new approach of personalised privacy awareness and control in the IoT, its work inevitably has limitations. Firstly, this paper does not claim its results can be generalized to precisely represent IoT users' behaviours in the real world. This is since there wasn't the resources to build nor modify an IoT device using facial recognition technology. Instead, the online experiments were limited to one IoT device simulated in a hypothetical scenario. Subsequently, participants were asked to watch videos of a user using the IoTAware application, to reason about how they saw the user interact with the system and to make decisions of whether the user should change the permission settings for the device or keep sharing their biometric data.

Despite these limitations in organic validity and thus generalisability, the quantitative and qualitative results suggest the privacy discrepancy approach has the potential to more effectively give users awareness and control of the collection, storage and processing of personal data within IoT systems, more so than other approaches. This paper applied sanity checks to ensure participants took each task seriously and joined data from different sources (e.g., behavioural data, such as the nudge response option users choose, and qualitative data from the exit survey) in its analysis to ensure the reliability of findings. For instance, quantitative data suggests participants did take the nudge response choice tasks seriously and selectively chose and rejected options while explaining and justifying their reasoning.

9.4 Results

The full results of both online experiments can be found in appendix item L and M respectively. Important elements of the results include:

Completing the CFIP survey**:** completing the CFIP survey is important to measure the underlying privacy attitudes of users in the IoT context. During the experiment, each participant was shown a video of the user completing the CFIP survey. The first experiment revealed 70% of participants agreed that completing the CFIP survey would be straightforward*.* This suggests that IoTAware captures the underlying privacy attitudes of users in the IoT context in an uncomplicated and easy to do or understand manner. Of the remaining 30% that didn't know or disagreed, feedback included that:

> *"Concepts (of the CFIP survey) may need to be further explained to those who aren't as familiar with tech to make it completely accessible"* and *"Easy to answer, seems lengthy though and some questions seem to repeat themselves".*

To address this feedback, following the first experiment, the button "How does IoTAware work?" (see Figure 9.B.1) was added in the CFIP introduction page. When pressed, the button opens a pop-up view which describes the general concept of IoTAware and the function of the CFIP survey. More specifically, it mentions how the CFIP survey measures privacy concern across four constructs, and how these scores are compared with the privacy risk scores of an IoT device in order to highlight discrepancies.

***Influence on Decision Making*:** Influencing users to make a decision is important in allowing users to achieve meaningful notice and consent to privacy agreements and preventing the privacy paradox. All (100%) of participants who saw the privacy icons and/or privacy risk report agreed that these icons and/or the report influenced their decision to change their settings (see figure 11). Communicating privacy risk was the main goal of the privacy nudges and privacy risk report, and this appears to have been achieved. When asked why the privacy nudge and/or report influenced them to change their settings, users commented:

> *"The nudge makes it clear that there is a risk and the user should take action"* and *"The report showed me the extent of the discrepancy between the user's privacy concerns and the privacy riskiness of the device".*

This result shows that IoTAware effectively nudged users into modifying permissions to accurately reflect their level of privacy concern.

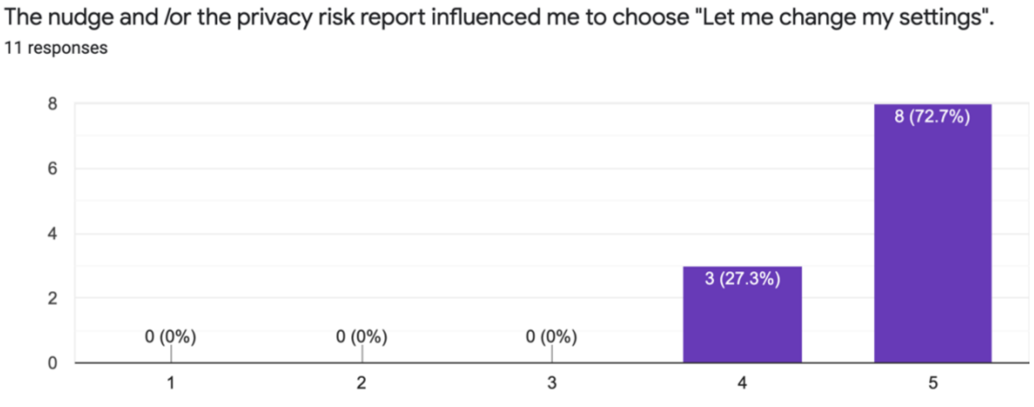


Figure 11. The nudge and/or the privacy risk report influenced me to choose "Let me change my settings".

To target users into making decisions to change the IoT device's permission requests, user responses to the privacy nudge are designed using a three-option approach, similar to the one used by Almuhimed et al. (2014). At the bottom of the nudge there are three options for users to respond to the privacy nudge they receive, these include "Let me change my settings", "Show me more before I make changes or "Keep sharing my [data]".

The "Let me change my settings" option opens the privacy permission settings page directly. Theoretically, by facilitating access to the permission settings

How did participants interact with the nudge? To target users into making decisions to change the IoT device's permission requests, it's important for IoTAware to facilitate access to the permission settings. As Figure 12 illustrates, when participants were asked which option the user should choose, participants responded by choosing "Let me change my settings" (36.4%) and "Show me before I make changes" (63.6%), no users chose "Keep sharing my biometric data". This finding suggests that IoTAware adequately highlighted the damages present in the non-favoured alternative ("Keep sharing my [data]").

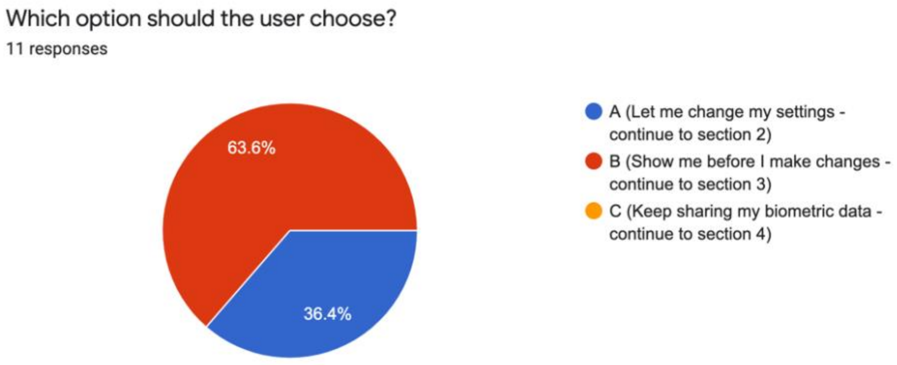


Figure 12. Which nudge options should the user choose?

Participants Understood the Privacy Discrepancy: To address inconsistencies between a user's actual privacy behaviour and their stated attitudes (the privacy paradox), it is important that the privacy nudge highlights any privacy discrepancy to the user. 90% of participants agreed the privacy nudge, including the colour of privacy icons, reflected the user's privacy beliefs (see Figure 13). To a similar extent, 60% of participants agreed that, based on the privacy nudge, the user would not be comfortable with the intrusion of the IoT device. Together with all participants correctly answering that "if an icon is red, there is a high level of discrepancy between the user's privacy concerns and the riskiness of the IoT device", it suggests that the majority of participants understood how the privacy nudge represents a high level of discrepancy between the user's privacy concern and the riskiness of the device. 36.4% of participants chose "Let me change my settings" after seeing the privacy nudge, they commented that:

> "*The nudge was clear enough"* and *"With red privacy icons, the nudge caught my attention and encouraged me to do something".*

This result suggests that by highlighting any privacy discrepancies, users were nudged toward making decisions to control their privacy in alignment with their privacy attitudes. During the first experiment, 30% of participants did not understand the actual meaning of each privacy icon. Feedback included suggestions for:

> *“Better explanation of the icons in more of a lay man’s terms”* and *“Suggestions on what to do next”.*

To address this feedback, a “What does this mean?” button (see Figure 9.H.2) was added to the privacy nudge and positioned below the privacy icons. When pressed, the button, opens a pop-up view, which describes the CFIP constructs and, based on the privacy discrepancy, gives the user a suggested course of action. The second experiment found that the added button with recommendations were helpful. 81.9% of participants in the second experiment agreed that the "What does this mean" option and suggestion on what to do next helped them make a decision.

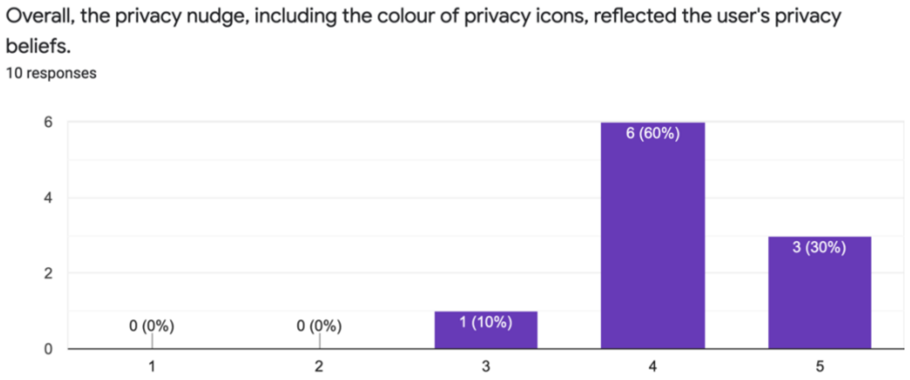


Figure 13. Overall, the privacy nudge, including the colour of privacy icons, reflected the user’s privacy beliefs.

The privacy risk report helped decision making: The privacy risk report is important to further highlight any mismatch between the user’s privacy concerns and the privacy risks of the IoT device. By choosing “Show me before I make changes”, 63.6% of participants viewed the detailed privacy risk report. Reasons for why participants thought the user should choose this option include

> *“To understand why the device is risk”* and *“To make a better/more information design”.*

All of the participants agreed that the report reflected the user’s privacy beliefs and 62.5% agreed that the information in the report was understandable and helpful in their decision making. Feedback included that that:

> *“The bar chart comparison helped me understand how the device is not in my best interests”.*

However, comments for improvement included:

> *"More detail would have been helpful such as the company which owns the device, the name of third parties, where they are based (local or abroad) etc."* and, *"A bit more detail about the device and its vendor would be helpful".*

Nevertheless, after reading the report, between choosing "Let me change my settings" and "Keep sharing my biometric data", all the participants (100%) chose to change their settings.

Privacy settings enabled users to control their privacy**:** The privacy setting options are fundamental to allow users to control their privacy in IoT systems. All (100%) of participants agreed that privacy settings were understandable and easy to change, 100% of participants also agreed that the user made all the changes necessary for the settings to reflect their privacy preferences accurately. Further, 100% of users agreed that the user's changes to their privacy settings during the study improved their privacy regarding facial recognition, and 90.0% of participants disagreed that the user needed to make further changes to their privacy settings before they reflect their privacy preferences more accurately. When asked why, reasons included that

> *"By obscuring their face, the user is essentially blocking the device from infringing their privacy" and "By obscuring their face, the user prevents and breach of their privacy".*

One comment for improvement mentioned:

> *"A 'delete any record of me' option would give me further confidence in the system".*

Overall, these results show that IoTAware provided the privacy control settings necessary for users to accurately reflect their privacy preferences and improve their privacy in an IoT system.

Usability has improved: Participants answered the same three Systems Usability Scale (SUS) questions in the exist surveys of both experiments. Based on the responses to the second experiment, the usability of the interface has improved from the first experiment. Participants agreeing that the system was easy to use increased by 5% (see Figure 14.A), participants agreeing they felt very confident using the system increased by 66.6% (see Figure 14.B), meanwhile participants disagreeing they needed to learn a lot before using the system increased by 400% (see Figure 14.C). These findings suggests that the adjustments made to IoTAware have particularly improved user confidence and learnability when using the interface.

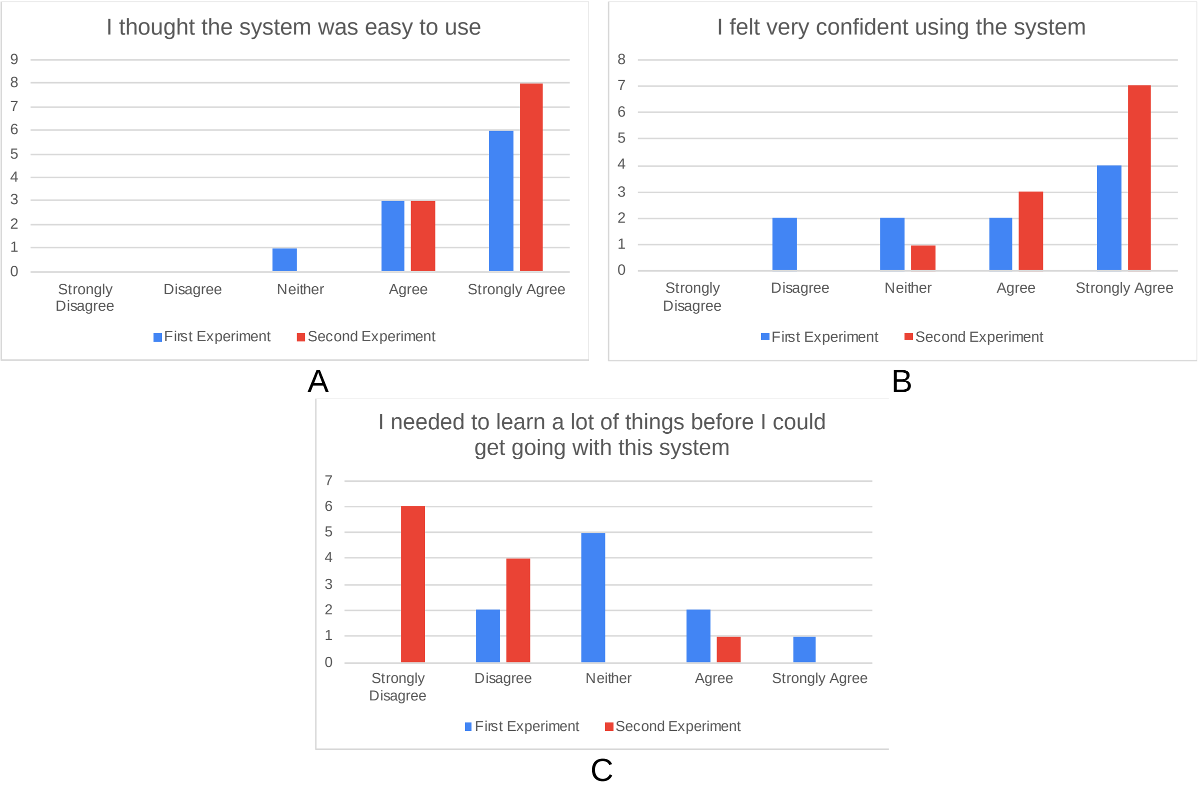


Figure 14. Responses to the Systems Usability Scale (SUS) questions.

10 Evaluation

The aim of this project is to answer the research question: *How to ensure users have awareness and control of the collection, storage and processing of personal data within IoT systems.* Objectives to achieve this desired outcome include: (1) accurately and efficiently measuring the privacy riskiness of IoT devices, (2) precisely measuring individual user's underlying privacy attitudes in the IoT context, (3) influence informed decision making, highlighting any discrepancy between a user's privacy attitudes and the privacy risk of an IoT device and, (4) allowing users to control their privacy in IoT systems

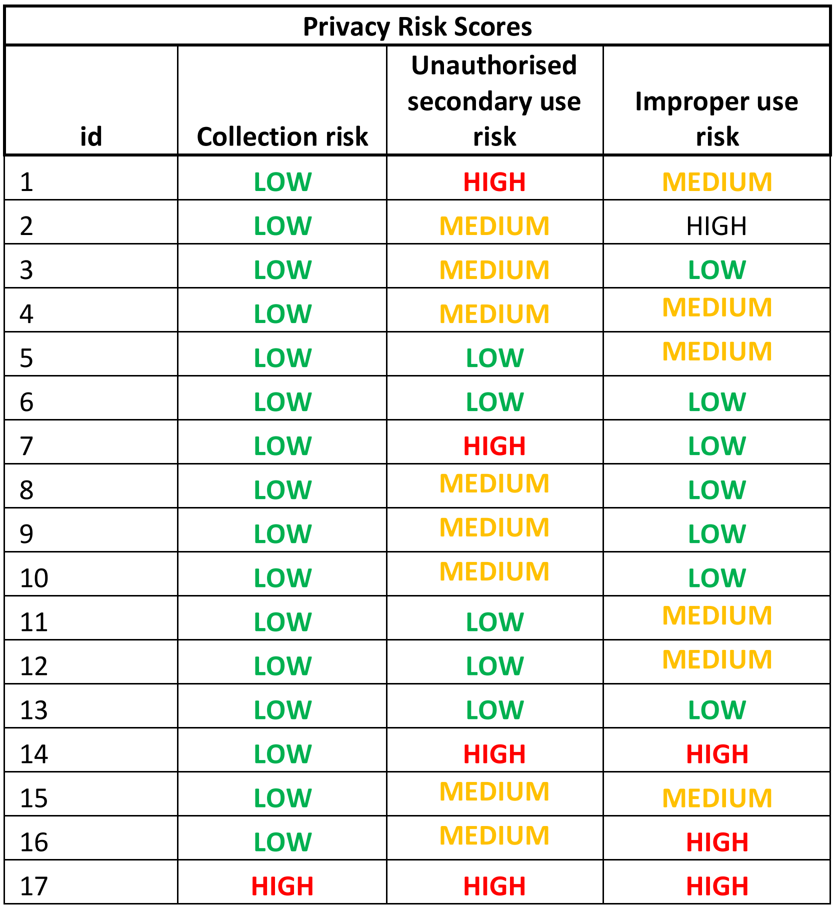
To meet these objectives and answer the research question, this project puts forth four main contributions. First, a reusable method for measuring the underlying privacy attitudes and decision processes of individuals in the IoT context. Second, a reusable framework for measuring the privacy riskiness of IoT devices. Third, a prototype user interface of the IoTAware app which notifies users of the existence of nearby IoT sensors (facial recognition cameras) and nudges users toward making decisions to control their privacy in line with their privacy attitudes. And, finally, a facial recognition case study deploying the IoTAware system in an important application domain.

Using the results of the user study, this section will evaluate this project's design of a personalised IoT privacy warning and control application, and discuss how to design a more system based on lessons learned from the study.

10.1 Measuring the Privacy Riskiness of IoT devices

The case study evaluation revealed a lack of established methods for conducting privacy assessments at scale for a wide range of IoT devices. Therefore, to (1) accurately and efficiently measure the privacy riskiness of IoT devices, this paper presents a method of using taint source analysis with SaINT to measure the privacy riskiness of IoT devices. This approach involves identifying data flow information which constitutes collection, unauthorised secondary use and improper use and using an algorithm to calculate whether a device has low, medium or high privacy risk.

Participants were not shown the inner computations of the IoTAware system, therefore this paper’s method was not evaluated in the user study. However, the accuracy and efficiency of the method and algorithm can be demonstrated by inputting the source code of different IoT device’s and reviewing the each device’s resulting privacy risk score. Appendix item G, implements this paper’s method in the ‘Device’ Java class. By creating and populating an array list with the device information of the 19 IoT apps, and adding appropriate getters and setters etc., the privacy risk scores of each device change with the different data flow information of each device (see Table 5). For instance, device 17 has 37 data flow paths (12 points above the high-risk threshold of 25) whereas, device 14 has 6 flow paths (6 points below the low threshold of 12) therefore, the output of the program is device 17 has high collection risk and device 14 has low collection risk.



Privacy Risk Scores			
id	Collection risk	Unauthorised secondary use risk	Improper use risk
1	LOW	HIGH	MEDIUM
2	LOW	MEDIUM	HIGH
3	LOW	MEDIUM	LOW
4	LOW	MEDIUM	MEDIUM
5	LOW	LOW	MEDIUM
6	LOW	LOW	LOW
7	LOW	HIGH	LOW
8	LOW	MEDIUM	LOW
9	LOW	MEDIUM	LOW
10	LOW	MEDIUM	LOW
11	LOW	LOW	MEDIUM
12	LOW	LOW	MEDIUM
13	LOW	LOW	LOW
14	LOW	HIGH	HIGH
15	LOW	MEDIUM	MEDIUM
16	LOW	MEDIUM	HIGH
17	HIGH	HIGH	HIGH

18	LOW	LOW	LOW
19	LOW	LOW	LOW

Table 5. Summary of the output of the ‘Device’ Java class, showing the privacy risk scores of the 19 IoT apps.

Subsequently, this paper’s method serves as a stimulus for an accurate and part-automated solution for calculating and scoring the privacy riskiness of IoT devices. Likewise, while the activity of linking taint source analysis and data flows to specific privacy risks has not been covered in the literature, this feature of this paper’s work is exploratory but necessary for the functionality of a personalsied IoT privacy awareness and control interface. For instance, SaINT analysis reports cannot measure errors in personal data, therefore, future work should incorporate a more accurate measure of personal data accuracy, this could include integrity checking tools and/or version checking tools. Another interesting challenge is measuring the privacy riskiness of multiple IoT devices in composition. This paper focuses on a scenario of a single IoT device using facial recognition technology and measures the privacy risk of 19 IoT apps/devices as if they are working independently of one another and not part of one system. However, at deployment, there could be multiple IoT devices recorded in the IPRR that are part of a combined system. Therefore, future work should use methods other than source code analysis to measure the details of data flowing between IoT devices as a wider system and consider the amplified privacy risk.

10.2 Measuring Individual User’s Privacy Attitudes towards IoT Technologies

The case study evaluation revealed the significance of measuring individual’s underlying privacy attitudes and using this information to tailor decision support mechanisms, such as nudges, and aid informed privacy decision making in the IoT. However, the case study evaluation also revealed a lack of general methods for measuring the underlying privacy attitudes of users in the context of IoT. Therefore, to (2) precisely measure individual user’s privacy attitudes in the IoT context, this paper requires users to input their attitudes via a modified version of the CFIP survey. Figure 13 reveals the majority (90%) of participants agreed that the privacy nudge, including the colour of privacy icons, reflected the user's privacy beliefs. This implies that IoTAware’s use of the CFIP survey in the IoT context, measures privacy attitudes in the IoT precisely, and, in turn, ensures its privacy nudges, including the colour of privacy icons, are correctly tailored to users’ levels of privacy concern. Otherwise, without IoTAware and its CFIP survey for the IoT context, there would be no validated method for measuring individual user’s privacy attitudes in the IoT context. In turn, this would prevent influencing informed decision making by accurately highlighting any discrepancy between a user’s privacy attitudes and the privacy risk of an IoT device.

Two participants found completing the CFIP survey a lengthy process. This situation reflects a fundamental trade-off between the accuracy at which IoTAware captures and operationalises user’s underlying privacy attitudes and decision processes, and the burden it imposes on users to complete the CFIP survey. The majority of participants (70%) agreed that completing the CFIP would be straightforward.

Nevertheless, to reduce the burden of the CFIP survey, its length could be reduced, however, this would also reduce the accuracy with which the privacy-concern score of users is measured. Alternatively, the length of the CFIP survey could be reduced, and to maintain accuracy, machine learning techniques could be used to model and predict segments of users' privacy attitudes. It is already proven possible to identify privacy profiles that sufficiently capture diverse privacy preferences in both social media settings (Fang et al., 2012; Wisniewski et al., 2014) and mobile app privacy management (Lin et al., 2014; Liu, Lin and Sadeh, 2014). There is yet to be evidence of these techniques working well to capture privacy attitudes concerning privacy in the IoT. However, any developments could be considered for future improvements of the speed and accuracy in which an IoT privacy awareness and control interface captures users' privacy attitudes.

10.3 Addressing Privacy Discrepancies Through Personalised Nudges

Given that privacy behaviours of individuals are often inconsistent with their stated attitudes (the privacy paradox), and this is likely to be aggravated in the IoT, it's crucial that the interface (3) influences informed decision making highlight any discrepancy between a user's privacy attitudes and the privacy risk of an IoT device. The tailored privacy warning icons in the privacy nudges and the additional risk information in the privacy risk report are designed to bring inconsistencies between user's privacy attitudes and the riskiness of IoT devices to the fore, and nudge users into modifying permissions to accurately reflect their level of privacy concern. This appears to have been successful, as Figure 11 reveals, all (100%) of participants agreed that the nudge and /or the privacy risk report influenced them to choose "Let me change my settings". The additional quantitative and qualitative results from the study suggest the interface enables users to make permission decisions accurately reflecting their privacy preferences. In other words, these promising results indicate the privacy discrepancy approach is effective at nudging users to behave in line with their privacy attitudes. Therefore, it is encouraged that this discrepancy approach, along with this paper's recommendations for future work, can be successfully applied to assist users in the IoT domain and address the privacy paradox.

Content of the Privacy Report

If users require more information about the discrepancy between their privacy concerns and the privacy riskiness of an IoT device, they can choose the "Show me before I make changes" option. Results of the study indicate that two participants found the information in the report too abstract and would have found the report more helpful if it provided more contextual information about the IoT device. Given consumers' scarce attention, presenting them with the most relevant privacy information in the most digestible form is crucial. To determine the most important information to include in the privacy risk report, future work should solicit the opinions of privacy and security experts. In the case that there is a need for further additional layers of information, on top of the device's contextual information, this could include independent privacy ratings, expert opinions and other user's opinions (crowd-sourced). This information should be incorporated alongside the current device information in the report by including a plus symbol which can be pressed to reveal the relevant additional information. This type of information could prove effective in informing users of their privacy, as social cues and expert recommendations are proven to have a significant impact on users' decisions (Blythe, Sombatruang and Johnson, 2019). With this, users will have different preferences and acceptance of different sources (Draper et al., 2013) as there will be inherent biases, therefore, a well-designed privacy risk report should also allow users to choose preferred sources.

10.4 Privacy Control Settings

The case study evaluation revealed a lack of effective mechanisms for providing users with awareness and control of the collection, storage and processing of their personal data in IoT systems, namely facial recognition systems. To fully deliver users their right to 'Notice and Choice' in IoT systems, it's important that IoTAware sufficiently gives users the option to opt-in or withdraw their consent. Subsequently, to meet the project's aim, it's crucial that the interface (4) allows users to control their privacy in IoT systems. IoTAware's privacy control settings are designed to enable users to make decisions which reflect their privacy attitudes and improve their privacy. This appears to have been achieved, as 100% of participants agreed that privacy settings were (a) understandable and easy to change, (b) allow the user to make all the changes necessary for the settings to reflect their privacy preferences accurately, and (c) improve the user's privacy regarding facial. This suggests that without IoTAware, users would not only be unaware of the sensitive data collections taking place around them, but also unable to provide explicit consent in the form of opting-in or opting-out of IoT systems.

This paper demonstrates privacy control settings in a particular IoT facial recognition scenario, however, to accommodate a broader range of IoT scenario's, IoTAware should be vigilant to not overwhelm users with settings options and notifications. An increasing the number of controls leads to serious efficiency problems (Smullen, 2020) and multiple unnecessary notifications can lead users to feeling anxious and resigned (Colnago, 2020). Therefore, to ensure users are not overwhelmed by unnecessary privacy notifications, IoTAware should incorporate a "trusted location" feature, saving users from being notified about IoT devices in such locations. This feature would be simple for the user to perform at setup, and it would avoid notifications for user-owned or known devices. For non-trusted locations, on the "Let me change my settings" page, IoTAware could provide user's the option of classifying the device's location as being in a trusted location, therefore, any other devices within the radius of the trusted location would not trigger further privacy notifications. To accommodate this, a general settings page is also needed within the interface to list the devices within trusted locations and allow users to edit their trusted locations, including the radius.

In terms of whether further privacy settings options would be required, feedback from the second experiment included that a "delete any record of me" would have given participants additional confidence in the system. It is possible to request deletion from an IoT resource, however, given IoTAware's benefit provided to consumers is mainly in the information tied to privacy control settings, processing this request doesn't fit into the scope of IoTAware. Moreover, it is unrealistic to assume that IoT resources will grant IoTAware interaction with their systems and request addition and deletion of data.

11 Conclusion

Similar to human behaviours in other life domains, people's privacy behaviours may divert from their stated attitudes (i.e., the privacy paradox). These inconsistencies can be troublesome and problematic, for instance, engendering regrettable experiences or ramifications. To help individuals address this privacy paradox in the IoT, this paper proposes a conceptual architectural model and mock-up prototype design of providing a personalised privacy interface. The interface juxtaposes users' general privacy attitudes towards certain IoT technologies and the potential privacy riskiness of a particular instance of such IoT technology, and influences the user to make decisions about whether and/or how the technology uses their personal data. Over time, planned future work should potentially leverage machine learning models to reduce user burden when measuring privacy attitudes in the context of IoT, add additional layers on information in the privacy risk report, and incorporate a "trusted location" feature, saving users from being overwhelmed with notifications about IoT devices in safe locations.

The single most significant challenge is to amass a substantial amount IoT technology providers (e.g., device manufacturers, app developers, service providers, sensor providers) to release their source code for taint source analysis or agree on a common taxonomy to describe their data collection and use practices. Moreover, it also includes persuading IoT technology providers to adopt protocols, such as the ones designed for IoTAware to support the advertisement and discovery of IoT device risk registries. It is hoped that new regulations such as GDPR, rising consumer concerns about privacy, and the desire by, at least, some technology providers to differentiate themselves from their competitors based on privacy, will all contribute to creating the incentives necessary for this to happen.

It also goes without saying that this paper's concept is not intended to be impeccable nor irreplaceable to the personalsied privacy discrepancy approach. Conversely, configuring privacy assistants to ensure they are as usable as possible will require significantly more research and empirical evaluation with users. While this paper has been successful in proposing a privacy discrepancy approach which is effective at nudging users to behave in line with their privacy attitudes, this has only been tested in an IoT scenario of facial recognition technology. The IoT presents a significantly broader set of scenarios and contexts. Therefore, recognising relevant contextual attributes, such as automatically turning off Alexa when a privacy-concerned guest visits your home and doing so in a privacy-preserving manner, will require more work.

12 References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M. and Wang, Y., 2017. Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), pp.1-41.

Acquisti, A., Brandimarte, L. and Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science, 347(6221), pp.509-514.

Ahonen, T., Hadid, A. and Pietikainen, M., 2006. Face description with local binary patterns: Application to face recognition. IEEE transactions on pattern analysis and machine intelligence, 28(12), pp.2037-2041.

Al-Hasnawi, A. and Lilien, L., 2017, December. Pushing data privacy control to the edge in IoT using policy enforcement fog module. In Companion Proceedings of the10th International Conference on Utility and Cloud Computing (pp. 145-150).

Allied Market Research. 2016. Facial Recognition Market Expected To Reach $9.6B By 2022. [online] Available at: <https://www.alliedmarketresearch.com/press-release/facial-recognition-market.html> [Accessed 10 July 2020].

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F. and Agarwal, Y., 2015, April. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In Proceedings of the 33rd annual ACM conference on human factors in computing systems (pp. 787-796).

Apple Homekit. 2020. Ios - Home. [online] Available at: <https://www.apple.com/ios/home/> [Accessed 20 July 2020].

Apple. 2020. Swift. [online] Available at: <https://www.apple.com/uk/swift/> [Accessed 10 August 2020].

Bashir, M., Hayes, C., Lambert, A.D. and Kesan, J.P., 2015. Online privacy and informed consent: The dilemma of information asymmetry. Proceedings of the Association for Information Science and Technology, 52(1), pp.1-10.

Belhumeur, P.N., Hespanha, J.P. and Kriegman, D.J., 1997. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Transactions on pattern analysis and machine intelligence, 19(7), pp.711-720.

Blythe, J.M., Sombatruang, N. and 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), p.tyz005.

BOSUA, R., CLARK, K., RICHARDSON, M. and WEBB, J., 2014. 19: Intelligent Warning Systems:'Technological Nudges' to En-hance User Control of IoT Data Collection, Storage and Use. GOOD DATA, 47, p.330.

Celik, Z.B., Babun, L., Sikder, A.K., Aksu, H., Tan, G., McDaniel, P. and Uluagac, A.S., 2018. Sensitive information tracking in commodity IoT. In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 1687-1704).

Celik, Z.B., McDaniel, P. and Tan, G., 2018. Soteria: Automated iot safety and security analysis. In 2018 {USENIX} Annual Technical Conference ({USENIX}{ATC} 18) (pp. 147-158).
chapter 7.5, pages 398–415.

Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L.F. and Sadeh, N., 2020, April. Informing the design of a personalized privacy assistant for the internet of things. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-13).

Developer.apple.com. 2020. Ios Human Interface Guidelines. [online] Available at: <https://developer.apple.com/design/human-interface-guidelines/ios/overview/themes/> [Accessed 15 September 2020].

De Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D.F., Ren, J., Rode, J.A. and Silva Filho, R., 2005. In the eye of the beholder: a visualization-based approach to information system security. International Journal of Human-Computer Studies, 63(1-2), pp.5-24.

Doerrfeld, B., 2015. 20+ Emotion Recognition Apis That Will Leave You Impressed, And Concerned | Nordic Apis |. [online] Nordic APIs. Available at: <https://nordicapis.com/20-emotion-recognition-apis-that-will-leave-you-impressed-and-concerned/> [Accessed 10 July 2020].

Dormehl, L., 2014. Facial Recognition: Is The Technology Taking Away Your Identity?. [online] The Guardian. Available at: <https://www.theguardian.com/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues> [Accessed 10 July 2020].

Draper, A.K., Adamson, A.J., Clegg, S., Malam, S., Rigg, M. and Duncan, S., 2013. Front-of-pack nutrition labelling: are multiple formats a problem for consumers?. The European Journal of Public Health, 23(3), pp.517-521.

Duby, G., 1992. A history of private life: From pagan Rome to Byzantium (Vol. 1). Belknap Press.

EDPB. 2019. European Data Protection Board - Facial Recognition In School Renders Sweden’S First GDPR Fine. [online] Available at: <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en#:~:text=The%20Swedish%20DPA%20has%20fined,attendance%20of%20students%20in%20school.&text=This%20is%20the%20first%20fine%20issued%20by%20the%20Swedish%20DPA> [Accessed 3 July 2020].

Egelman, S. and Peer, E., 2015, September. The myth of the average user: Improving privacy and security systems through individualization. In Proceedings of the 2015 New Security Paradigms Workshop (pp. 16-28).

Fang, L. and LeFevre, K., 2010, April. Privacy wizards for social networking sites. In Proceedings of the 19th international conference on World wide web (pp. 351-360).

Ferreira, D., Kostakos, V., Beresford, A.R., Lindqvist, J. and Dey, A.K., 2015, June. Securacy: an empirical investigation of Android applications' network usage, privacy and security. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 1-11).

Frey, C., 2017. Revealed: How Facial Recognition Has Invaded Shops – And Your Privacy. [online] the Guardian. Available at: <https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto> [Accessed 10 September 2020].

Friedman, D., 2000. Privacy and technology. Social Philosophy and Policy, 17(2), pp.186-212.

Gates, K.A., 2011. Our biometric future: Facial recognition technology and the culture of surveillance (Vol. 2). NYU Press.

Gessner, D., Olivereau, A., Segura, A.S. and Serbanati, A., 2012, June. Trustworthy infrastructure services for a secure and privacy-respecting internet of things. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (pp. 998-1003). IEEE.

Gibbs, S., 2015. Samsung Smart Tvs Send Unencrypted Voice Recognition Data Across Internet. [online] the Guardian. Available at: <https://www.theguardian.com/technology/2015/feb/19/samsung-smart-tvs-send-unencrypted-voice-recognition-data-across-internet> [Accessed 8 June 2020].

GitHub. 2020. Smartthings Community. [online] Available at: <https://github.com/SmartThingsCommunity> [Accessed 20 July 2020].

Good, N., 2012. The Deadly Sins of Security User Interfaces. The Death of the Internet,
chapter 7.5, pages 398–415.

HP. 2014. Www8.hp.com. HP News - HP Study Reveals 70 Percent Of Internet Of Things Devices Vulnerable To Attack. [online] Available at: <http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.V-e1I7Wa1fA> [Accessed 2 July 2020].

Iapp.org. 2011. AICPA/CICA Privacy Maturity Model. [online] Available at: <https://iapp.org/resources/article/2012-06-01-aicpa-cica-privacy-maturity-model/> [Accessed 29 June 2020].

Introna, L. and Wood, D., 2004. Picturing algorithmic surveillance: The politics of facial recognition systems. Surveillance & Society, 2(2/3), pp.177-198.

IoT for All. 2017. The 5 Worst Examples of IoT. [online] Available at: http://www.iotforall.com/5-worst-iot-hackingvulnerabilities/ [Accessed 2 September 2020].

ISO. 1999. ISO 13407:1999. [online] Available at: <https://www.iso.org/standard/21197.html> [Accessed 11 August 2020].

Jacko, J.A. ed., 2012. Human computer interaction handbook: Fundamentals, evolving technologies, and emerging applications. CRC press.

Jackson, C.B. and Wang, Y., 2018. Addressing the Privacy Paradox through personalized privacy notifications. Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies, 2(2), pp.1-25.

John, L.K., Acquisti, A. and Loewenstein, G., 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. Journal of consumer research, 37(5), pp.858-873.

Keller, P.A., Harlam, B., Loewenstein, G. and Volpp, K.G., 2011. Enhanced active choice: A new method to motivate behavior change. Journal of Consumer psychology, 21(4), pp.376-383.

Kelley, P.G., Cranor, L.F. and Sadeh, N., 2013, April. Privacy as part of the app decision-making process. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 3393-3402).

Knijnenburg, B.P. and Kobsa, A., 2013, March. Helping users with information disclosure decisions: potential for adaptation. In Proceedings of the 2013 international conference on Intelligent user interfaces (pp. 407-416).

Korzaan, M.L. and Boswell, K.T., 2008. The influence of personality traits and information privacy concerns on behavioral intentions. Journal of Computer Information Systems, 48(4), pp.15-24.

Kumaraguru, P. and Cranor, L.F., 2005. Privacy indexes: a survey of Westin's studies (pp. 368-394). Carnegie Mellon University, School of Computer Science, Institute for Software Research International.

LaFrance, A., 2017. Who Owns Your Face?. [online] The Atlantic. Available at: <https://www.theatlantic.com/technology/archive/2017/03/who-owns-your-face/520731/> [Accessed 22 June 2020].

Lederer, S., Mankoff, J. and Dey, A.K., 2003, April. Who wants to know what when? privacy preference determinants in ubiquitous computing. In CHI'03 extended abstracts on Human factors in computing systems (pp. 724-725).

Lin, J., Amini, S., Hong, J.I., Sadeh, N., Lindqvist, J. and Zhang, J., 2012, September. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM conference on ubiquitous computing (pp. 501-510).

Lin, J., Liu, B., Sadeh, N. and Hong, J.I., 2014. Modeling users’ mobile app privacy preferences: Restoring usability in a sea of permission settings. In 10th Symposium On Usable Privacy and Security ({SOUPS} 2014) (pp. 199-212).

Lin, J., Liu, B., Sadeh, N. and Hong, J.I., 2014. Modeling users’ mobile app privacy preferences: Restoring usability in a sea of permission settings. In 10th Symposium On Usable Privacy and Security ({SOUPS} 2014) (pp. 199-212).

Liu, B., Andersen, M.S., Schaub, F., Almuhimedi, H., Zhang, S.A., Sadeh, N., Agarwal, Y. and Acquisti, A., 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (pp. 27-41).

Liu, B., Lin, J. and Sadeh, N., 2014, April. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?. In Proceedings of the 23rd international conference on World wide web (pp. 201-212).

Manyika, J., 2015. The Internet of Things: Mapping the value beyond the hype. McKinsey Global Institute.

Met.police.uk. 2020. Metropolitan Police Service Live Facial Recognition Trials. [online] Available at: <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf> [Accessed 3 July 2020].

Misra, S., Maheswaran, M. and Hashmi, S., 2017. Security challenges and approaches in internet of things. Cham: Springer International Publishing.
Moore Jr, B., 2017. Privacy: Studies in Social and Cultural History: Studies in Social and Cultural History. Routledge.

Moye, D., 2018. Amazon Admits Alexa Device Eavesdropped On Portland Family. [online] Huffingtonpost.co.uk. Available at: <https://www.huffingtonpost.co.uk/entry/alexa-eavesdropping-portland-familiy_n_5b0727cae4b0fdb2aa51b23e> [Accessed 8 June 2020].

Newman, P., 2020. The Internet Of Things 2020 Report: How The Iot Is Evolving To Reach The Mainstream With Business And Consumers. [online] Business Insider. Available at: <https://www.businessinsider.com/internet-of-things-report?r=US&IR=T> [Accessed 8 June 2020].

Nissenbaum, H., 2009. Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Oauth.net. 2020. Oauth 2.0. [online] Available at: <https://oauth.net/2/> [Accessed 11 August 2020].

Openhab.org. 2020. Openhab. [online] Available at: <https://www.openhab.org/> [Accessed 20 July 2020].

Paas, F., Tuovinen, J.E., Tabbers, H. and Van Gerven, P.W., 2003. Cognitive load measurement as a means to advance cognitive load theory. Educational psychologist, 38(1), pp.63-71.

Pollach, I., 2005. A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. Journal of Business Ethics, 62(3), p.221.

Psaras, I., 2018, June. Decentralised edge-computing and iot through distributed trust. In Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (pp. 505-507).

Rajput, A., 2016. Smart CCTV And The Internet Of Things: 2016 Trends And Predictions - IFSEC Global | Security And Fire News And Resources. [online] IFSEC Global | Security and Fire News and Resources. Available at: <https://www.ifsecglobal.com/video-surveillance/smart-cctv-and-the-internet-of-things-2016-trends-and-predications/> [Accessed 10 July 2020].

Regulation, G.D.P., 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. Official Journal of the European Union (OJ), 59(1-88), p.294.

Rhodes, S.D., Bowie, D.A. and Hergenrather, K.C., 2003. Collecting behavioural data using the world wide web: considerations for researchers. Journal of Epidemiology & Community Health, 57(1), pp.68-73.

Schroff, F., Kalenichenko, D. and Philbin, J., 2015. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 815-823).

Sennaar, K. 2018. Facial Recognition Applications – Security, Retail, and Beyond. Available at: https://www.techemergence.com/facial-recognition-applications/. [Accessed 1 July 2020].

SmartThings Community. 2020. Smartthings Community. [online] Available at: <https://community.smartthings.com/> [Accessed 20 July 2020].

SmartThings.com. 2020. Smartthings. [online] Available at: <https://www.smartthings.com/uk> [Accessed 20 July 2020].

Smith, H.J., Milberg, S.J. and Burke, S.J., 1996. Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly, pp.167-196.

Spiekermann, S., Grossklags, J. and Berendt, B., 2001, October. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In Proceedings of the 3rd ACM conference on Electronic Commerce (pp. 38-47).

Stewart, K.A. and Segars, A.H., 2002. An empirical examination of the concern for information privacy instrument. Information systems research, 13(1), pp.36-49.

The Noun Project. 2020. Design Guidelines For User Submissions. [online] Available at: <https://blog.thenounproject.com/post/13118286227/design-guidelines-for-user-submissions> [Accessed 17 September 2020].

Tsai, L., Wijesekera, P., Reardon, J., Reyes, I., Egelman, S., Wagner, D., Good, N. and Chen, J.W., 2017. Turtle guard: Helping android users apply contextual privacy preferences. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 145-162).

Turk, M. and Pentland, A., 1991. Eigenfaces for recognition. Journal of cognitive neuroscience, 3(1), pp.71-86.

Ukil, A., Bandyopadhyay, S. and Pal, A., 2015, June. Privacy for IoT: Involuntary privacy enablement for smart energy systems. In 2015 IEEE International Conference on Communications (ICC) (pp. 536-541). IEEE.

Ukil, A., Sen, J. and Koilakonda, S., 2011, March. Embedded security for Internet of Things. In 2011 2nd National Conference on Emerging Trends and Applications in Computer Science (pp. 1-6). IEEE.

US GAO. 2015. FACIAL RECOGNITION TECHNOLOGY Commercial Uses, Privacy Issues, And Applicable Federal Law. [online] Available at: <https://www.gao.gov/assets/680/671764.pdf> [Accessed 10 July 2020].

Van Der Geest, T., Pieterson, W. and De Vries, P., 2005. Informed consent to address trust, control, and privacy concerns in user profiling. Privacy Enhanced Personalisation, PEP, pp.23-34.

Vasseur, J.P. and Dunkels, A., 2010. Interconnecting smart objects with ip: The next internet. Morgan Kaufmann.

Wachter, S., 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Computer law & security review, 34(3), pp.436-449.

Wang, J., Amos, B., Das, A., Pillai, P., Sadeh, N. and Satyanarayanan, M., 2017, June. A scalable and privacy-aware IoT service for live video analytics. In Proceedings of the 8th ACM on Multimedia Systems Conference (pp. 38-49).

Westin, A.F., 1966. Science, privacy, and freedom: Issues and proposals for the 1970's. Part I--The current impact of surveillance on privacy. Columbia Law Review, 66(6), pp.1003-1050.

Wisniewski, P., Knijnenburg, B.P. and Lipford, H.R., 2014, July. Profiling facebook users privacy behaviors. In SOUPS2014 Workshop on Privacy Personas and Segmentation.

Xu, H., Gupta, S., Rosson, M.B. and Carroll, J.M., 2012. Measuring mobile users' concerns for information privacy.

Yurieff, K. 2019. Google says Nest Guard’s hidden microphone wasn’t meant to be a secret. [online] CNN. Available at: http://www.cnn.com/2019/02/20/tech/google-nestmicrophone-secret/index.html. (2019). [Accessed 2 September 20202].

Zeng, E., Mare, S. and Roesner, F., 2017. End user security and privacy concerns with smart homes. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 65-80).

Ziegeldorf, J.H., Morchon, O.G. and Wehrle, K., 2014. Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), pp.2728-2742.

13 Bibliography

Beresford, A.R., Kübler, D. and Preibusch, S., 2012. Unwillingness to pay for privacy: A field experiment. Economics letters, 117(1), pp.25-27.

Debatin, B., Lovejoy, J.P., Horn, A.K. and Hughes, B.N., 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of computer-mediated communication, 15(1), pp.83-108.

Federal Trade Commission, 2015. Internet of things: Privacy & security in a connected world. Washington, DC: Federal Trade Commission.

Glanville, B., 2018. 72% Of Brits Haven'T Heard About GDPR. [online] Yougov.co.uk. Available at: <https://yougov.co.uk/topics/politics/articles-reports/2018/03/01/72-brits-havent-heard-about-gdpr> [Accessed 8 June 2020].

Hughes-Roberts, T., 2014. The effect of privacy salience on end-user behaviour: An experimental approach based on the theory of planned behaviour (Doctoral dissertation, University of Salford).

Mackay, W.E., 1991, March. Triggers and barriers to customizing software. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 153-160).

Masiello, B., 2009. Deconstructing the privacy experience. IEEE Security & Privacy, 7(4), pp.68-70.

Norberg, P.A., Horne, D.R. and Horne, D.A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), pp.100-126.

Norman, D.A., 1988. The psychology of everyday things. Basic books.

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S. and Dabbish, L., 2013. Anonymity, privacy, and security online. Pew Research Center, 5.

The Harris Poll, 2018. IBM Cybersecurity And Privacy Research. [online] Newsroom.ibm.com. Available at: <http://newsroom.ibm.com/download/IBM+Cybersecurity+PR+Research+-+Final.pdf> [Accessed 8 June 2020].

14 Appendices

14.1 Appendix A – Concern for Information Privacy Instrument (Smith et al.1996)

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by circling the appropriate number.

Collection
C1 It usually bothers me when companies ask me for personal information.
C2. When companies ask me for personal information, I sometimes think twice before providing it.
C3. It bothers me to give personal information to so many companies.
C4. I'm concerned that companies are collecting too much personal information about me.

Errors
E1 All the personal information in computer databases should be double-checked for accuracy-no matter how much this costs.
E2. Companies should take more steps to make sure that the personal information in their files is accurate.
E3. Companies should have better procedures to correct errors in personal information.
E4. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

Unauthorised Secondary Use
US1. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
US2. When people give personal information to a company for some reason, the company should never use the information for any other reason.
US3. Companies should never sell the personal information in their computer databases to other companies.
US4. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

Improper Access
IA1. Companies should devote more time and effort to preventing unauthorized access to personal information.
IA2. Computer databases that contain personal information should be protected from unauthorized access-no matter how much it costs.
IA3. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

14.2 Appendix B – Concern for Information Privacy Instrument in the IoT Context

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by circling the appropriate number.

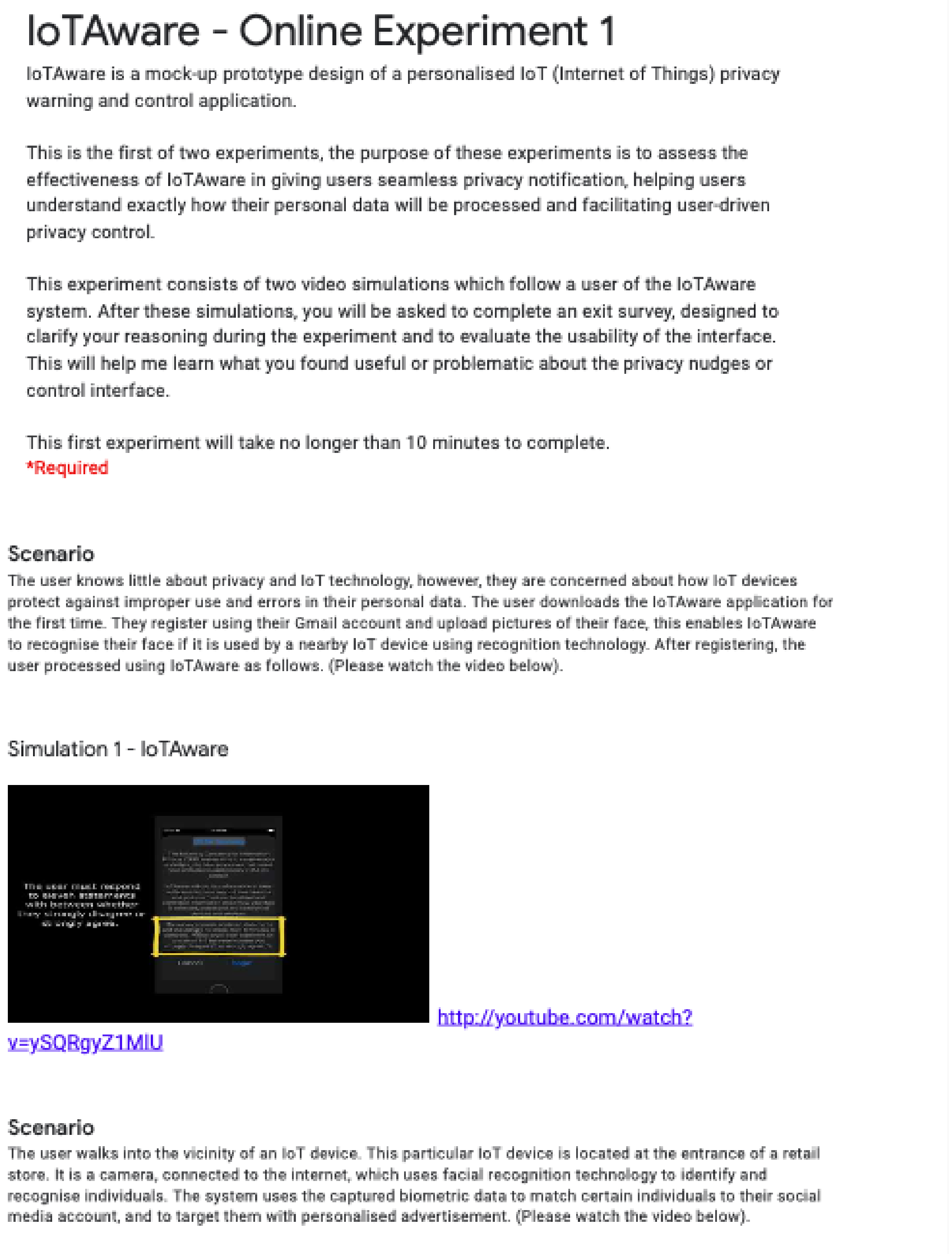
Collection
CN1. I am concerned that IoT service providers are collecting too much personal information about me.
CN2. It bothers me to give personal information to so many IoT service providers.

Unauthorised Secondary Use
US1. IoT service providers should not use personal information for any purpose not specifically authorized by the user.
US2. IoT service providers should never sell personal information to other companies.
US3. IoT service providers should never share personal information with other companies unless specifically authorized to do so by the user.

Improper Access
IA1. IoT service providers should devote more time and effort to preventing unauthorized access to personal information.
IA2. IoT service providers should take more steps to ensure that the personal information in their files is accurate.
IA3. IoT service providers should take more steps to ensure that unauthorized people cannot access personal information.

Errors
ER1 All personal information held by the IoT service providers should be double-checked for accuracy - no matter how much the costs.
ER2. IoT service providers should have better procedures to correct errors in personal information.
ER3. IoT service providers should devote more time and effort to verifying the accuracy of the personal information in their databases.

14.3 Appendix C – Online Experiment 1



IoTAware - Online Experiment 1

IoTAware is a mock-up prototype design of a personalised IoT (Internet of Things) privacy warning and control application.

This is the first of two experiments, the purpose of these experiments is to assess the effectiveness of IoTAware in giving users seamless privacy notification, helping users understand exactly how their personal data will be processed and facilitating user-driven privacy control.

This experiment consists of two video simulations which follow a user of the IoTAware system. After these simulations, you will be asked to complete an exit survey, designed to clarify your reasoning during the experiment and to evaluate the usability of the interface. This will help me learn what you found useful or problematic about the privacy nudges or control interface.

This first experiment will take no longer than 10 minutes to complete.

*Required

Scenario

The user knows little about privacy and IoT technology, however, they are concerned about how IoT devices protect against improper use and errors in their personal data. The user downloads the IoTAware application for the first time. They register using their Gmail account and upload pictures of their face, this enables IoTAware to recognise their face if it is used by a nearby IoT device using recognition technology. After registering, the user processed using IoTAware as follows. (Please watch the video below).

Simulation 1 - IoTAware

The user must respond to seven statements with between whether they strongly disagree or strongly agree.

http://youtube.com/watch?v=ySQRgyZ1MIU

Scenario

The user walks into the vicinity of an IoT device. This particular IoT device is located at the entrance of a retail store. It is a camera, connected to the internet, which uses facial recognition technology to identify and recognise individuals. The system uses the captured biometric data to match certain individuals to their social media account, and to target them with personalised advertisement. (Please watch the video below).

Simulation 2 - Notification

The user is concerned about improper use in IoT devices and the IoT device under consideration has a high level of riskiness in improper use. This means the user would divert from their privacy attitudes/concerns towards improper use if they were to accept all permission requests...

http://youtube.com/watch?v=_qkdmNDrgw

Skip to question 1

Exit Survey 1

Upon completing the simulations, please respond with how much you either agree or disagree with the following statements:

1. Completing the CFIP survey would be straightforward. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

2. Why?

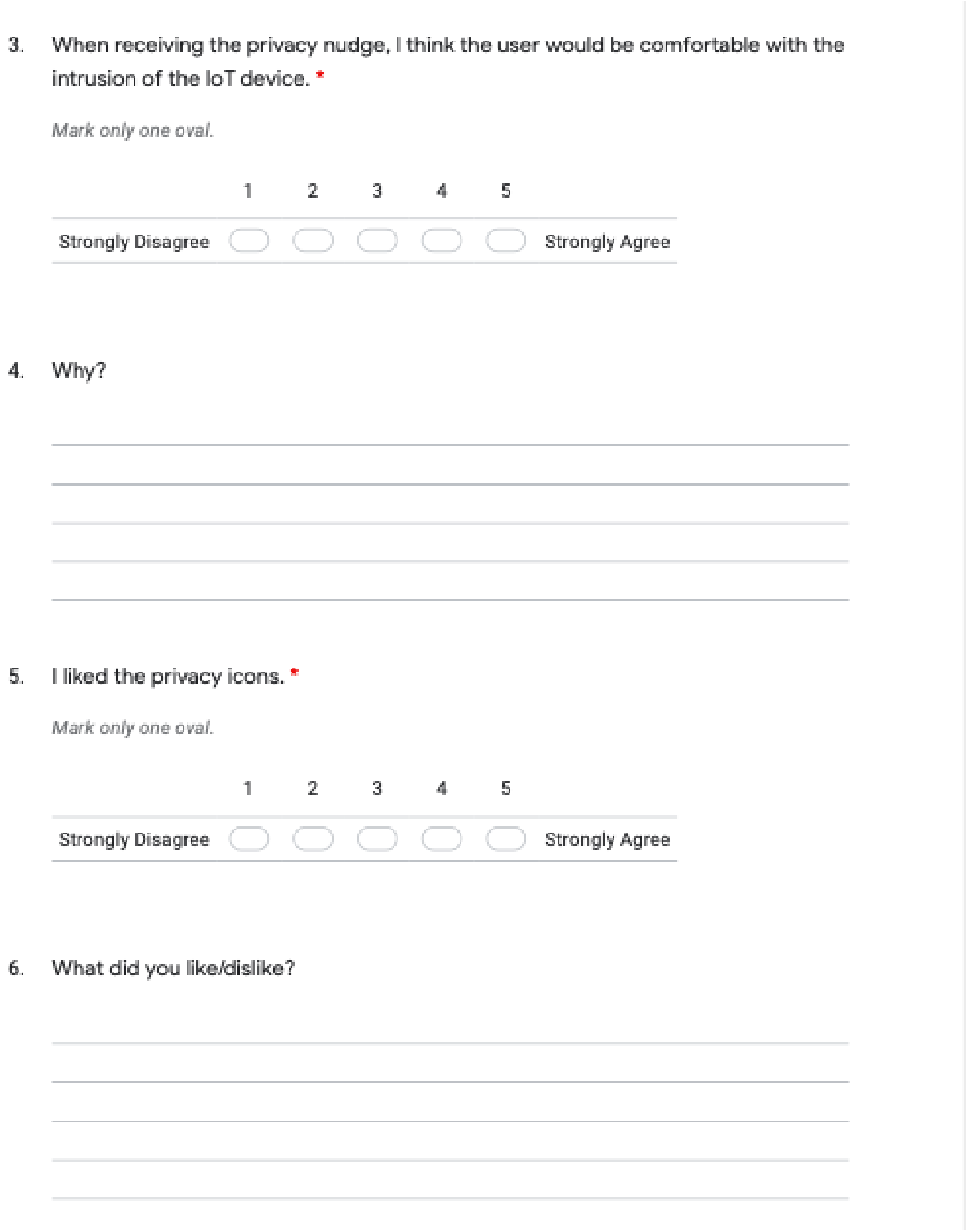
____

____

____

____

____



3. When receiving the privacy nudge, I think the user would be comfortable with the intrusion of the IoT device. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

4. Why?

5. I liked the privacy icons. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

6. What did you like/dislike?

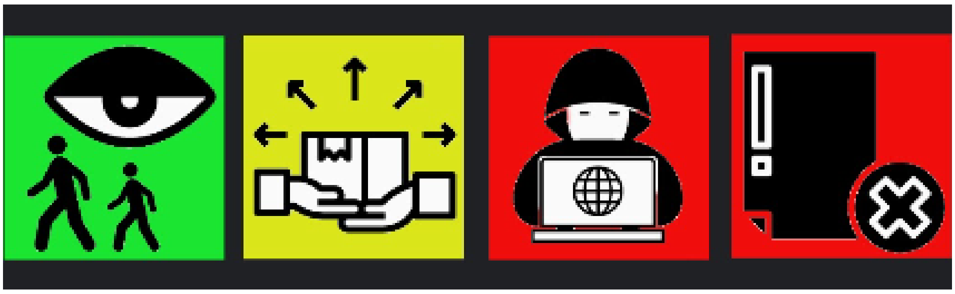
7. I understood the meaning of the privacy icons. *

Mark only one oval.

○ Agree

○ Disagree

Privacy Icons:



8. Recall, what do these four icons represent? (Please answer from the left icon to the right) *

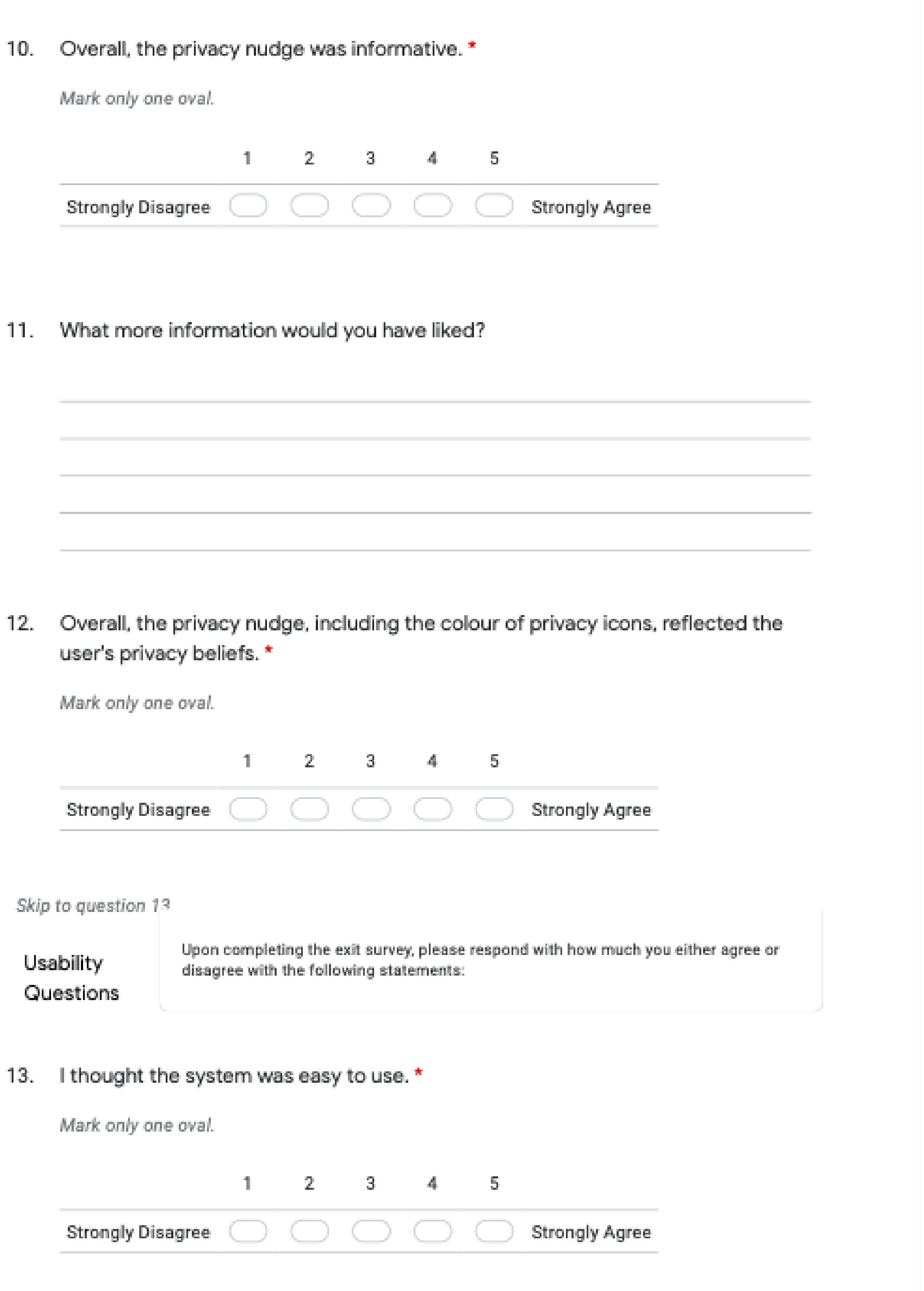
____

9. What does it mean if a privacy icon is coloured red? *

Mark only one oval.

○ There is a low level of discrepancy between my privacy concerns and the riskiness of the IoT device.

○ There is a high level of discrepancy between my privacy concerns and the riskiness of the IoT device.



10. Overall, the privacy nudge was informative. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

11. What more information would you have liked?

12. Overall, the privacy nudge, including the colour of privacy icons, reflected the user's privacy beliefs. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Skip to question 13

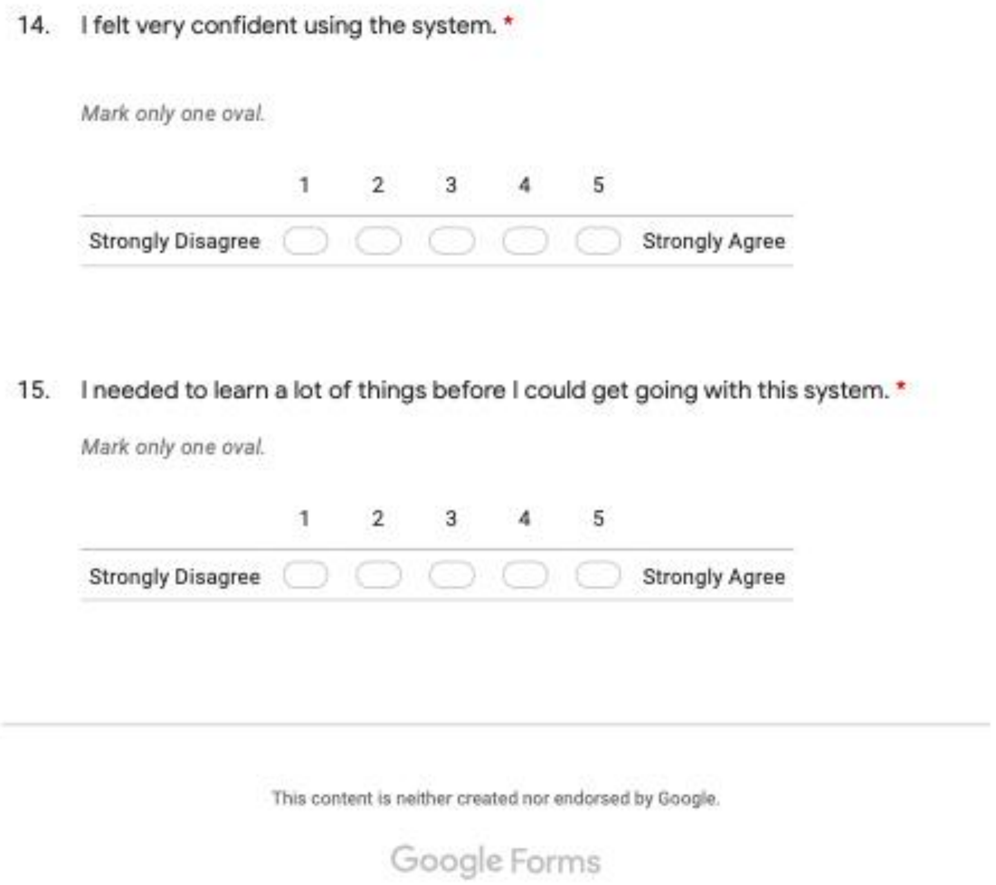
Usability Questions

Upon completing the exit survey, please respond with how much you either agree or disagree with the following statements:

13. I thought the system was easy to use. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



14. I felt very confident using the system. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

15. I needed to learn a lot of things before I could get going with this system. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

This content is neither created nor endorsed by Google.

Google Forms

14.4 Appendix D – Online Experiment 2

IoTAware - Online Experiment 2

IoTAware is a mock-up prototype design of a personalised IoT (Internet of Things) privacy warning and control application.

This is the second of two experiments, the purpose of these experiments is to assess the effectiveness of IoTAware in giving users seamless privacy notification, helping users understand exactly how their personal data will be processed and facilitating user-driven privacy control.

This experiment consists of two video simulations which follow a user of the IoTAware system. When conducting this experiment, please reason about what you see the user doing and how they interact with IoTAware. After these simulations, you will be asked to complete an exit survey, designed to clarify this reasoning during the experiment.

This second experiment will take no longer than 10 minutes to complete.
*Required

Scenario

The user knows little about privacy and IoT technology, however, they are concerned about how IoT devices protect against improper use and errors in their personal data. The user downloads the IoTAware application for the first time. They register using their Gmail account and upload pictures of their face, this enables IoTAware to recognise their face if it is used by a nearby IoT device using recognition technology. After registering, the user proceeds using IoTAware as follows. (Please watch the video below).

Simulation 1 - IoTAware

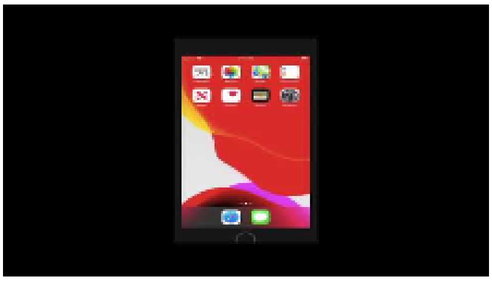
Any discrepancy between the user's privacy concern and the privacy-riskiness of the device will be presented to the user in a personalised privacy notification.

http://youtube.com/watch?v=A4g_a552F7s

Scenario

The user walks into the vicinity of an IoT device. This particular IoT device is located at the entrance of a retail store. It is a camera, connected to the internet, which uses facial recognition technology to identify and recognise individuals. The system uses the captured biometric data to match certain individuals to their social media account, and to target them with personalised advertisement. (Please watch the video below).

Simulation 2 - Notification



http://youtube.com/watch?v=LLarOg17ZiM

1. How much do you agree with the following statement: the nudge's "What does this mean" option and suggestion on what to do next helped me make a decision. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

2. Which option should the user choose? *

Mark only one oval.

○ A (Let me change my settings - continue to section 2)

○ B (Show me before I make changes - continue to section 3)

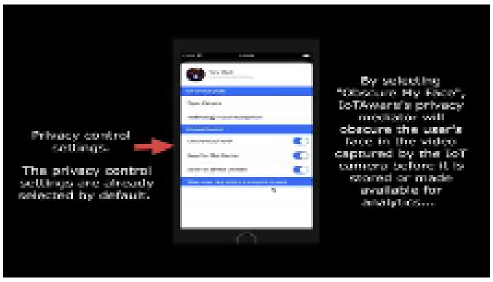
○ C (Keep sharing my biometric data - continue to section 4)

Section 2: "Let me change my settings"

The user has high concern over their privacy and has selected to change their privacy settings. By choosing this option, it enables the user to control whether their personal data is collected, processed and used to the IoT device. The user selects to "Obscure my Face" which ensures the user's facial images aren't collected, processed or used by the IoT device.

Please watch the video below and please respond with how much you either agree or disagree with the following statements:

"Let me change my settings"



Privacy control settings.

The privacy control settings are already selected by default.

By selecting "Obscure My Face", IoTAware's privacy mediator will obscure the user's face in the video captured by the IoT camera before it is stored or made available for analytics...

http://youtube.com/watch?v=uGlGWiHnrew

3. The nudge and /or the privacy risk report influenced me to choose "Let me change my settings".

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

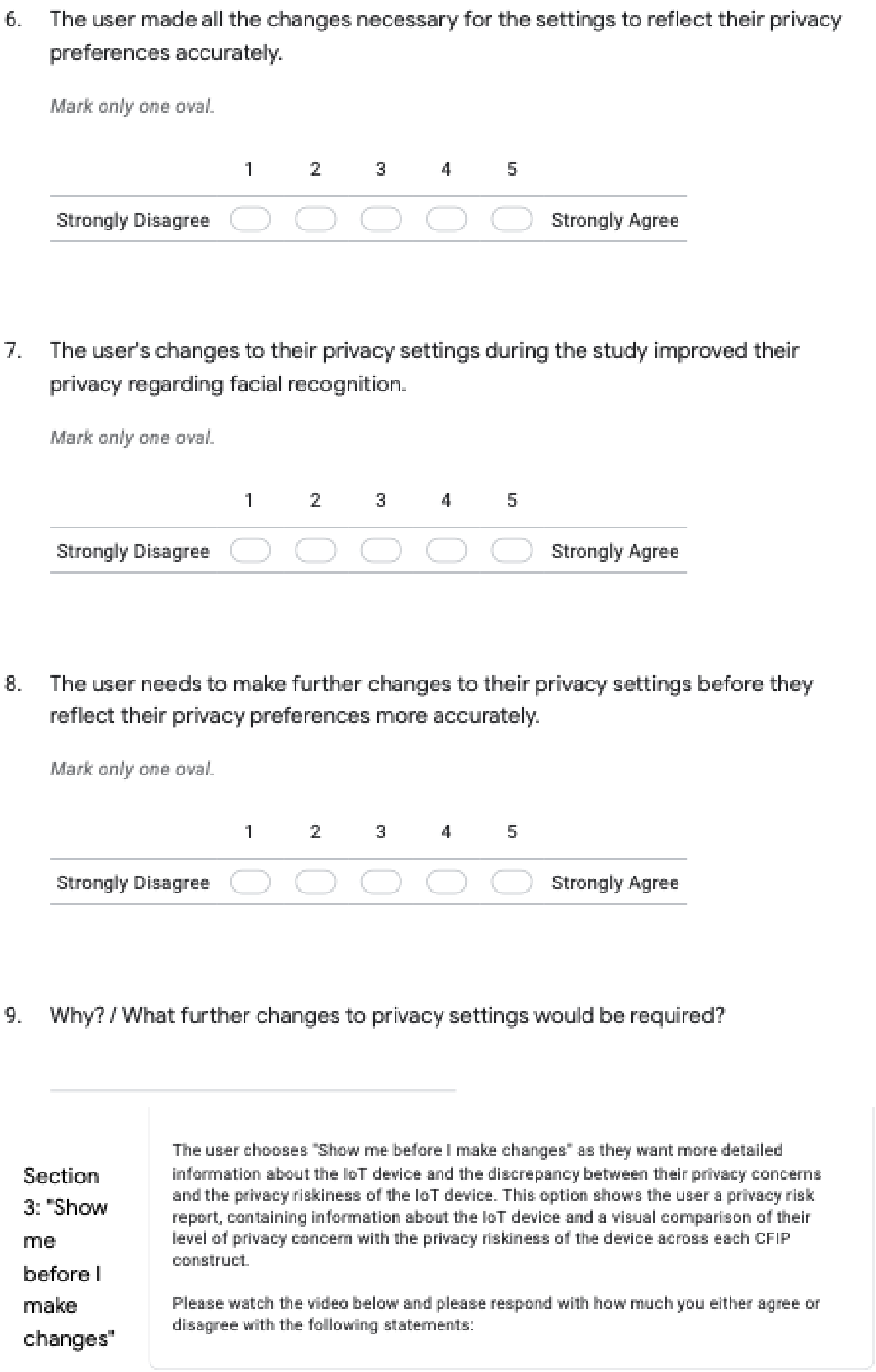
4. Why?

____

5. The privacy settings were understandable and easy to change.

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



6. The user made all the changes necessary for the settings to reflect their privacy preferences accurately.

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

7. The user's changes to their privacy settings during the study improved their privacy regarding facial recognition.

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

8. The user needs to make further changes to their privacy settings before they reflect their privacy preferences more accurately.

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

9. Why? / What further changes to privacy settings would be required?

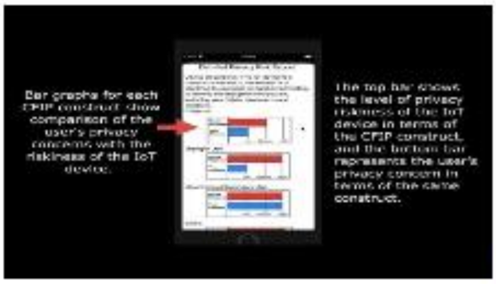
____

Section 3: "Show me before I make changes"

The user chooses "Show me before I make changes" as they want more detailed information about the IoT device and the discrepancy between their privacy concerns and the privacy riskiness of the IoT device. This option shows the user a privacy risk report, containing information about the IoT device and a visual comparison of their level of privacy concern with the privacy riskiness of the device across each CFIP construct.

Please watch the video below and please respond with how much you either agree or disagree with the following statements:

"Show me before I make changes"



Bar graphs for each CFIP construct show comparison of the user's privacy concerns with the riskiness of the IoT device.

The top bar shows the level of privacy riskiness of the IoT device in terms of the CFIP construct, and the bottom bar represents the user's privacy concern in terms of the same construct.

http://youtube.com/watch?v=JfP_fKtqYvU

10. Why should the user choose "Show me before I make changes" ?

____

11. The information in the report was understandable and helpful in my decision making.

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

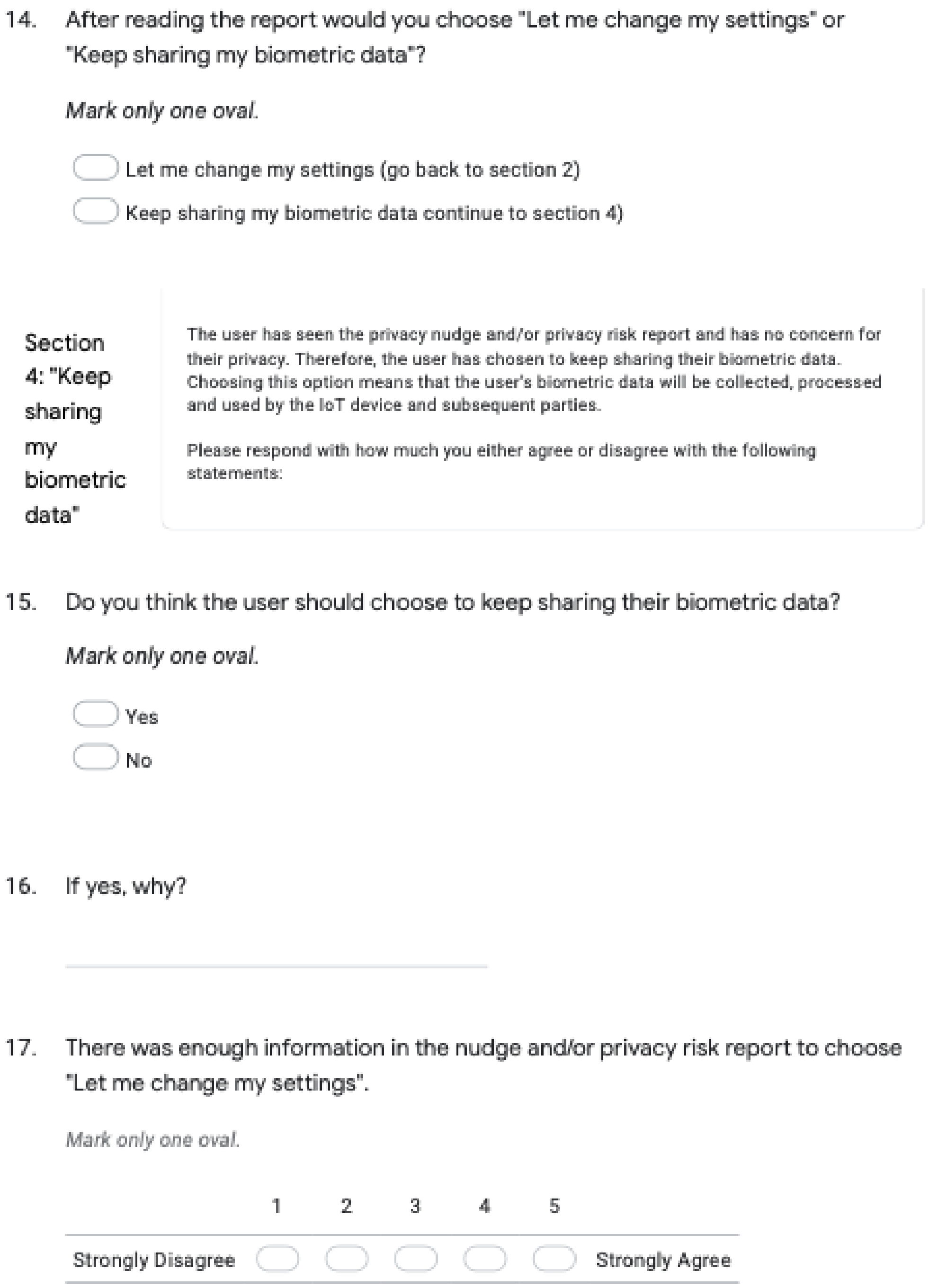
12. Why was the information helpful or unhelpful?

____

13. The privacy report reflected the user's privacy beliefs.

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



14. After reading the report would you choose "Let me change my settings" or "Keep sharing my biometric data"?

Mark only one oval.

○ Let me change my settings (go back to section 2)

○ Keep sharing my biometric data continue to section 4)

Section 4: "Keep sharing my biometric data"

The user has seen the privacy nudge and/or privacy risk report and has no concern for their privacy. Therefore, the user has chosen to keep sharing their biometric data. Choosing this option means that the user's biometric data will be collected, processed and used by the IoT device and subsequent parties.

Please respond with how much you either agree or disagree with the following statements:

15. Do you think the user should choose to keep sharing their biometric data?

Mark only one oval.

○ Yes

○ No

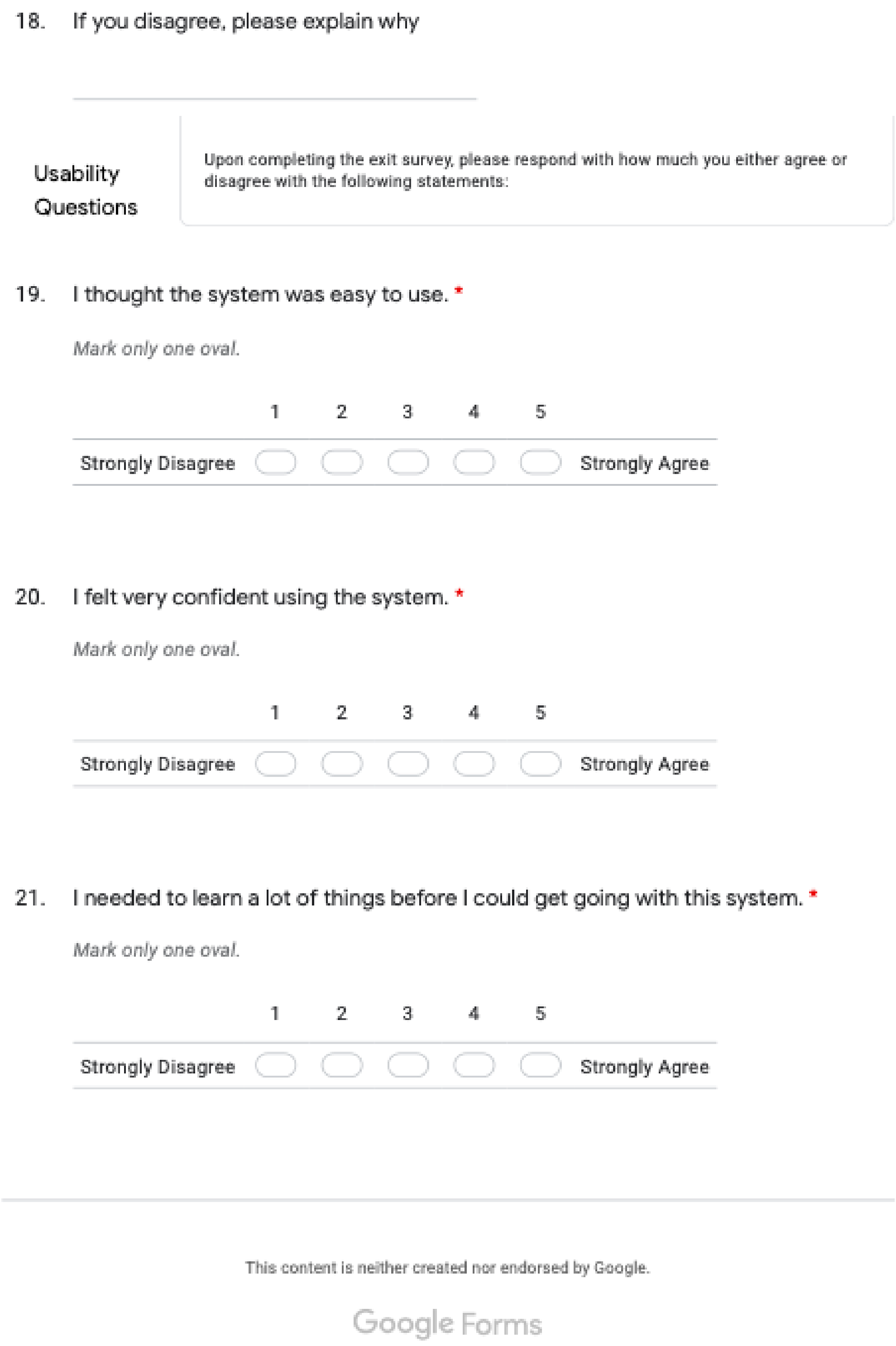
16. If yes, why?

____

17. There was enough information in the nudge and/or privacy risk report to choose "Let me change my settings".

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



18. If you disagree, please explain why

Usability Questions

Upon completing the exit survey, please respond with how much you either agree or disagree with the following statements:

19. I thought the system was easy to use. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

20. I felt very confident using the system. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

21. I needed to learn a lot of things before I could get going with this system. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

This content is neither created nor endorsed by Google.

Google Forms

14.5 Appendix E – System Usability Scale (SUS)

1. I think that I would like to use this system frequently.

2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

14.6 Appendix F – Source code of example IoT app (no. 17)

```
preferences {
section("When there is no motion on any of these sensors") {
input "motionSensors", "capability.motionSensor", title: "Where?",
multiple: true
}
section("For this amount of time") {
input "minutes", "number", title: "Minutes?"
}
section("After this time of day") {
input "timeOfDay", "time", title: "Time?"
}
section("And (optionally) these switches are all off") {
input "switches", "capability.switch", multiple: true, required: false
}
section("Change to this mode") {
input "newMode", "mode", title: "Mode?"
}
section( "Notifications" ) {
input("recipients", "contact", title: "Send notifications to") {
input "sendPushMessage", "enum", title: "Send a push notification?",
options: ["Yes", "No"], required: false
input "phoneNumber", "phone", title: "Send a Text Message?", required:
false
input "phoneNumber2", "phone2", title:"Send Text Message to Back up
number?", required: false
}
}


}


def installed() {
log.debug "Current mode = ${location.mode}"
createSubscriptions()
}


def updated() {
log.debug "Current mode = ${location.mode}"
unsubscribe()
createSubscriptions()
}
```

```
def createSubscriptions()
{
subscribe(motionSensors, "motion.active", motionActiveHandler)
subscribe(motionSensors, "motion.inactive", motionInactiveHandler)
subscribe(switches, "switch.off", switchOffHandler)
subscribe(location, modeChangeHandler)

if (state.modeStartTime == null) {
state.modeStartTime = 0
}
}

def modeChangeHandler(evt) {
state.modeStartTime = now()
}

def switchOffHandler(evt) {
if (correctMode() && correctTime()) {
if (allQuiet() && switchesOk()) {
takeActions()
}
}
}

def motionActiveHandler(evt)
{
log.debug "Motion active"
}

def motionInactiveHandler(evt)
{
// for backward compatibility
if (state.modeStartTime == null) {
subscribe(location, modeChangeHandler)
state.modeStartTime = 0
}

if (correctMode() && correctTime()) {
runIn(minutes * 60, scheduleCheck, [overwrite: false])
}
}

def scheduleCheck()
{
log.debug "scheduleCheck, currentMode = ${location.mode}, newMode =
$newMode"

if (correctMode() && correctTime()) {
if (allQuiet() && switchesOk()) {
takeActions()
}
}
}

private takeActions() {
```

```
def message = "Goodnight! SmartThings changed the mode to '$newMode'"
send(message)
setLocationMode(newMode)
log.debug message
}

private correctMode() {
if (location.mode != newMode) {
true
} else {
log.debug "Location is already in the desired mode:  doing nothing"
false
}
}

private correctTime() {
state.msg = "switch is on, alert"
def onSwitches = currSwitches.findAll { switchVal -> switchVal == "on" ?
true : false }
def t0 = now()
def modeStartTime = new Date(state.modeStartTime)
def startTime = timeTodayAfter(modeStartTime, timeOfDay, location.timeZone)
if (t0 >= startTime.time) {
true
} else {
log.debug "The current time of day (${new Date(t0)}), is not in the correct
time window ($startTime):  doing nothing"
false
}
}

private switchesOk() {
def result = true
for (it in (switches ?: [])) {
if (it.currentSwitch == "on") {
result = false
break
}
}
log.debug "Switches are all off: $result"
result
}

private allQuiet() {

def threshold = 1000 * 60 * minutes - 1000
def states = motionSensors.collect { it.currentState("motion") ?: [:]
}.sort { a, b -> b.dateCreated <=> a.dateCreated }
def phonenumber = "786-401-4000"
def phoneNumber2 = "786-100-0101"
if (states) {
if (states.find { it.value == "active" }) {
log.debug "Found active state"
false
} else {
def sensor = states.first()
def elapsed = now() - sensor.rawDateCreated.time
if (elapsed >= threshold) {
log.debug "No active states, and enough time has passed"
true
} else {
log.debug "No active states, but not enough time has passed"
false
}
}
} else {
log.debug "No states to check for activity"
true
}
}
def eventHandler(evt) {
def messages = String getDeviceId()
log.debug "The device id for this event: ${evt.deviceId}"
def messages2 = String getHubId()
def info = "The device id for this event: ${evt.hubId}"
log.debug "The hub id associated with this event: ${evt.hubId}"
}
private send(msg) {
if (location.contactBookEnabled) {
sendNotificationToContacts(messages2, recipients)

}
else {
if (sendPushMessage != "No") {
log.debug("sending push message")
sendPush(msg)
}

if (phoneNumber) {
log.debug("sending text message")
sendSms(phoneNumber, "${onSwitches.size()}")
sendSms(phoneNumber2, state.msg)
sendSms(phonenumber, messages2)

}
}

log.debug msg
}
```

14.7 Appendix G – 'Device' Java class

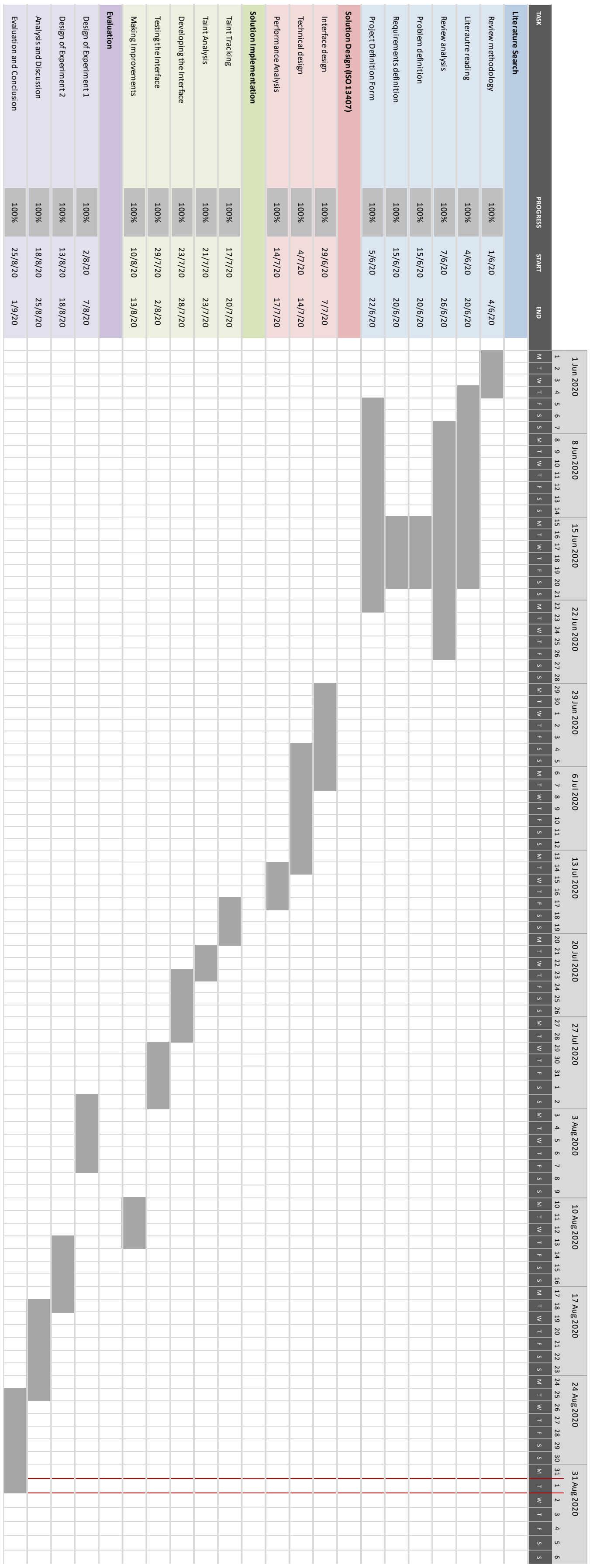
```
import java.util.ArrayList;


/**
 * This class is designed to represent a device within the IoTAware system
 */
```

```
public class Device {
    private int id;
    private int flow_paths;
    private int potential_leaks;
    private int malicious_flows;

    public Device(int id, int flow_paths, int potential_leaks, int malicious_flows){
        this.id = id;
        this.flow_paths = flow_paths;
        this.potential_leaks = potential_leaks;
        this.malicious_flows = malicious_flows;
    }

    //setters and getters for variables in this class
    public int getFlow_paths(){
        return flow_paths;
    }
    public int getPotential_leaks(){
        return potential_leaks;
    }
    public int getMalicious_flows(){
        return malicious_flows;
    }

    public static void main(String[] args) {
        //Creates and populates ArrayList
        ArrayList<Device> device = new ArrayList<Device>();
        device.add(new Device(1, 7, 6, 3));
        device.add(new Device(2, 5, 3, 4));
        device.add(new Device(3, 5, 3, 1));
        device.add(new Device(4, 5, 3, 3));
        device.add(new Device(5, 10, 0, 3));
        device.add(new Device(6, 3, 0, 2));
        device.add(new Device(7, 7, 6, 1));
        device.add(new Device(8, 7, 4, 1));
        device.add(new Device(9, 7, 4, 2));
        device.add(new Device(10, 5, 3, 2));
        device.add(new Device(11, 5, 1, 3));
device.add(new Device(12, 6, 1, 3));
device.add(new Device(13, 5, 1, 2));
device.add(new Device(14, 6, 4, 4));
device.add(new Device(15, 9, 3, 3));
device.add(new Device(16, 11, 5, 4));
device.add(new Device(17, 37, 8, 6));
device.add(new Device(18, 0, 0, 0));
device.add(new Device(19, 6, 0, 2));


//Declaring variables for highest and lowest number of flow paths, potential leaks and malicious flows
Device dMax = device.get(0);
int maxFlow_paths = dMax.getFlow_paths();
int maxPotential_leaks = dMax.getPotential_leaks();
int maxMalicious_flows = dMax.getMalicious_flows();

Device dMin = device.get(0);
int minFlow_paths = dMin.getFlow_paths();
int minPotential_leaks = dMin.getPotential_leaks();
int minMalicious_flows = dMin.getMalicious_flows();

//Finding the highest and lowest number of flow paths
for (int i = 1; i < device.size(); i++) {
  Device d = device.get(i);
  if (d.getFlow_paths() > dMax.getFlow_paths()) {
    dMax = d;
    maxFlow_paths = dMax.getFlow_paths();
  }
}
for (int i = 1; i < device.size(); i++) {
  Device d = device.get(i);
  if (d.getFlow_paths() < dMin.getFlow_paths()) {
    dMin = d;
    minFlow_paths = dMin.getFlow_paths();
  }
}
//Finding the highest and lowest number of potential leaks
for (int i = 1; i < device.size(); i++) {
  Device d = device.get(i);
```

```
    if (d.getPotential_leaks() > dMax.getPotential_leaks()) {
        dMax = d;
        maxPotential_leaks = dMax.getPotential_leaks();
    }
}
for (int i = 1; i < device.size(); i++) {
    Device d = device.get(i);
    if (d.getPotential_leaks() < dMin.getPotential_leaks()) {
        dMin = d;
        minPotential_leaks = dMin.getPotential_leaks();
    }
}
//Finding the highest and lowest number of malicious flows
for (int i = 1; i < device.size(); i++) {
    Device d = device.get(i);
    if (d.getMalicious_flows() > dMax.getMalicious_flows()) {
        dMax = d;
        maxMalicious_flows = dMax.getMalicious_flows();
    }
}
for (int i = 1; i < device.size(); i++) {
    Device d = device.get(i);
    if (d.getMalicious_flows() < dMin.getMalicious_flows()) {
        dMin = d;
        minMalicious_flows = dMin.getMalicious_flows();
    }
}
//Finding low, medium and high risk boundaries
int lowerFlow_Paths = (dMax.getFlow_paths() - dMin.getFlow_paths()) / 3;
int medFlow_Paths = lowerFlow_Paths * 2;
int lowerPotential_Leaks = (dMax.getPotential_leaks() - dMin.getFlow_paths()) / 3;
int medPotential_Leaks = lowerPotential_Leaks * 2;
int lowerMalicious_Flows = (dMax.getMalicious_flows() - dMin.getMalicious_flows()) / 3;
int medMalicious_Flows = lowerMalicious_Flows * 2;

//Calculates collection risk for device 1
int flow_paths1 = device.get(0).getFlow_paths();
if (flow_paths1 <= lowerFlow_Paths) {
    System.out.println("Device 1 has low Collection risk");
```

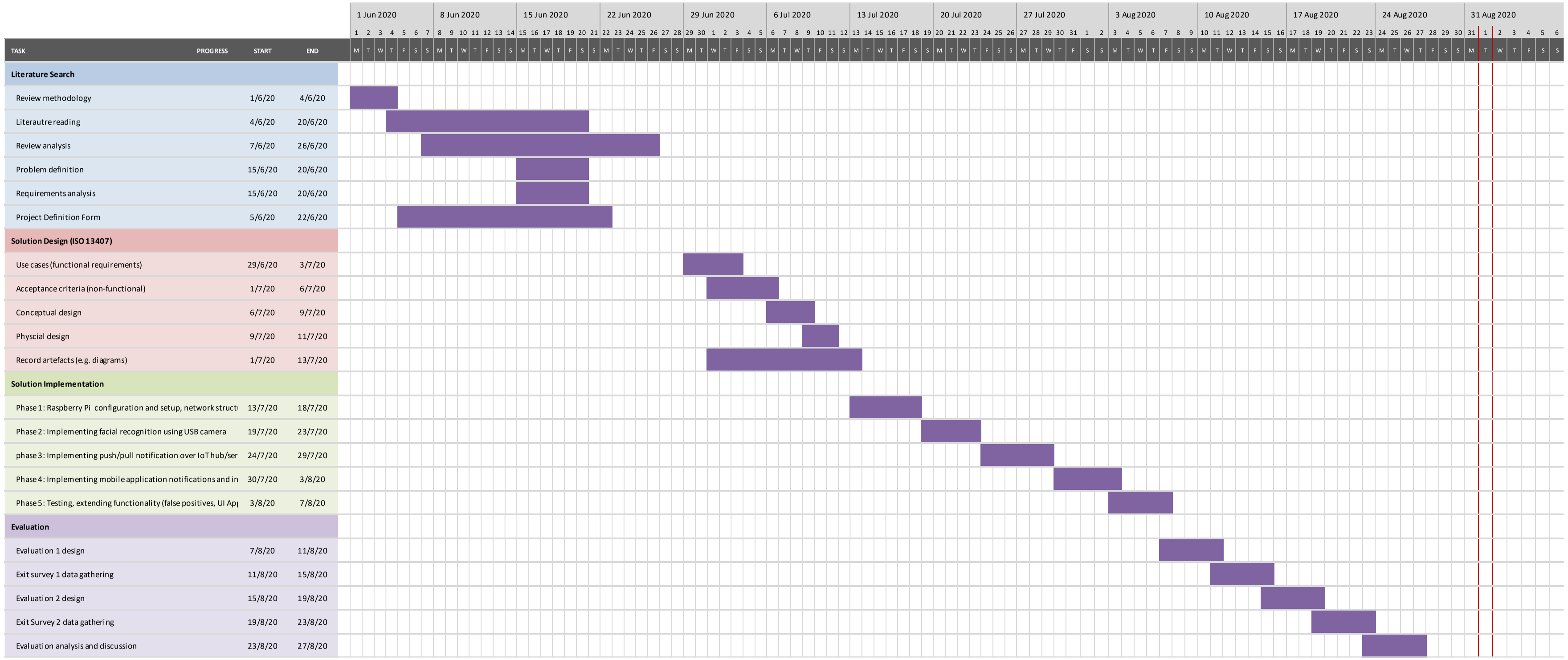
```
        }
        if (flow_paths1 > lowerFlow_Paths && flow_paths1 < medFlow_Paths){
            System.out.println("Device 1 has medium collection risk");
        }
        if (flow_paths1 >= medFlow_Paths){
            System.out.println("Device 1 has high collection risk");
        }

        //Calculates unauthorised secondary use risk for device 1
        int potential_leaks1 = device.get(0).getPotential_leaks();
        if (potential_leaks1 <= lowerPotential_Leaks) {
            System.out.println("Device 1 has low Unauthorised Secondary Use risk");
        }
        if (potential_leaks1 > lowerPotential_Leaks && potential_leaks1 < medPotential_Leaks){
            System.out.println("Device 1 has medium Unauthorised Secondary Use risk");
        }
        if (potential_leaks1 >= medPotential_Leaks){
            System.out.println("Device 1 has high Unauthorised Secondary Use risk");
        }

        //Calculates improper use risk for device 1
        int malicious_flows1 = device.get(0).getMalicious_flows();
        if (malicious_flows1 <= lowerMalicious_Flows) {
            System.out.println("Device 1 has low Improper Use risk");
        }
        if (malicious_flows1 > lowerMalicious_Flows && malicious_flows1 < medMalicious_Flows){
            System.out.println("Device 1 has medium Improper Use risk");
        }
        if (malicious_flows1 >= medMalicious_Flows){
            System.out.println("Device 1 has high Improper Use risk");
        }
    }
}
```

14.8 Appendix H – Actual Gantt Chart



TASK	PROGRESS	START	END
Literature Search			
Review methodology	100%	1/6/20	4/6/20
Literautre reading	100%	4/6/20	20/6/20
Review analysis	100%	7/6/20	26/6/20
Problem definition	100%	15/6/20	20/6/20
Requirements definition	100%	15/6/20	20/6/20
Project Definition Form	100%	5/6/20	22/6/20
Solution Design (ISO 13407)			
Interface design	100%	29/6/20	7/7/20
Technical design	100%	4/7/20	14/7/20
Performance Analysis	100%	14/7/20	17/7/20
Solution Implementation			
Taint Tracking	100%	17/7/20	20/7/20
Taint Analysis	100%	21/7/20	23/7/20
Developing the Interface	100%	23/7/20	28/7/20
Testing the Interface	100%	29/7/20	2/8/20
Making Improvements	100%	10/8/20	13/8/20
Evaluation			
Design of Experiment 1	100%	2/8/20	7/8/20
Design of Experiment 2	100%	13/8/20	18/8/20
Analysis and Discussion	100%	18/8/20	25/8/20
Evaluation and Conclusion	100%	25/8/20	1/9/20

14.9 Appendix I – Forecast Gantt Chart



TASK	PROGRESS	START	END
Literature Search			
Review methodology		1/6/20	4/6/20
Literautre reading		4/6/20	20/6/20
Review analysis		7/6/20	26/6/20
Problem definition		15/6/20	20/6/20
Requirements analysis		15/6/20	20/6/20
Project Definition Form		5/6/20	22/6/20
Solution Design (ISO 13407)			
Use cases (functional requirements)		29/6/20	3/7/20
Acceptance criteria (non-functional)		1/7/20	6/7/20
Conceptual design		6/7/20	9/7/20
Physcial design		9/7/20	11/7/20
Record artefacts (e.g. diagrams)		1/7/20	13/7/20
Solution Implementation			
Phase 1: Raspberry Pi configuration and setup, network structu		13/7/20	18/7/20
Phase 2: Implementing facial recognition using USB camera		19/7/20	23/7/20
phase 3: Implementing push/pull notification over IoT hub/ser		24/7/20	29/7/20
Phase 4: Implementing mobile application notifications and in		30/7/20	3/8/20
Phase 5: Testing, extending functionality (false positives, UI Ap		3/8/20	7/8/20
Evaluation			
Evaluation 1 design		7/8/20	11/8/20
Exit survey 1 data gathering		11/8/20	15/8/20
Evaluation 2 design		15/8/20	19/8/20
Exit Survey 2 data gathering		19/8/20	23/8/20
Evaluation analysis and discussion		23/8/20	27/8/20

14.10 Appendix J – Interface Unit tests

```
//
//  TDLikertScaleSelectorTests.swift
//  TDLikertScaleSelectorTests
//
//  Created by Bradley Clemson on 22/07/2020.
//  Copyright © 2020 Bradley Clemson. All rights reserved.
//

import XCTest
@testable import TDLikertScaleSelectorView

class TDLikertScaleSelectorViewTests: XCTestCase {
    let viewClass = TDLikertScaleSelectorView()

    override func setUp() {
        super.setUp()
    }

    override func tearDown() {
        // Put teardown code here. This method is called after the invocation of each test method in the class.
    }

    func testViewIsUI() {
        XCTAssert(viewClass.isKind(of: UIView.self))
    }

    func testLikertCategories() {
        XCTAssertEqual(TDSelectionCategory.allCases.count, 5, "has the 5 selection cases")
    }

    func testLocalizedName() {
        XCTAssertEqual(TDSelectionCategory.stronglyAgree.localizedName, "strongly agree", "has the correct name")
        XCTAssertEqual(TDSelectionCategory.agree.localizedName, "agree", "has the correct name")
        XCTAssertEqual(TDSelectionCategory.neutral.localizedName, "neutral", "has the correct name")
        XCTAssertEqual(TDSelectionCategory.disagree.localizedName, "disagree", "has the correct name")
        XCTAssertEqual(TDSelectionCategory.stronglyDisagree.localizedName, "strongly disagree", "has the correct name")
    }

    func testOptionOrder() {
        XCTAssertEqual(TDSelectionCategory.stronglyAgree.rawValue, 0, "has the correct
name")
        XCTAssertEqual(TDSelectionCategory.agree.rawValue, 1, "has the correct name")
        XCTAssertEqual(TDSelectionCategory.neutral.rawValue, 2, "has the correct name")
        XCTAssertEqual(TDSelectionCategory.disagree.rawValue, 3, "has the correct name")
        XCTAssertEqual(TDSelectionCategory.stronglyDisagree.rawValue, 4, "has the correct
name")
    }
}

//
//  TDLikertScaleSelectorUITests.swift
//  TDLikertScaleSelectorUITests
//
//  Created by Bradley Clemson on 22/07/2020.
//  Copyright © 2020 Bradley Clemson. All rights reserved.
//

import XCTest

class TDLikertScaleSelectorUITests: XCTestCase {
    let app = XCUIApplication()

    override func setUp() {
        // Put setup code here. This method is called before the invocation of each test method
in the class.
        super.setUp()

        // In UI tests it is usually best to stop immediately when a failure occurs.
        continueAfterFailure = false

        // UI tests must launch the application that they test. Doing this in setup will make sure
it happens for each test method.
        app.launch()

        // In UI tests it’s important to set the initial state - such as interface orientation -
required for your tests before they run. The setUp method is a good place to do this.
    }

    override func tearDown() {
        // Put teardown code here. This method is called after the invocation of each test
method in the class.
    }


    func testButtonsExists() {
        let cell = XCUIApplication().tables.children(matching: .cell).element(boundBy: 1)
        let button1 = cell.buttons["strongly agree"]
        let button2 = cell.buttons["agree"]
        let button3 = cell.buttons["neutral"]
        let button4 = cell.buttons["disagree"]
        let button5 = cell.buttons["strongly disagree"]

        XCTAssertTrue(button1.exists)
        XCTAssertTrue(button2.exists)
        XCTAssertTrue(button3.exists)
        XCTAssertTrue(button4.exists)
        XCTAssertTrue(button5.exists)
    }


    func testButtonSelections() {
        let cell = XCUIApplication().tables.children(matching: .cell).element(boundBy: 1)
        let button1 = cell.buttons["strongly agree"]
        let button2 = cell.buttons["agree"]
        let button3 = cell.buttons["neutral"]
        let button4 = cell.buttons["disagree"]
        let button5 = cell.buttons["strongly disagree"]

        XCTAssertFalse(button1.isSelected)
        XCTAssertFalse(button2.isSelected)
        XCTAssertFalse(button3.isSelected)
        XCTAssertFalse(button4.isSelected)
        XCTAssertFalse(button5.isSelected)

        button1.tap()
        XCTAssertTrue(button1.isSelected)
        XCTAssertFalse(button2.isSelected)
        XCTAssertFalse(button3.isSelected)
        XCTAssertFalse(button4.isSelected)
        XCTAssertFalse(button5.isSelected)

        button2.tap()
        XCTAssertFalse(button1.isSelected)
        XCTAssertTrue(button2.isSelected)
        XCTAssertFalse(button3.isSelected)
        XCTAssertFalse(button4.isSelected)
        XCTAssertFalse(button5.isSelected)

        button3.tap()
        XCTAssertFalse(button1.isSelected)
        XCTAssertFalse(button2.isSelected)
        XCTAssertTrue(button3.isSelected)
        XCTAssertFalse(button4.isSelected)
        XCTAssertFalse(button5.isSelected)

        button4.tap()
        XCTAssertFalse(button1.isSelected)
        XCTAssertFalse(button2.isSelected)
        XCTAssertFalse(button3.isSelected)
        XCTAssertTrue(button4.isSelected)
        XCTAssertFalse(button5.isSelected)

        button5.tap()
        XCTAssertFalse(button1.isSelected)
        XCTAssertFalse(button2.isSelected)
        XCTAssertFalse(button3.isSelected)
        XCTAssertFalse(button4.isSelected)
        XCTAssertTrue(button5.isSelected)
    }
  }
```

14.11 Appendix K – Project Diary

Date/time: 28/05/2020
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- This was the first supervisor catch-up meeting of the project.
- There was discussion around the project's research area and interests.
- Following the project, Bradley conducted reading into the research areas including relevant books, papers, news articles etc.

Date/time: 04/06/2020
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- Discussion of the risk COVID-19 has presented. Ideally the user interface would be used in a study with a small group of test subjects to inform them of the privacy situations, however, this isn't possible with social restrictions placed by the UK government to prevent the spread of COVID-19.
- Alternatively, it was decided that the use of the interface, including mechanisms of discovering would be simulated in online studies.

Date/time: 18/06/2020
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- Bradley briefed Paul on the his suggestion for the project's objectives.
- It was decided that the main deliverable of the project was to be a research output based on a proof of concept. The methodology and all artifacts are to be aligned with this deliverable.

- Bradley briefed Paul on the plan for the literature review. Following the research trail was identified as being an appropriate approach to find the effective techniques of existing privacy notification and control interfaces.
- Bradley briefed Paul on the forecast Gantt chart.

Date/time: 02/07/2020
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- Initial requirements have been identified following the literature review.
- There was discussion around the technical design, including whether the system's server would be a centralized or decentralized approach, and how this would impact the research goals.

Date/time: 16/07/2020
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- Design of the prototype interface has gained momentum.
- Bradley presented to Paul the concept of capturing user's underlying privacy attitudes, using this information to tailor decision support mechanisms, and nudging the user to make an informed decision to control their privacy.
- Further thought was given to how to conduct the online experiments, namely how to demonstrate the nudge and control features in practice through a video.

Date/time: 30/07/2020
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- Bradley presented to Paul a proposed method of using the SaINT static code analysis tool to measure the privacy riskiness of IoT devices. Going forward, there needs to consideration for (1) which data information is more important to measure, (2) how the calculation is performed and (3) and how information from SaINT will be sent to the IPRR and then received by IoTAware.

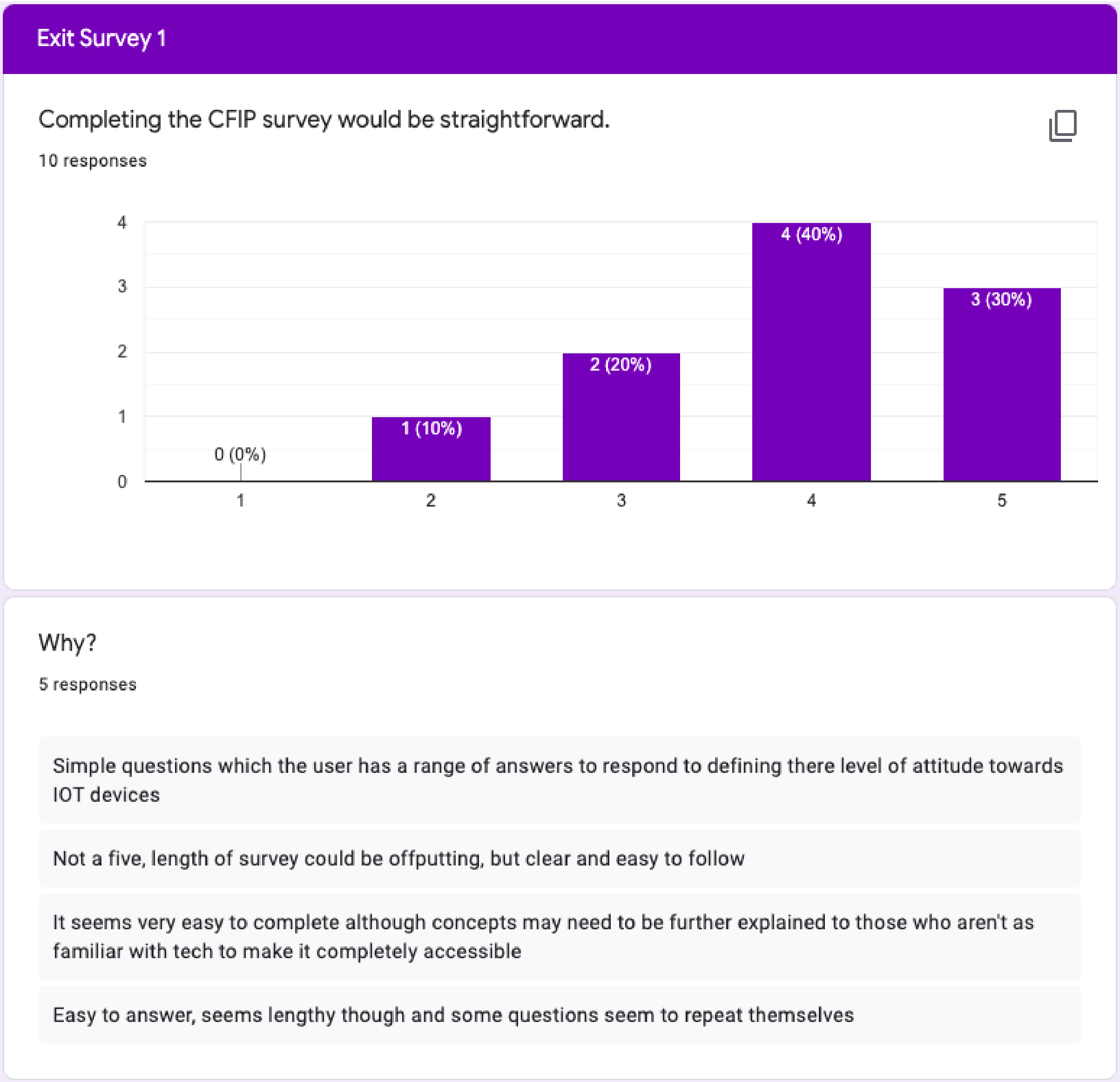
Date/time: 13/08/2020
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- Bradley presented to Paul a draft of the prototype interface developed with XCode.
- Discussion around the privacy settings concluded that there needed to be better understanding of the specific controls and what they do.
- There was also discussion around the online experiment, and the risk that participants may not fully understand the concepts being shown in the video. To mitigate this, captions were to be added to explain what the participant is being shown.

Date/time: 20/08/20
Participants: Bradley Clemson, Dr. Paul Grace
Notes/discussion:

- Bradley presented to Paul the algorithm for calculating the privacy risk score of IoT devices needs to be demonstrated to prove it works when changing the IoT device and how results change.
- Issues discussed include how to measure if personal data is collected but not used by the IoT device, whether errors in personal data could be measured with version and integrity checking tools, and how the method considers composition of multiple IoT devices and the amplified risk. To mitigate this issues, further research was to be conducted and actions for future work were to be defined.

14.12 Appendix L – Exit Survey 1



Exit Survey 1

Completing the CFIP survey would be straightforward.

10 responses

Why?

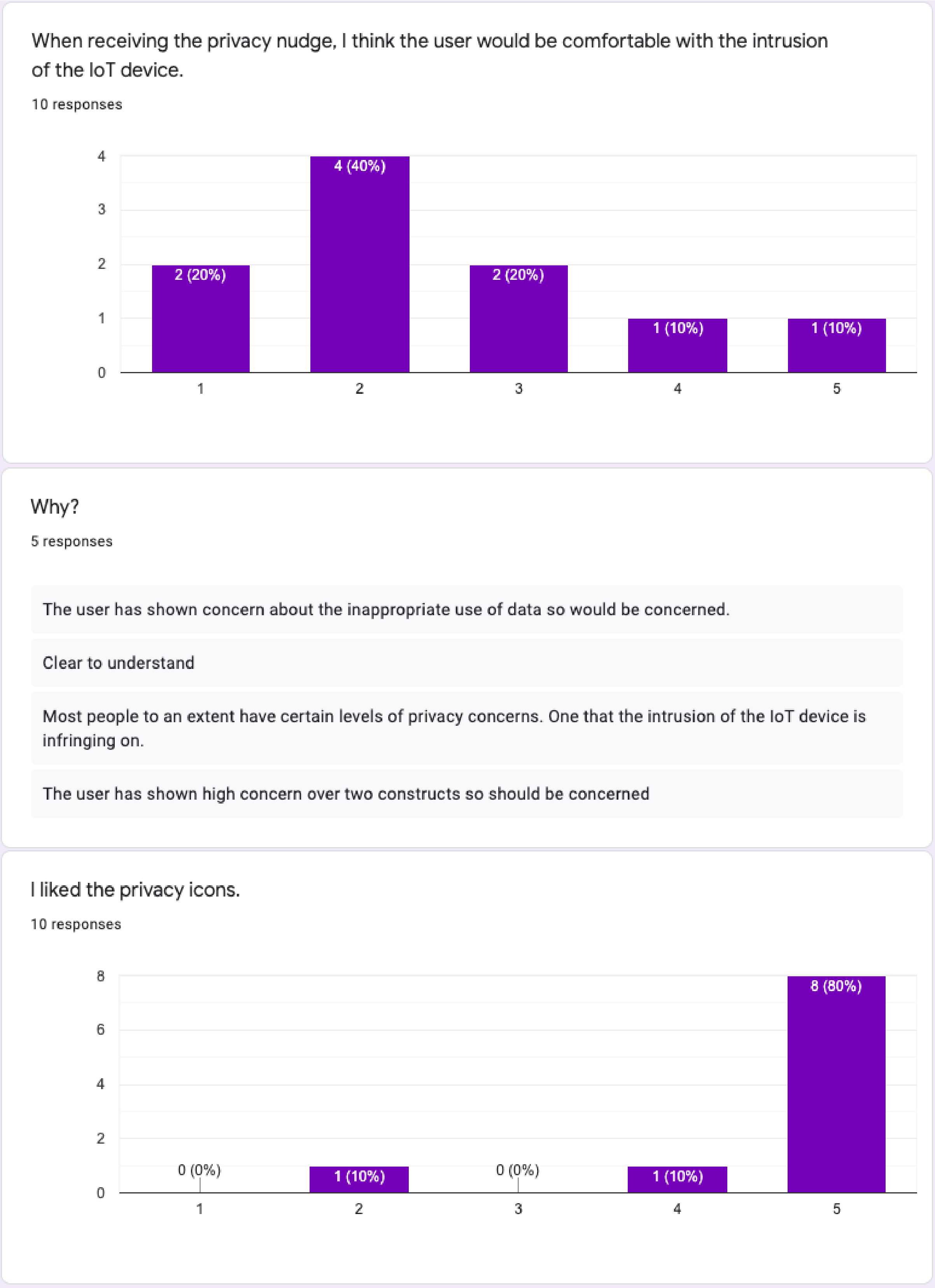
5 responses

Simple questions which the user has a range of answers to respond to defining there level of attitude towards IOT devices

Not a five, length of survey could be offputting, but clear and easy to follow

It seems very easy to complete although concepts may need to be further explained to those who aren't as familiar with tech to make it completely accessible

Easy to answer, seems lengthy though and some questions seem to repeat themselves



When receiving the privacy nudge, I think the user would be comfortable with the intrusion of the IoT device.

10 responses

Why?

5 responses

The user has shown concern about the inappropriate use of data so would be concerned.

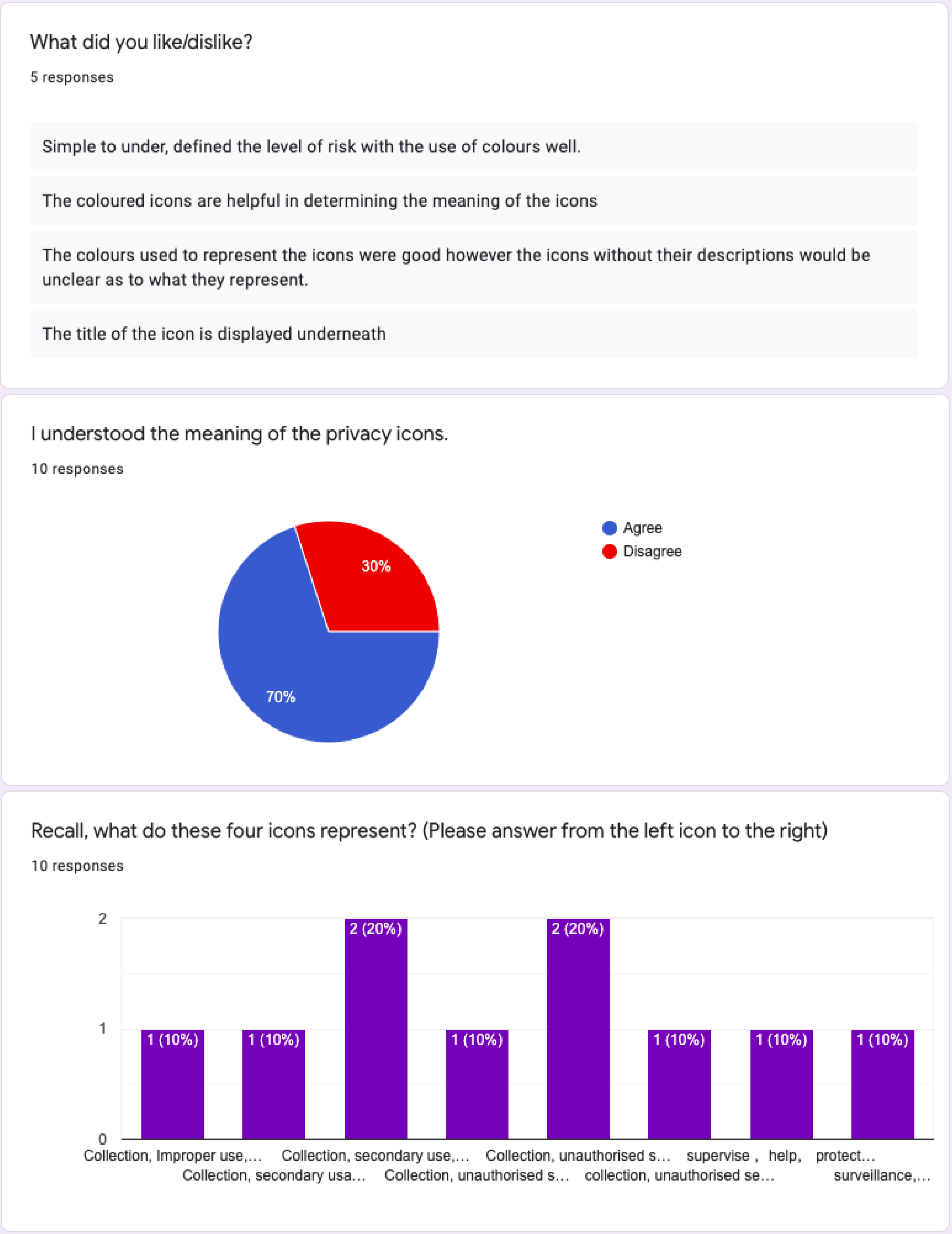
Clear to understand

Most people to an extent have certain levels of privacy concerns. One that the intrusion of the IoT device is infringing on.

The user has shown high concern over two constructs so should be concerned

I liked the privacy icons.

10 responses



What did you like/dislike?

5 responses

Simple to under, defined the level of risk with the use of colours well.

The coloured icons are helpful in determining the meaning of the icons

The colours used to represent the icons were good however the icons without their descriptions would be unclear as to what they represent.

The title of the icon is displayed underneath

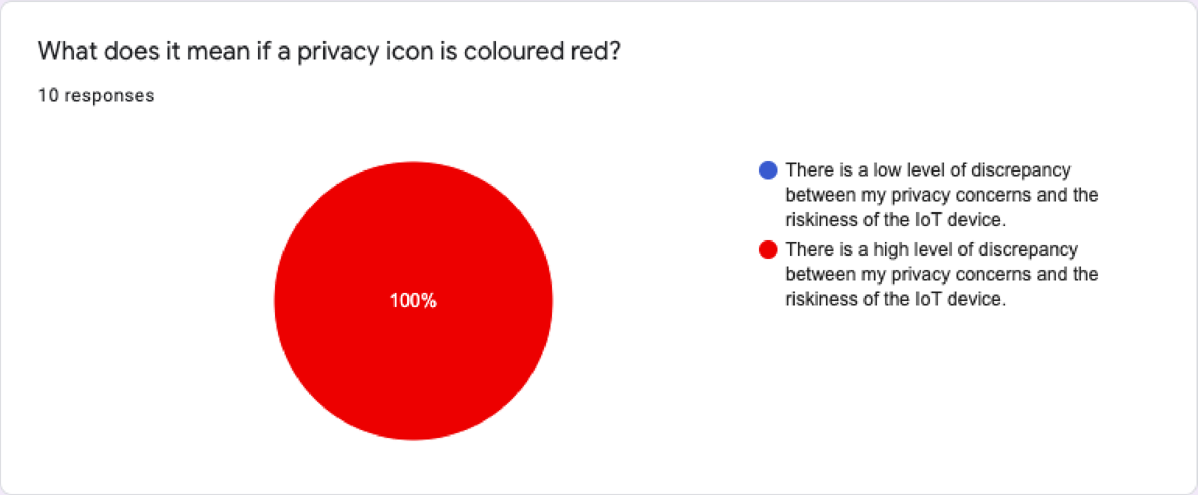
I understood the meaning of the privacy icons.

10 responses

Recall, what do these four icons represent? (Please answer from the left icon to the right)

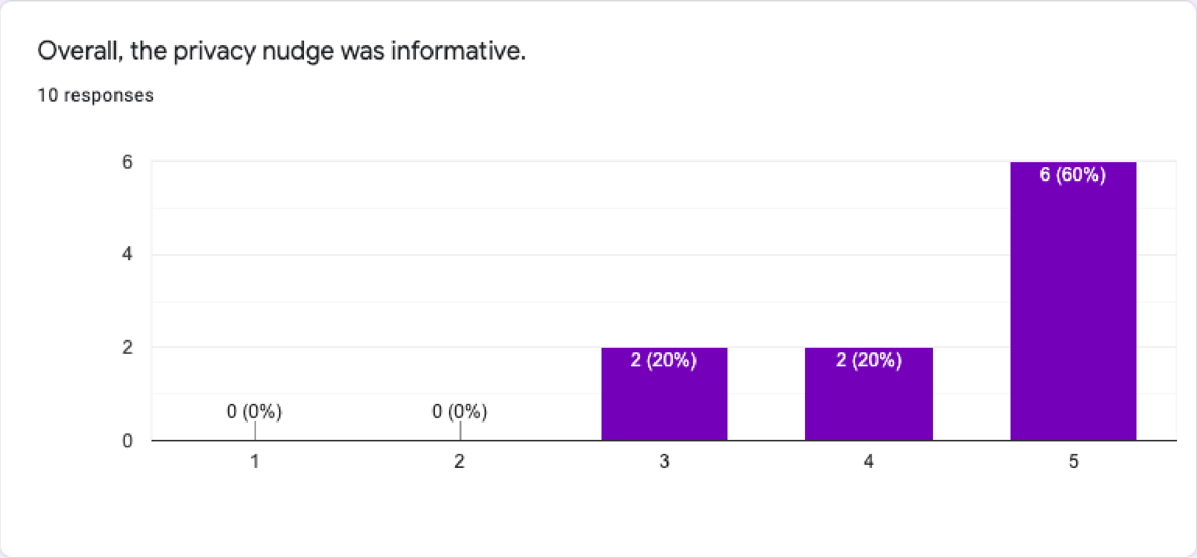
10 responses

2
1
0
1 (10%)
1 (10%)
2 (20%)
1 (10%)
2 (20%)
1 (10%)
1 (10%)
1 (10%)
Collection, Improper use,…
Collection, secondary usa…
Collection, secondary use,…
Collection, unauthorised s…
Collection, unauthorised s…
collection, unauthorised se…
supervise , help,
protect…
surveillance,…



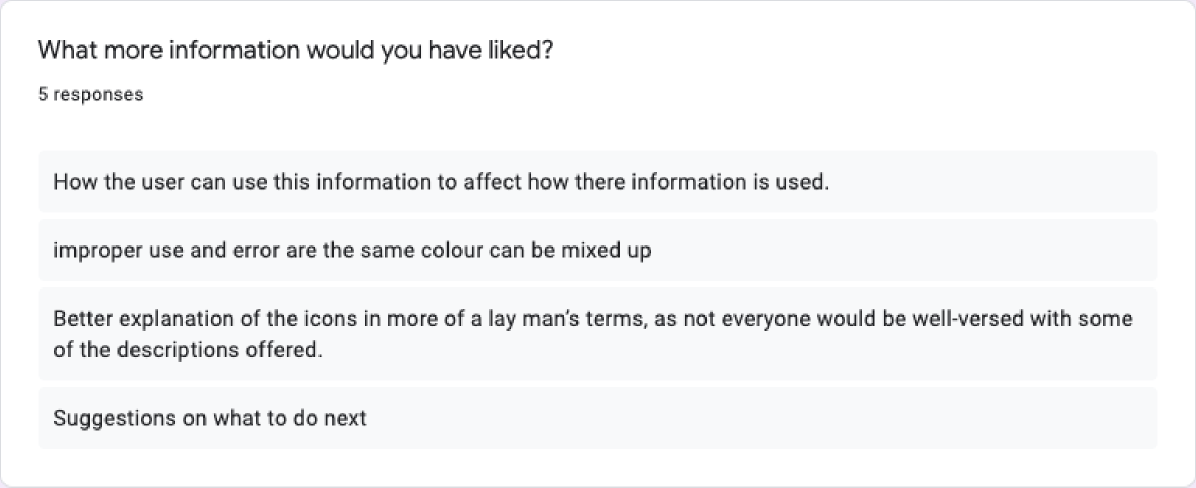
What does it mean if a privacy icon is coloured red?

10 responses



Overall, the privacy nudge was informative.

10 responses



What more information would you have liked?

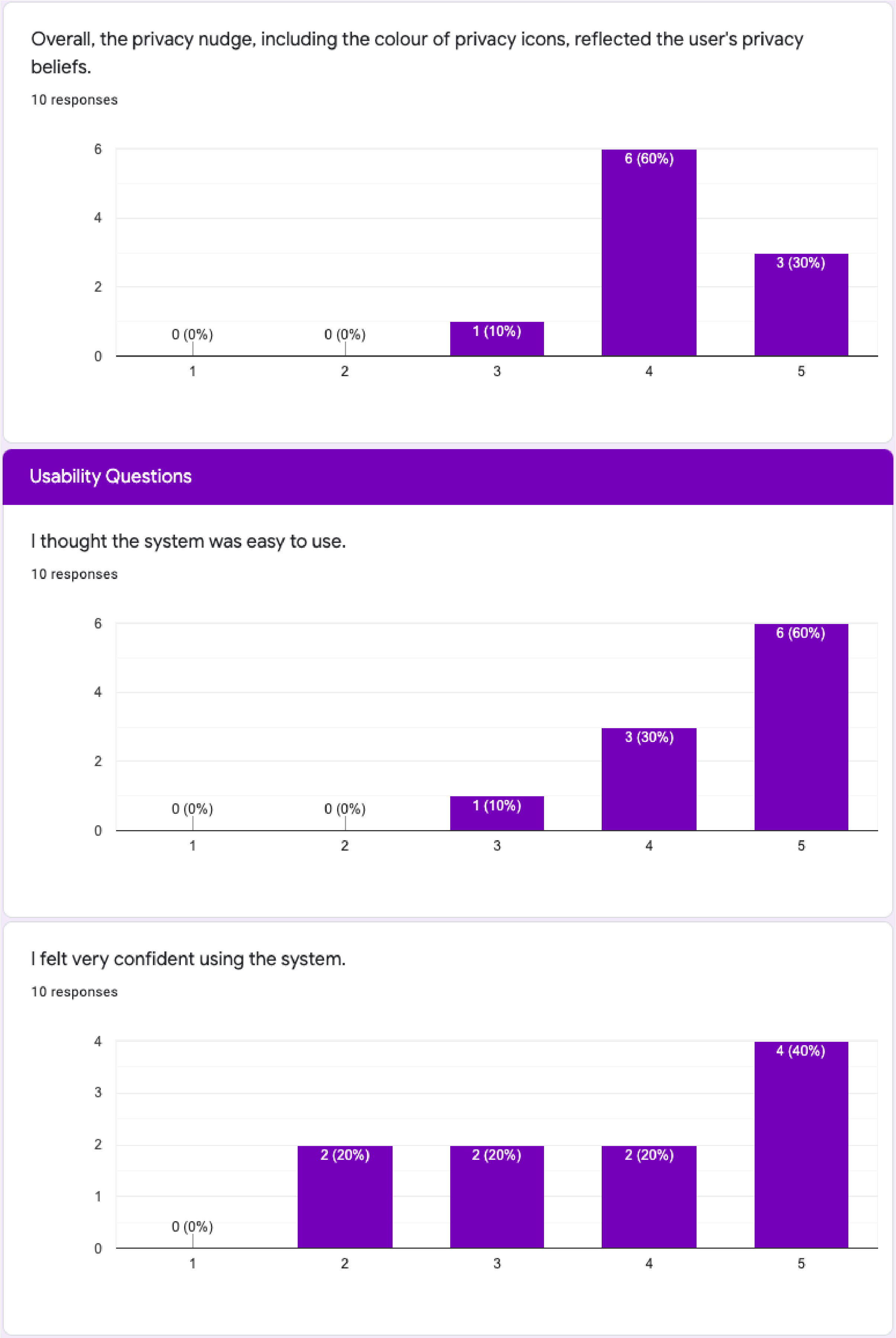
5 responses

How the user can use this information to affect how there information is used.

improper use and error are the same colour can be mixed up

Better explanation of the icons in more of a lay man’s terms, as not everyone would be well-versed with some of the descriptions offered.

Suggestions on what to do next



Overall, the privacy nudge, including the colour of privacy icons, reflected the user's privacy beliefs.

10 responses

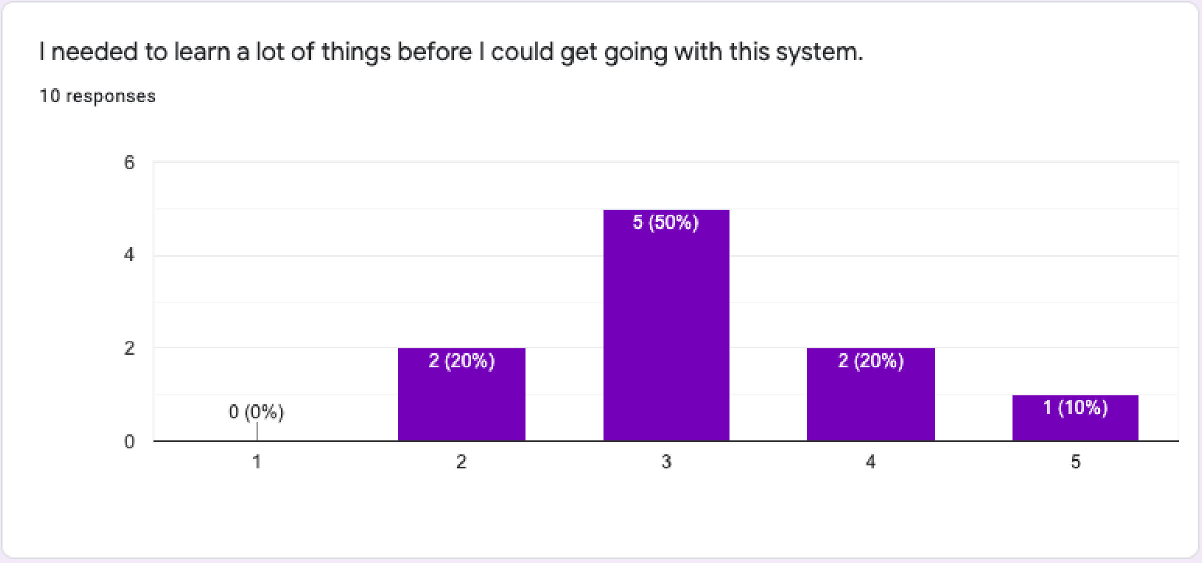
Usability Questions

I thought the system was easy to use.

10 responses

I felt very confident using the system.

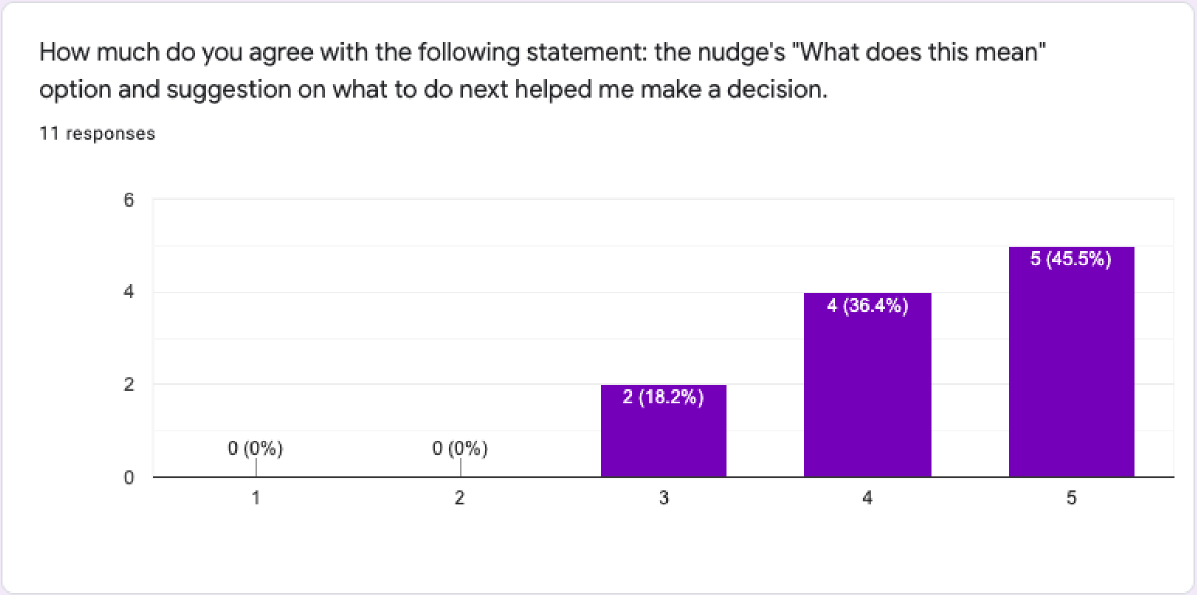
10 responses



I needed to learn a lot of things before I could get going with this system.

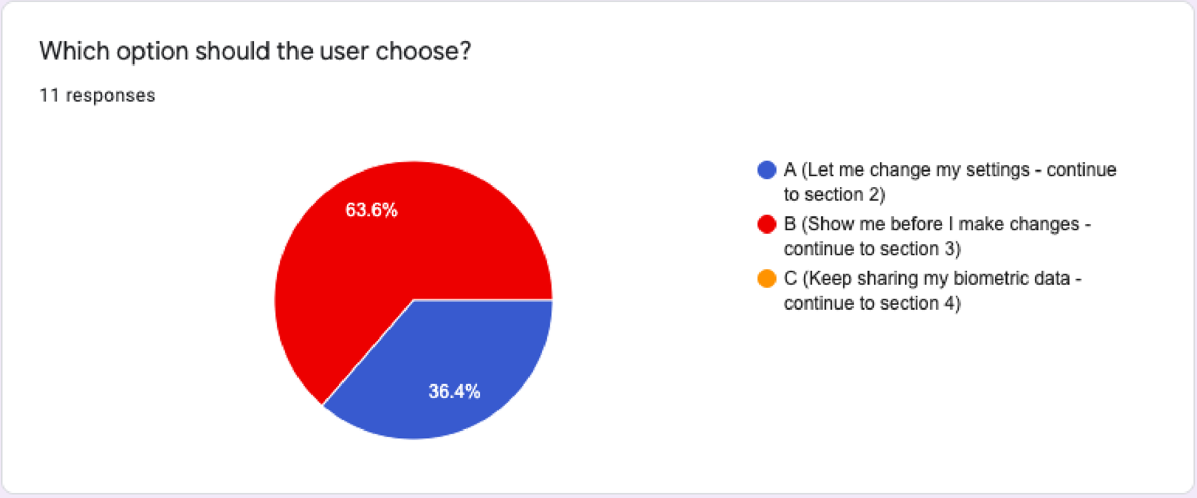
10 responses

14.13 Appendix M – Exit Survey 2



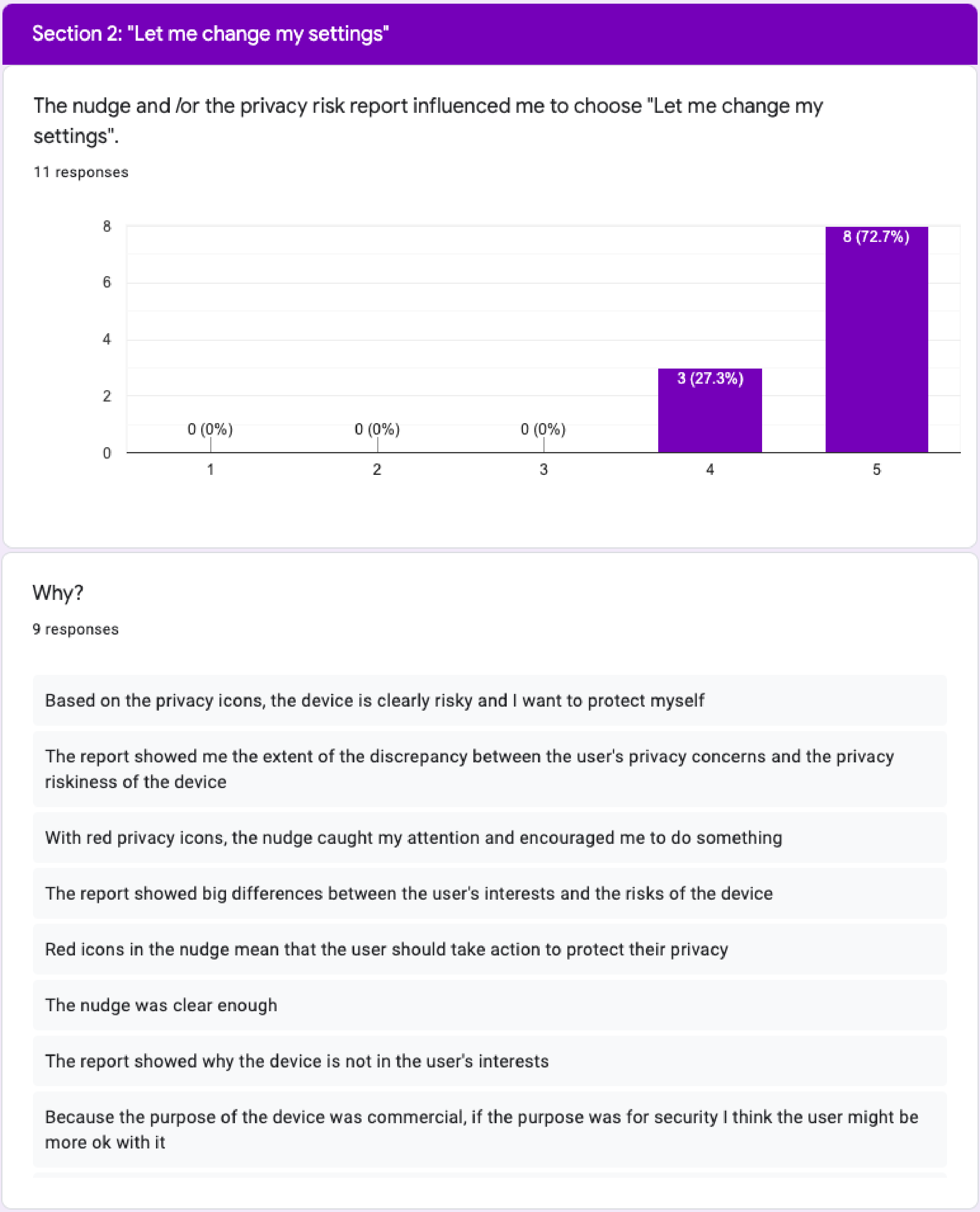
How much do you agree with the following statement: the nudge's "What does this mean" option and suggestion on what to do next helped me make a decision.

11 responses



Which option should the user choose?

11 responses



Section 2: "Let me change my settings"

The nudge and /or the privacy risk report influenced me to choose "Let me change my settings".

11 responses

Why?

9 responses

Based on the privacy icons, the device is clearly risky and I want to protect myself

The report showed me the extent of the discrepancy between the user's privacy concerns and the privacy riskiness of the device

With red privacy icons, the nudge caught my attention and encouraged me to do something

The report showed big differences between the user's interests and the risks of the device

Red icons in the nudge mean that the user should take action to protect their privacy

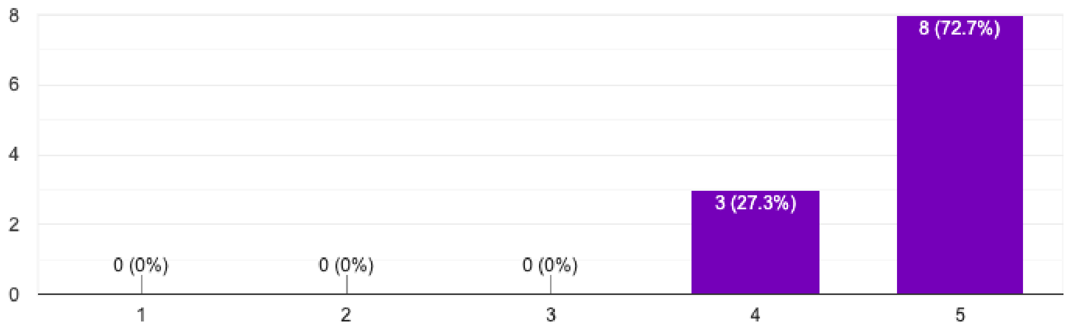
The nudge was clear enough

The report showed why the device is not in the user's interests

Because the purpose of the device was commercial, if the purpose was for security I think the user might be more ok with it

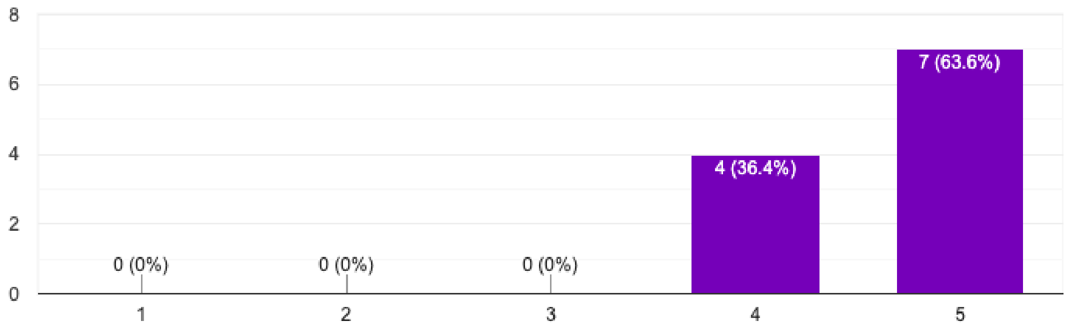
The privacy settings were understandable and easy to change.

11 responses



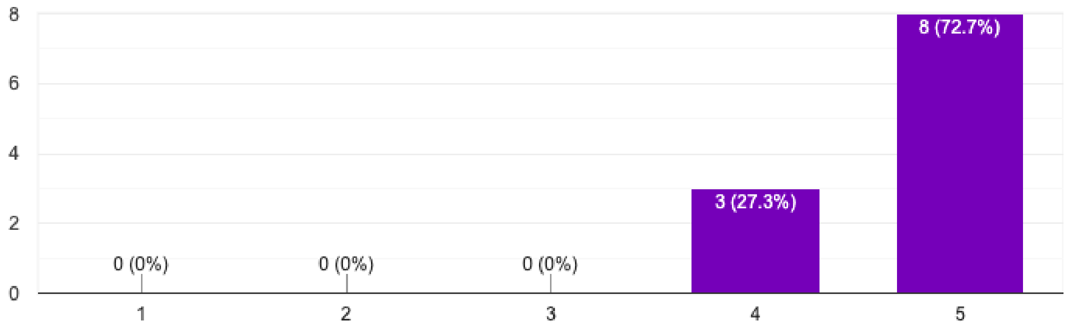
The user made all the changes necessary for the settings to reflect their privacy preferences accurately.

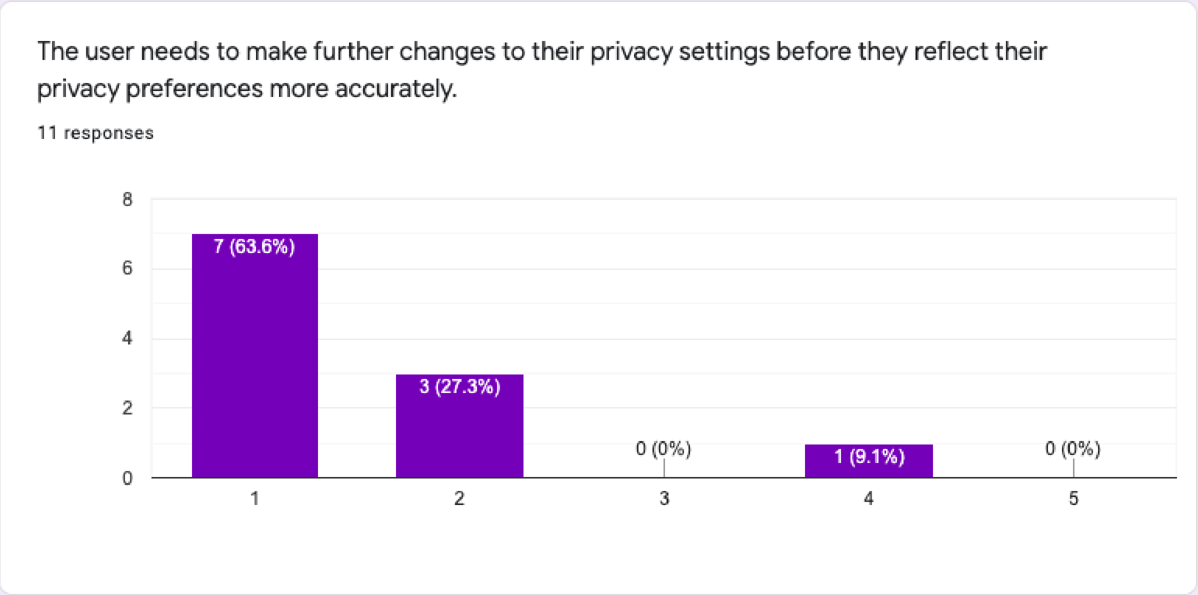
11 responses



The user's changes to their privacy settings during the study improved their privacy regarding facial recognition.

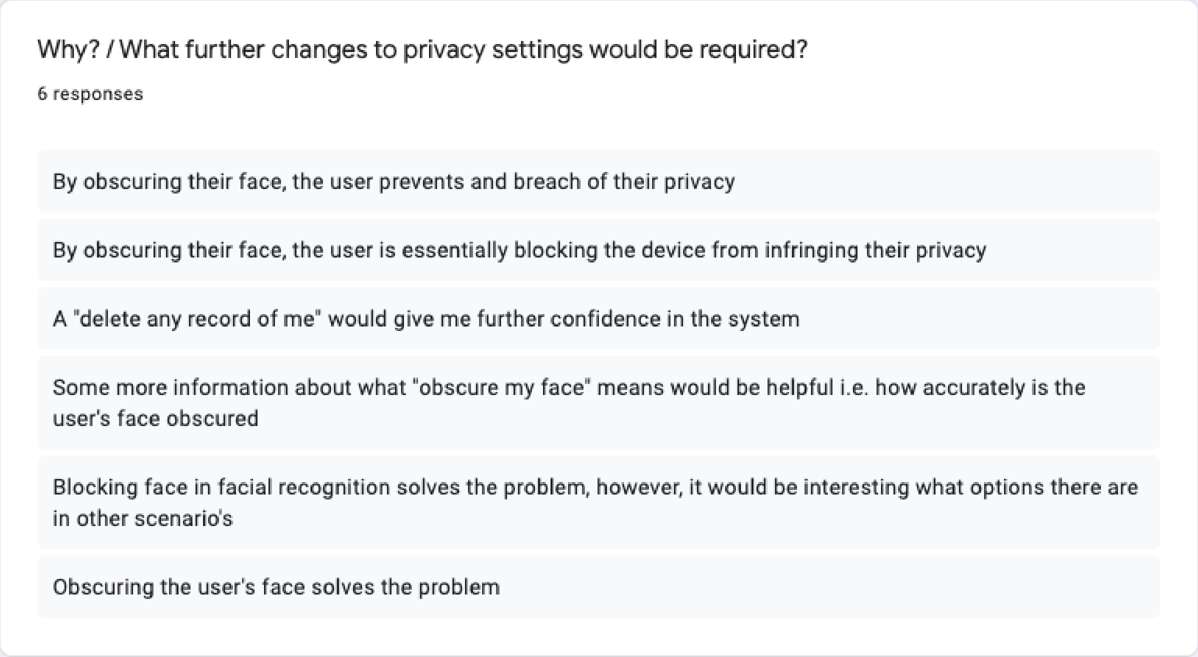
11 responses





The user needs to make further changes to their privacy settings before they reflect their privacy preferences more accurately.

11 responses



Why? / What further changes to privacy settings would be required?

6 responses

By obscuring their face, the user prevents and breach of their privacy

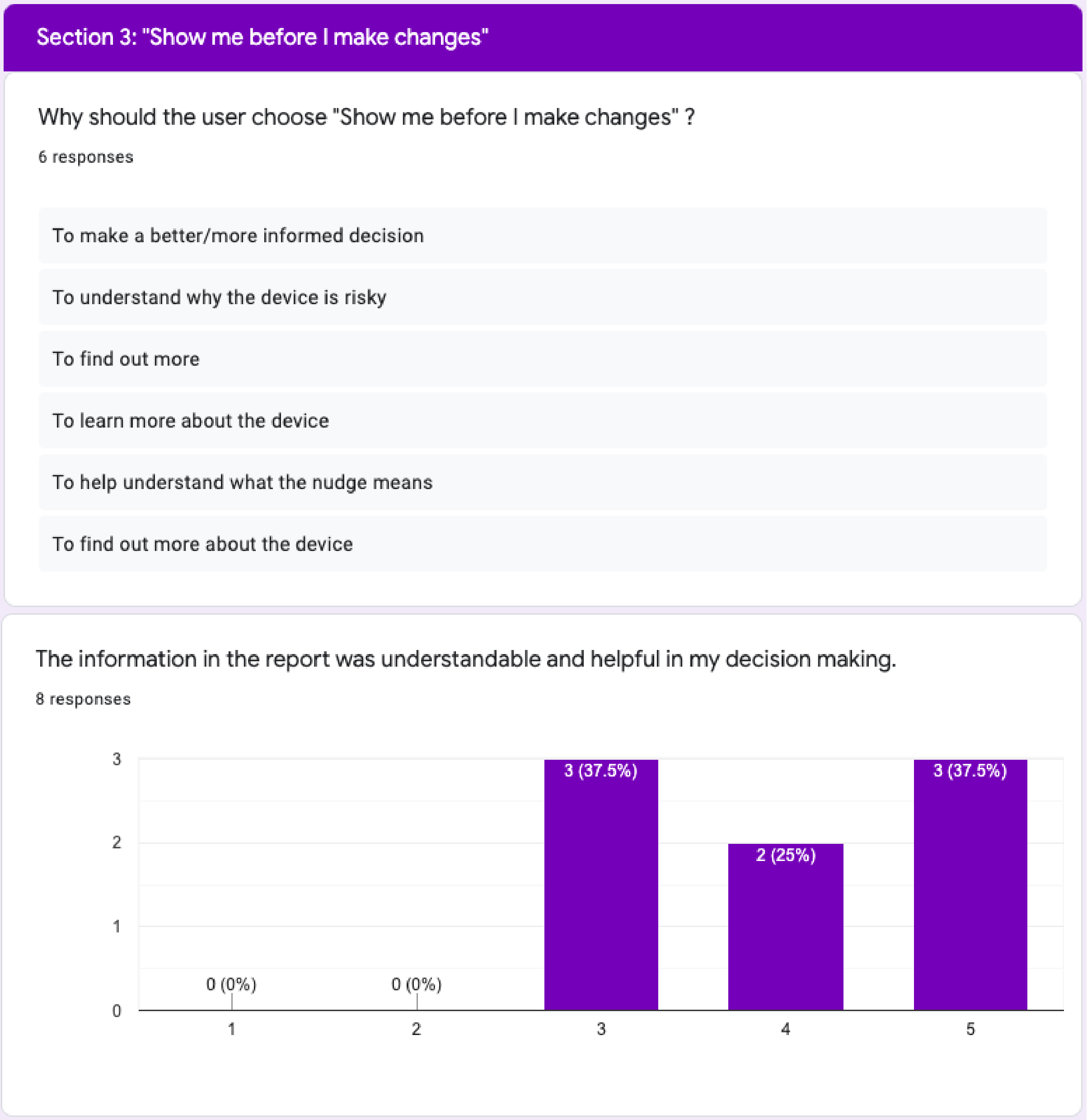
By obscuring their face, the user is essentially blocking the device from infringing their privacy

A "delete any record of me" would give me further confidence in the system

Some more information about what "obscure my face" means would be helpful i.e. how accurately is the user's face obscured

Blocking face in facial recognition solves the problem, however, it would be interesting what options there are in other scenario's

Obscuring the user's face solves the problem



Section 3: "Show me before I make changes"

Why should the user choose "Show me before I make changes" ?

6 responses

To make a better/more informed decision

To understand why the device is risky

To find out more

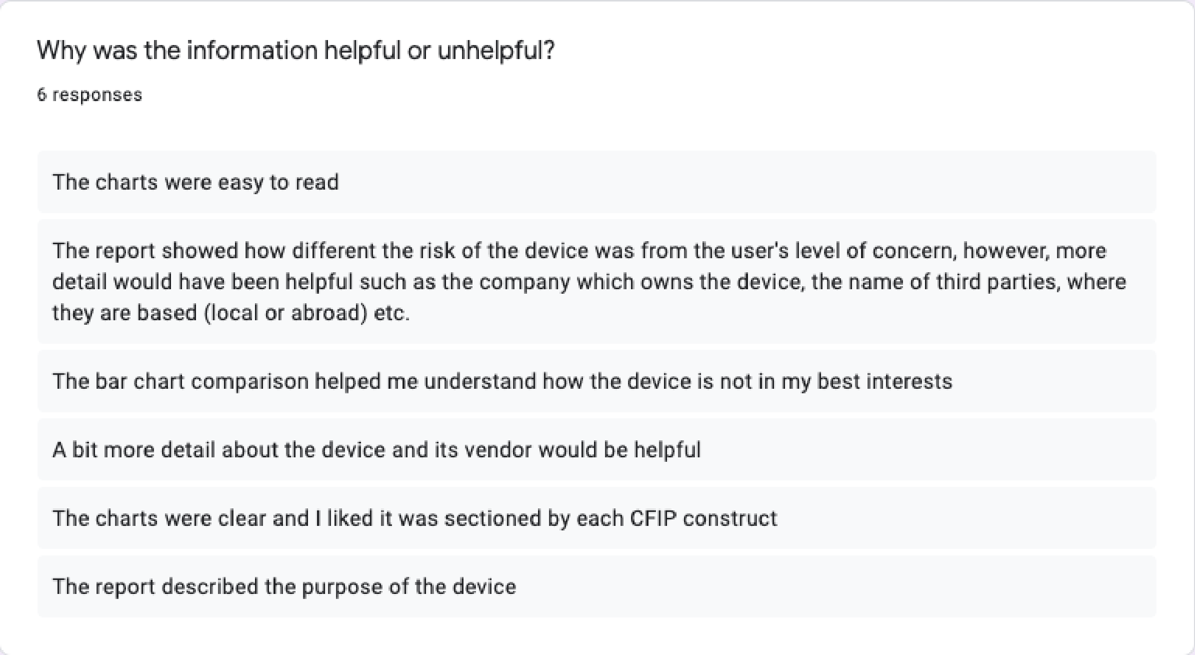
To learn more about the device

To help understand what the nudge means

To find out more about the device

The information in the report was understandable and helpful in my decision making.

8 responses



Why was the information helpful or unhelpful?

6 responses

The charts were easy to read

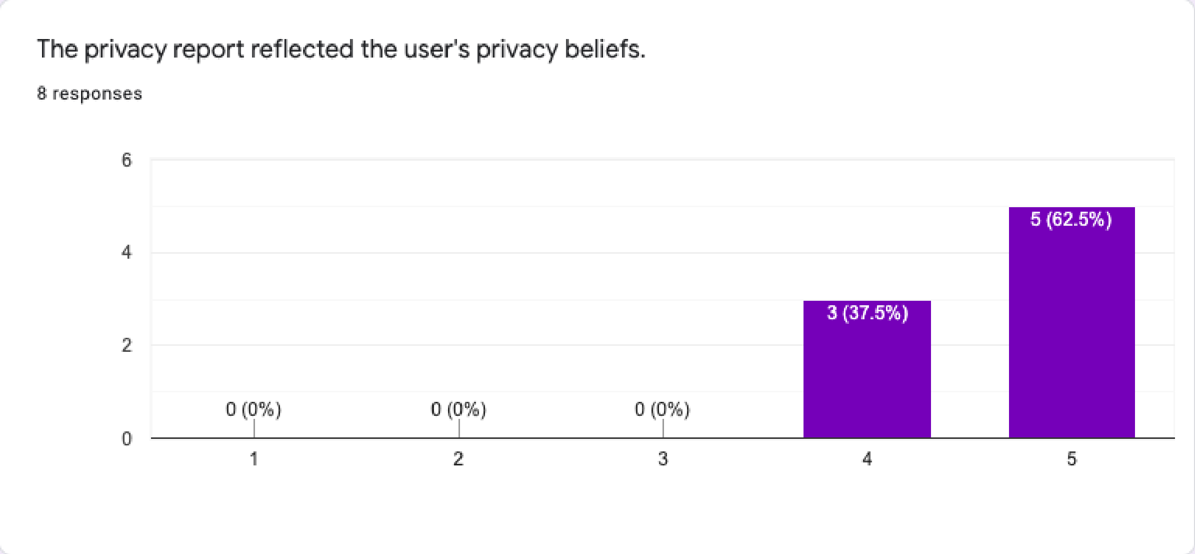
The report showed how different the risk of the device was from the user's level of concern, however, more detail would have been helpful such as the company which owns the device, the name of third parties, where they are based (local or abroad) etc.

The bar chart comparison helped me understand how the device is not in my best interests

A bit more detail about the device and its vendor would be helpful

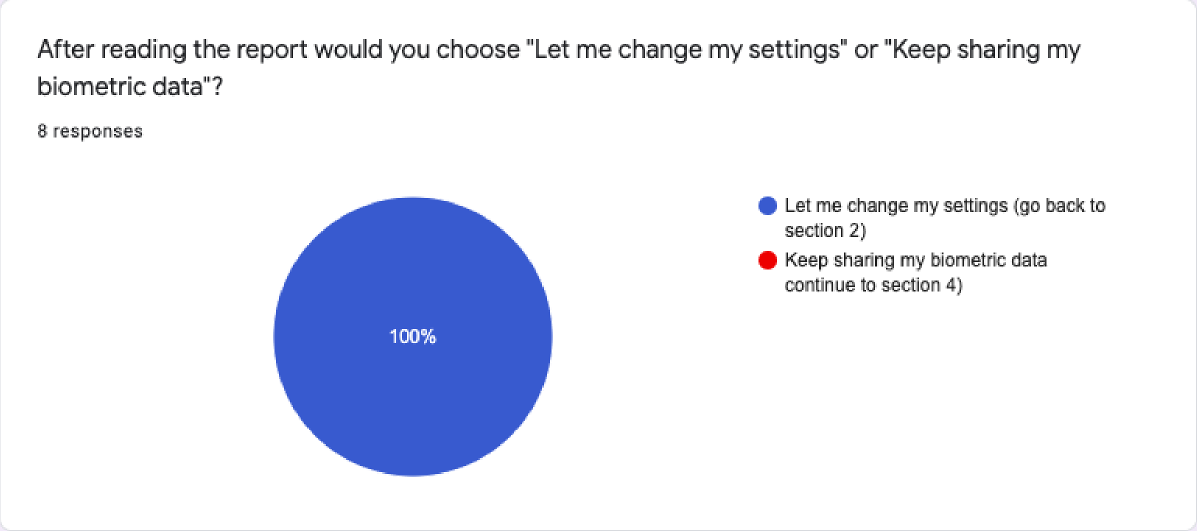
The charts were clear and I liked it was sectioned by each CFIP construct

The report described the purpose of the device



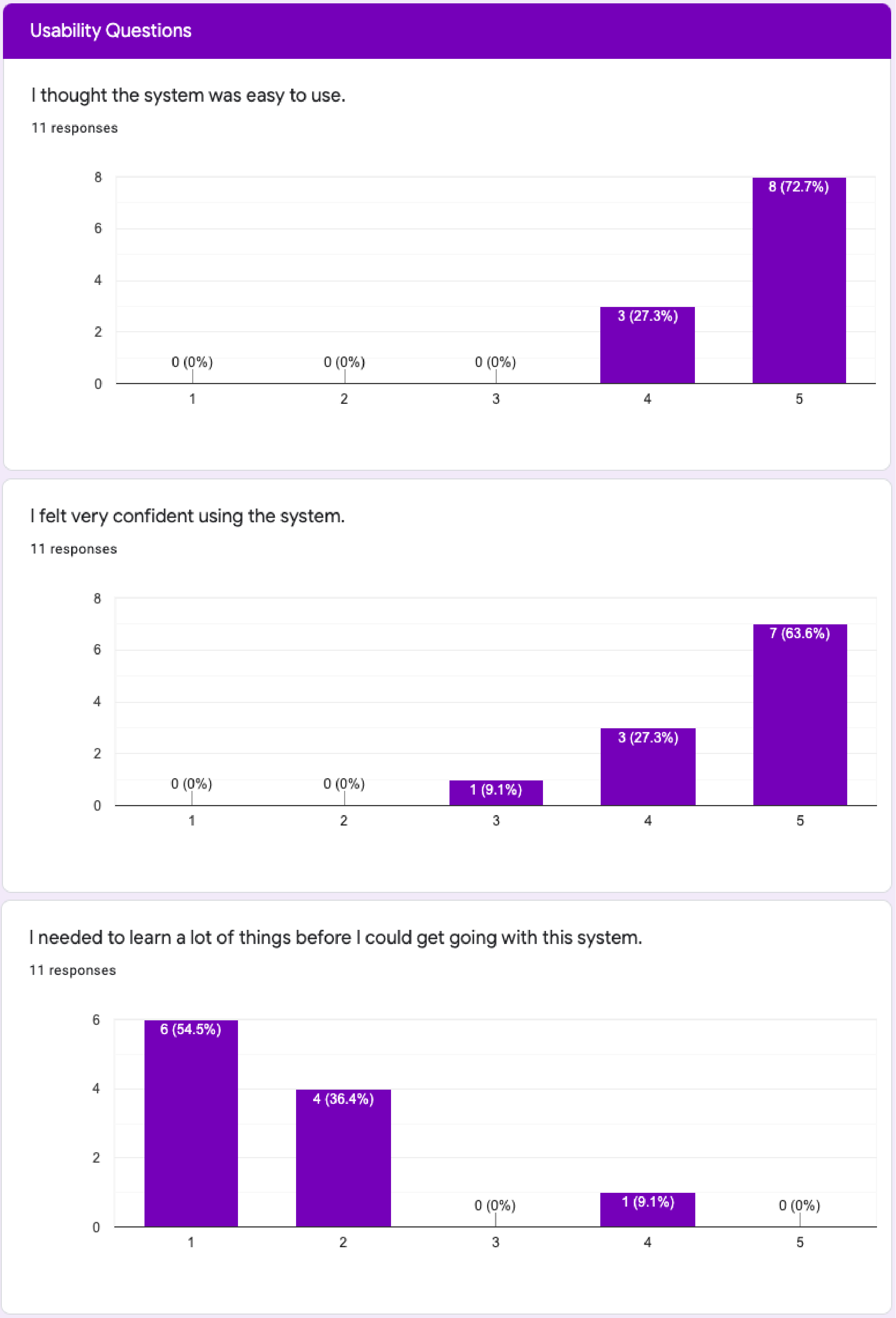
The privacy report reflected the user's privacy beliefs.

8 responses



After reading the report would you choose "Let me change my settings" or "Keep sharing my biometric data"?

8 responses



Usability Questions

I thought the system was easy to use.

11 responses

I felt very confident using the system.

11 responses

I needed to learn a lot of things before I could get going with this system.

11 responses