19: Intelligent Warning Systems: 'Technological Nudges' to Enhance User Control of IoT Data Collection, Storage and Use

RACHELLE BOSUA, KARIN CLARK, MEGAN RICHARDSON AND JEB WEBB

Abstract

The modern digital world of networking and connectivity enabled by the Internet of Things (IoT) has the paradoxical result of introducing a new era of 'smart computing' while reducing the intelligent control that individuals can exercise over their personal data. In this digital realm of big data and predictive analytics, we argue that users should be able to exert greater control over the collection, storage and use of their personal data. Our focus groups with IoT designers and users indicate that they are worried about the handling of their data, with users voicing concerns including surveillance and insecure storage of their data in the Cloud. Overall users wish for greater involvement in the management of their data. In response, we propose a high-level design prototype of an *Intelligent Warning Application* ('IWA') titled 'DataMind', empowering users to better control their IoT data collection, storage and use through: i) registering devices they wish to control; ii) setting and controlling required risk levels of their personal data flows; and iii) reacting on app warnings in the form of 'technological nudges' that report risky data flows. We present three illustrating scenarios of the latter together with corrective user actions, and conclude with a discussion of further steps of the design of this app.

Introduction

As we move into an era of big data, the mass collection, aggregation and processing of personal data through multiple connected devices signal many concerns. In particular, the uncontrolled collection, storage and use of individuals' data enabled by the Internet of Things (IoT) is unsettling in a world of more connectivity, networking and collaboration. The research question that can be asked is: *how can users better control the management of their personal data in an increasingly connected and digitised world?* While this is a key question, we acknowledge that new technologies and their accompanying data collection practices provide multiple new services and promises to significantly ease and enrich our lives in many different ways. For example, the flick of a single switch can instantaneously set a variety of devices into operation and customise information fed back to users based on unique predetermined individual needs. However, the mass collection of personal data, unknown methods of storage of this data (e.g. in the cloud), and the analyses, aggregation and processing of big data sets using modern data mining techniques, are growing concerns. In short, there is a serious question about how intelligent IoT users are really allowed to be in the new world of 'smart computing' - especially when it comes to their personal information. Specific concerns at the global level relate to privacy, data protection and cybersecurity.[1] In this chapter we respond to

[1] See, for instance, Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad 'Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)' in *International Conference on Network Security and Applications*, Berlin/Heidelberg: Springer, 2010: 420-429; Denis

our initial research question by introducing a new generation of protective systems designed to enable users to better control data flows associated with their personal data.

The chapter consists of four substantive sections. The first describes more background to the problem, followed by our research methodology and findings of our IoT project. The third section outlines the conceptual architectural model and a wireframe mock-up of our IWA prototype design, followed by a description of three scenarios that illustrate instances of nudging based on a user's profile built from knowledge garnered about the user's data privacy needs and inappropriate data flow patterns. A short discussion precedes the conclusion that elaborates on next stages of the study with some limitations and recommendations for further research.

Background Description of the Problem

The new world of computing is one of smarter living involving mass collection of IoT data from multiple devices, sensors and 'gadgets' we use in person as part of our daily lives. While it is already clear that mass IoT data collection and processing will bring significant positive change to our lives, the open internet-based infrastructure on which the IoT is based also raises some concerns. Firstly, 'interaction' comprises data collection, storage and sharing between multiple machines, devices and embedded sensors excluding any human intervention, immediate reception, or control of any personal data.[2] Secondly, entities, organisations or individuals other than those whose data is collected may take control of the data collected and shared through IoT devices. Finally, without their knowledge or consent, users are more vulnerable to surveillance, as personal data from multiple sources can be combined and processed intelligently to infer new insights about user actions, interactions and patterns of behaviour.[3] In addition, current legal frameworks in many jurisdictions, such as those in Australia, are often dated and immature in responding effectively to the diverse ongoing problems that may arise as a result of IoT processing of individuals' personal data.[4] In contrast, the new European General Data Protection Regulation (GDPR) which came into effect on 25 May

Kozlov, Jari Veijalainen and Yasir Ali, 'Security and Privacy Threats in IoT Architectures' in *Proceedings of the 7th International Conference on Body Area Networks*, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012: 256-262; Rolf H Weber, 'Internet of Things - New Security and Privacy Challenge', *Computer Law & Security Review 26* (2010): 23-30; Megan Richardson, Rachelle Bosua, Karin Clark, and Jeb Webb with Atif Ahmad and Sean Maynard, 'Privacy and the Internet of Things', *Media, Law & Arts Review* 21 (2016): 336-351; and Megan Richardson, Rachelle Bosua, Karin Clark, and Jeb Webb with Atif Ahmad and Sean Maynard, 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives' *Internet Policy Review: Journal on Internet Regulation* 6 (2017). Note that, unless otherwise specified, in this essay we use the generic label 'data privacy' to cover privacy and data protection.

[2] Weber, Internet of Things - New Security and Privacy Challenge'.

[3] Ibrahim AT Hashem, Ibrar Yaqoob, Nor Badrul Anuar, Salimeh Mokhtar, Abdullah Gani and Samee Ullah Khan, 'The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues Information Systems', *Information Systems* 47 (2014): 98-115.

[4] See Rolf H Weber, 'Internet of Things - Need for a New Legal Environment?' *Computer Law & Security Review* 25 (2009): 522-527; Richardson, Bosua, Clark and Webb, 'Privacy and the Internet of Things'; Richardson, Bosua, Clark and Webb, 'Towards Responsive Regulation of the Internet of Things'.

2018,[5] represents the biggest overhaul of modern data protection regulation in more than 20 years. Designed to give EU citizens more control over their personal data, GDPR aims to simplify and reshape ways in which EU organizations approach data collection and protection. It values data subjects' wishes signifying their agreement to processing of their personal data.[6] Hence, the GDPR is a timely response to a key problem associated with big data collection and processing using Information and Communications Technologies (ICTs).

Of course, another way to regulate for data protection is through more intelligent design of technologies themselves - and this is something that the GDPR also encourages.[7] A difficulty is that modern ICTs and applications (or 'apps') i) currently tend to present complex processes simplistically through heuristic interfaces that hide most of this complexity from the user, and ii) rely on the fact that users have been conditioned to accept personal disempowerment while using the internet. The former condition extends beyond using graphical user interfaces, saving users the effort of dealing with programming code. Actual audiences, relationships between entities, and information flows (to include who is doing what with data) are all effectively hidden from the average user of internet-connected services. The latter is self-evident insofar as users are routinely presented with situations engineered by other parties: i.e. programs that work in certain ways, allowing some forms of interaction while disallowing others. In other words, while people can engage in navigational and interactive behaviour in the online environment, they often do so with limited insight or control over the implications of their online behaviours. Furthermore, providers of services enabled by ICTs may have vested interests in data collection that lead them to actively obscure these interests or details of how data is used within their business models. Conditioning users to accept situations that serve these interests can also clearly be beneficial to the provider.

These problems are heightened in the case of the IoT. Personal IoT data collection is often unencrypted and uncontrolled e.g. automatically collected by sensors worn by users, embedded or concealed in the environment. In addition, IoT users are unaware of the following:

i. how and to what extent users' data is used or combined with other data sets;
ii. who acts as 'responsible owners' of collected data;
iii. when are users' data made available to external parties, or;
iv. how users' data is ultimately managed over time and by whom.

On the other side, the desire of consumers to exert control over their data has experienced a major shift over the last two decades. While a minority concern in the 1980s, individual fears about the potential abuse of personal (consumer) information have become a major concern by the 2000s.[8] Consumer concerns became focused on the ways in which users personal information is collected and used, with one study indicating that almost 88% of

[5] See General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), in effect 25 May 2018.

[6] Article 4(11) GDPR.

[7] Art. 25 GDPR (Data protection by design and by default).

[8] Batya Friedman, Peyina Lin and Jessica K Miller, *Informed Consent by Design in Security and Usability 2001*, (2005): 503-530.

US internet users expressed wishes to have an 'opt-in' privacy policy (in 2001) whereby internet companies need to first obtain users' permission to share their personal information with others.[9] This desire is becoming more pressing with the increased emittance of data as a by-product of user engagement with technological devices and services. The progressive 'giving-out' of individual data has both practical and political implications for ways in which people are seen and treated by the private sector and the state. In view of these concerns, the notion of minimal informed consent has evolved through political, legal, economic, social and technological realms.

Informed consent has been introduced as a mechanism to gain more user trust by articulating business practices for collecting and using personal information and giving users autonomous choice in terms of data collection and use. An Information Systems model of informed consent has been introduced in 2000,[10] constituting values associated with 'being informed' (including disclosure and comprehension) and 'giving consent' (i.e. voluntariness, competence and agreement). This model has since inception been incorporated in 'Value-Sensitive Design' frameworks touted by many authors as an integral part of large-scale real-world software systems.[11] Value sensitive designs appreciate and take account of human values in a principled and comprehensive way throughout the technological artefact design process.[12]

While the Information Systems model of informed consent is an attribute of many modern apps and technology artefacts, its ethical underpinnings related to informed consent are considered inadequate, outdated and limited in today's modern technology world.[13] More specifically, there are concerns that data collection, storage and use practices are not communicated 'in a manner that enables [users] to make an informed decision as to whether or not they want to divulge personal information' in the circumstances.[14] This problem is exacerbated in the interconnected world of the IoT. Prior studies indicate that users often unknowingly and even mindlessly 'consent' to data collection and use practices of online apps in exchange for services - and in fact this may well be encouraged by the apps themselves. Anecdotes from our empirical research confirm this aspect and also indicate that the inclusion of value-sensitive design frameworks in internet applications as a form of gaining informed

[9] Ibid.

[10] David Friedman, 'Privacy and Technology,' *Social Philosophy and Policy* 17 (2000): 186-212.

[11] See, for instance, Batya Friedman and Peter H Kahn Jr., 'Human Values, Ethics, and Design', in Andrew Sears and Julie Jacko (eds), *The Human-Computer Interaction Handbook, Boca Raton:* CRC Press, 2003, pp. 1177-1201; Batya Friedman and Helen Nissenbaum, 'Bias in Computer Systems', *ACM Transactions on Information Systems (TOIS)* 14 (1996): 330-347; and Jennifer Hagman, Ann Hendrickson and Amanda Whitty, 'What's in a Barcode? Informed Consent and Machine Scannable Driver Licenses', *CHI'03 Extended Abstracts on Human Factors in Computing Systems*, ACM (2003): 912-913.

[12] Friedman and Nissenbaum, 'Bias in Computer Systems'.

[13] Scott D Rhodes, DA Bowie and Kenneth C Hergenrather, ‚Collecting Behavioural Data using the World Wide Web: Considerations for Researchers', *Journal of Epidemiology and Community Health* 57 (2003): 68-73.

[14] Irene Pollach, 'A Typology of Communicative Strategies in Online Privacy Policies', *Journal of Business Ethics* 62 (2005): 221, 231.

consent is often ignored or bypassed.[15] Considering these and the increasing vulnerability of online personal data, the increasing collection and use of users' personal information require users to be more cognisant of IoT data collection and use, allowing users to control these activities in a more systematic way.

In response to our initial research question, the above challenges and limited-to-no practical control currently exercised by or on behalf of the users or data subjects concerned, and based on our empirical findings, we propose a conceptual architectural model and mock-up prototype design for an intelligent warning app (IWA) titled 'DataMind'. This app gives users more personalised control over the collection, storage and use of their individually collected IoT and social media. It deploys the idea of 'nudges' to alert users of changes in their known data collection and usage patterns allowing them to make decisions how they will respond and take further preventative steps[16] - in the same way that technological nudges employed in other contexts serve as 'soft reminders' that prompt users to take courses of action consistent with self-interest. For example, reinforcement for smokers trying to quit, or more recently, as part of the Facebook web interface, nudging users to more carefully consider the content and audience of their online disclosures.[17]

We believe that the IWA could be a useful example of the familiar 'privacy-by-design'/'data-protection-by-design' principle which has now been given legislative support with a special statutory provision encouraging such technologies in the GDPR.[18]

Research methodology and findings

Research Methodology

Our IoT research project funded by the University of Melbourne's Networked Society Institute was conducted from October 2015 to April 2017 and involved research teams from both

[15] Richardson, Bosua, Clark and Webb, 'Privacy and the Internet of Things'; Richardson, Bosua, Clark and Webb, 'Towards Responsive Regulation of the Internet of Things'.

[16] We appreciate that nudges can themselves sometimes be coercive: see Karen Yeung 'Nudge as Fudge', *Modern Law Review* 75 (2012): 122-148; Karen Yeung '"Hypernudge": Big Data as a Mode of Regulation by Design' *Information Communication & Society* 20 (2017): 118-136; Robert Baldwin 'From Regulation to Behaviour Change: Giving Nudge the Third Degree', *Modern Law Review* 77 (2014): 831-857. However, our design aims to minimise this problem by allowing users to effectively build their own preferences into the process of nudging.

[17] Yang Wang, Pedro G Leon, Alessandro Acquisti, Lorrie Cranor, Alain I Forget and Norman Sadeh, 'A Field Trial of Privacy Nudges for Facebook', *CHI*, 26 April-1 May 2014, Toronto, Canada. The notion of 'reminders' is not new and originated as computer-based 'reminder systems' in the 1990s, specifically in the context of ambulatory preventative care systems. In the medical domain reminder systems serve as invaluable prompts to alert medical staff to necessary interventions associated with treatment practices to enhance patient safety: Jennifer Meddings, Mary AM Rogers, Michelle Macy and Sanjay Saint, 'Systems Review and Meta-Analysis: Reminder Systems to Reduce Catheter Associated Urinary Tract Infections and Urinary Catheter Use in Hospitalized Patients, *Clinical Infectious Diseases* 55 (2010): 550-560.

[18] See Art. 25 GDPR (Data protection by design and by default).

the Melbourne Law School (Clark and Richardson) and the University's Computing and Information Systems Department (Bosua and Webb). We were specifically interested in regulatory aspects related to data privacy in a world of more connectivity and the IoT. In view of this our project commenced with an intensive requirements elicitation phase to get a deeper understanding of IoT data collection, use practices problems and concerns. Our overall aim was to gain specific knowledge of these concerns from two groups - IoT users and software engineers involved in the development of IoT software. We were specifically interested in privacy, data protection and security and wanted to hear views of both sets of stakeholders to verify whether and to what extent problems and concerns could be tackled.

Following ethics approval, our first study comprised 24 interviews with 14 IoT users and 10 experienced IoT designers/software engineers in October 2015 to April 2016. Individual one-hour face-to-face interviews were conducted in Melbourne with IoT users and software engineers in the 28 to 55-year age group. One of the authors (Webb) conducted the interviews and transcribed the audio-recorded interview data, followed by data analysis to identify key functional requirements. The other three authors participated in the data analysis to ensure triangulation and agreement of the key themes that emerged from the data. We reported on this study in two published papers,[19] where we argued (based on comments from users and designer findings) that laws ideally should go further in providing responsive regulation of IoT data practices, encouraging the inclusion of minimal standards of transparency and control integrated into the design of IoT.

Our second data collection stage involving 2 focus groups with 4 and 7 (total 11) users and 6 IoT designers/software engineers followed in April 2017. Four participants in our first stage participated in the stage 2 focus groups, while the other focus group participants were new - selected on the basis of their knowledge of or interest in privacy, data protection and/or security related to data practices of the IoT. With a deeper understanding of users' concerns about IoT data collection practices we used our initial study's findings to design a set of discussion questions. The second data collection stage aimed to confirm the veracity of the first stage's findings before moving on to obtain a more refined understanding of user requirements for data privacy and data security of IoT devices and comparing these with options that designers' thought were feasible. Both focus groups were conducted on the same day (one in the morning and the other in the afternoon), each lasting one and a half hours. All four authors were present with two authors (Bosua and Webb) leading the focus group discussions and the other two acting as observers. The focus group discussions were audio-recorded and used to confirm the key themes in the form of functional requirements to inform our architecture and initial app design.

Findings

As in the case of Stage 1, a large majority of participants who are users, said that they would like to have more transparency and control over their information as one commented about

[19] Richardson, Bosua, Clark and Webb, 'Privacy and the Internet of Things'; Richardson, Bosua, Clark and Webb, 'Towards Responsive Regulation of the Internet of Things'.

his personal data: '*once you have given [your] data out you are out of control and there is no way that you know where it is'*,[20] with another confirming: '*as an end user I want to know what my information is being used for, who is using it, for what - I want that sort of control of my information - I want to be able to say I want that information deleted'*,[21] and '*I just want to have my own control [over my privacy]'.*[22] Another participant stated '*from the perspective of a user you don't actually know what data is collected by these devices concerning you and your habits.... cheaper, faster and smarter often means unregulated*'.[23] Interestingly designer/engineers (who were also, of course, often users) often agreed with this summation with some emphasising the laissez-fare attitude of developers who monetise on data collection: *'..it all comes down to money, this profit to be made'*.[24] Particular examples were given of the treatment of sensitive data including health data ('*a lot of the stuff shared now is far more revealing than you could ever imagine and people are large unaware of it'),*[25] surveillance practices especially using geolocation data,[23] ('*if people knew the ramifications of the [geolocation] option on my phone and the consequences of that, they would drop it like a rock*'), the use of photographs or images going online,[26] ('*the one thing I find most disturbing is online baby monitors [images]'),* and data transferred overseas,[27] ('*the best form [of privacy] is do not plug it into the Internet*'). But participants also agreed there might be individual and cultural variations in terms of what information was considered particularly sensitive and how it should be treated.[28]

At the same time, participants generally questioned the value of the standard term consent regimes that IoT systems typically employ. In the words of one: '*who reads these terms and conditions, it's about 10 pages of really fine print - everyone just wants the facilities and it's only when there is a security incident then you go like I do have to read this'*. [29] Others said in terms of consent '*Australia is a bit cowboy land and in other countries it's not. In Germany consent is very explicit and its legally binding,*[24] and '*some have hidden uses that you as a user do not understand*' and essentially they are '*"click, click, click" regimes'* that allowed '*little scope for negotiation or individual variance'*.[30] As one of the participants summarised the situation, the current '*regime*' is a result of *'...the design of the [typical modern] user interface and having been trained as a user - that is the user experience - '...to click-click and don't worry about the rest of it*' the result is that '*there is no actual conscious thought in the [software design] process*'.[31]

[20] Designer/software engineer #1.
[21] Designer/software engineer #2.
[22] Designer/software engineer #3.
[23] Designer/software engineer #1.
[24] Designer/software engineer #3.
[25] Designer/software engineer #4.
[26] User #1.
[27] User #2.
[28] Designer/Software engineer #1.
[29] User #3.
[30] Designer/Software engineer #5.
[31] Designer/Software engineer #5.

As to legal standards, another participant expressed concern that these terms and conditions [of use] are subject to change without any notice,[32] while another participant indicated another issue with consent forms - '...*the difference is that US law is very different to Australian law with respect to fair and reasonable use - so you have this problem with terms and conditions which may be enforceable under a different law'*.[33] Another participant expressed his concern about the storage of the data, stating there is also this danger of terms and conditions and where data is stored: *'having all the data in the cloud, I do not know where it is.* [34]

The questions of data ownership once collected also came up especially when data is in the cloud, (*'Amazon provides fantastic services and things and if we record group meetings and basically use their IoT and there is a private discussion, who owns it [the data]?'*).[35]

Instead, some participants expressed a preference for more targeted *'warnings'* or '*notifications*'[36] that would '*allow them choices'* as to how to respond, *('...you want to give out some level of access or granting access'*). The idea once raised quickly became the subject of more discussion. One software engineer indicated that '*I talk about notification, about different actions you take within the software system. If a software engineer designs notifications keeping in mind* "*what are the side effects [of data collection] of whichever action I have taken within the software*", *it will help give users awareness about the implications of what you [the data collector] are doin*g'.[37] One theme that came up a few times is user naivety with one participant mentioning that the privacy problem is '*a social issue'* stating that '*there is not such thing as absolute security... we need to do better as developers in educating users in what the downside of these technologies are - so it's not enough to wait until there is a security incident before mitigating*'[38] and '*have the user know what s/he wants to give out'* educating users to '*be aware that they [external organisations] are using your data... you kind of guarantee that people are using your data, I give them my data so if something gets wrong, you the user is responsible*'.[39]

These findings were from a small sample, but they were insightful and a crucial part of the key considerations which informed our Intelligent Warning app architecture and prototype design as discussed in the next section.

Conceptual Architecture and Prototype Design of the IWA *The Conceptual Architecture*

Figure 1 proposes a conceptual model illustrating the client-server model comprising the IWA architecture. This distributed model presents the key app building blocks indicating

[32] User #3.
[33] Designer/Software engineer #6.
[34] Designer/Software engineer #1.
[35] Designer/Software engineer #1.
[36] Designer/Software engineer #6.
[37] User #3.
[38] Designer/Software engineer #5.
[39] Designer/Software engineer #6.

the division of tasks between the client (service requests from the user) and servers i.e. the application server, the database server with the data files and cloud storage and the Artificial Intelligence (AI) analytics engine. The application layer coordinates the app through the processing and analysis of user demands and logical decision-making related to the movement of data between the other remaining server layers. The AI analytics engine draws on logged historical user data, privacy settings customised by users through the app, IoT and Application Programming Interface (API) data stored in the Cloud to identify and learn more about a user's behaviour and data usage patterns. These patterns can be inferred over time through the user's customised privacy settings in combination with his/her historical data logs and interaction based on data flows to and from various APIs e.g. Google, IoT sensors/devices and social media APIs and external servers. Any deviations from the initial privacy settings will be alerted back to the user through the client in the form of one or more 'nudges' requesting corrective action. This could call for increasing specific API privacy settings or corrective user interventions (e.g. disconnecting from a specific Wi-Fi network).

Initially users set up their preferred data protection levels based on individual preferences, for example, control settings for i) GPS location; ii) processing of images and iii) data movement/transfer of data overseas. An initial period of use may lead to modification of the privacy settings stored in the app. The app engine will monitor data flows to and from various APIs in an inter-connected network with the consent and cooperation of the IoT service provider who may treat this as a way of offering an externalised system of privacy-by-design to users and complying with any relevant legal obligations in the jurisdiction (or jurisdictions). Figure 1 also presents the three data flow scenarios A, B and C that are described in the next section.

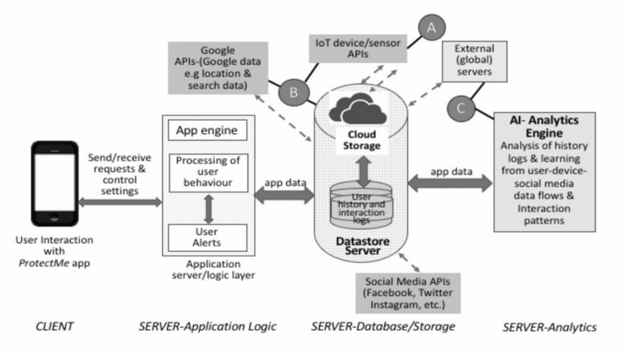
A
IoT device/sensor APIs
Google APIs-(Google data e.g location & search data)
B
External (global) servers
C
App engine
Processing of user behaviour
User Alerts
Application server/logic layer
Send/receive requests & control settings
User Interaction with *ProtectMe* app
app data
Cloud Storage
User history and interaction logs
Datastore Server
app data
AI- Analytics Engine
Analysis of history logs & learning from user-device-social media data flows & Interaction patterns
Social Media APIs (Facebook, Twitter Instagram, etc.)
CLIENT
SERVER-Application Logic
SERVER-Database/Storage
SERVER-Analytics

Figure 1: Conceptual Architectural Model of the Intelligent Warning app (IWA).

Three Scenarios Illustrating Instances of Nudging

The next three scenarios describe how the IWA 'nudges' users to update their 'DataMind' app's privacy settings or intervene through corrective actions. The scenarios relate to some particular dataflow concerns raised during our consultations and make provision for specific informed consent to be provided or requested for adaptating a user's pre-set controls for IoT data collection, storage, processing and use.

i) **Dataflow A** as set up by Abigail: The IWA will sense or track Abigail's fitness-monitoring IoT device, which is connected to her phone, access her location data through the mobile phone's geolocation technology and integrate this geolocation data with fitness i.e. health IoT data to target localised advertising about health and fitness services. Based on controls set up through control settings of the app by Abigail, this activity will either inform or alert Abigail for possible actions that include closing the port through which the geolocation data flows.

ii) **Dataflow B** as set up by Beatrice: The IWA will assess whether Beatrice's images or videos collected by her security camera which is linked to her smart phone (or her smart phone turned into a security camera) are encrypted prior to storing these on one or more server(s). The checking of encryption is not limited to images and videos but can also be applied to any other type of data being sent via one or more channels from an IoT device to a server. Beatrice will be aware through nudging that the collected data is not encrypted, as this data is sent out of a specific environmental boundary. Once again, Beatrice can decide to take preventative actions to stop the flow of her unencrypted data, for instance disconnecting the device or putting the device behind a 'firewall'.

iii) **Dataflow C** as set up by Chester: In this scenario, the IWA makes Chester aware of voluminous data flowing through one or more channels (e.g. connected to Chester's Wi-Fi network) to a third-party server overseas. Once again, the IWA will sense or track uncontrolled data movement. Hence the IWA should 'learn' of destinations of data and by knowing this and being aware of the setting of user controls the app will nudge Chester of any uncontrolled movement of data through specific communication channels. Chester might then formally act on this by consenting or reporting inadequate behaviour to an appropriate regulatory entity.

Wireframe mock-up prototype design

Figure 2 presents a wireframe diagram with a few initial mock-up screens of the IWA prototype design giving an idea of the IWA app's look and feel from a usability perspective. The aim is to design an interactive user-friendly app that is fairly intuitive in terms of use and functionality.

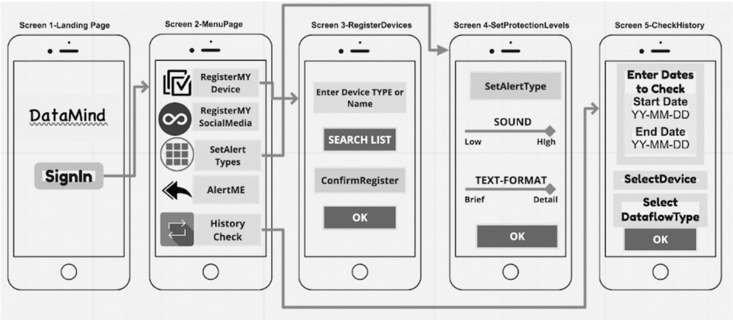

Figure 2: Excerpt of wireframe mock-up of the IWA prototype.

The initial landing page requires a secure user login taking the user to a second Menu Page screen which allows the user to provide his/her own control settings (for dataflows A, B and C mentioned above) based on the APIs in use (e.g. of social media applications) and IoT device apps. A third screen (Screen 3-RegisterDevices), allows the user to register specific IoT devices he/she wishes to control based on the device name or type using a search list (e.g. the fitness monitor for dataflow A and security camera for dataflow B). A similar screen (not yet shown here), will allow the user to register the social media applications in use he/she wishes to 'watch' or be 'nudged' about through linking to each application's API (e.g. Facebook, Twitter or Instagram). Screen 4 shows that users can also set their preferred alert types in the form of prompting sounds and/or 'nudges' in the form of textual warnings guiding the user for corrective action. The last screen (Screen 5) visualises how users can check a history of specific data flow interactions and/or violations for a specific period of time.

Discussion

Our recommended prototype design architecture is considered an initial attempt to address and illustrate the gaps in individually controlled data/information collection, processing and use through the IoT. While we only considered three different types of data flows that could compromise an individual's data through IoT devices, there are other more complex scenarios that involve the flow of collected data. We therefore consider the illustrated conceptual architecture in Figure 1 and the small prototype excerpt in Figure 2 as first steps towards developing a fully functional version of our proposed IWA. We acknowledge that the rich aspects of our initial prototype design cannot be presented in this limited space.

We envision that the IWA will create a greater user awareness of unauthorised data collection practices, while also helping users make more informed and conscious decisions about the different levels of privacy they require for their personal data. In addition, users will learn over time which devices, APIs and specific IoT devices and gadgets can be trusted from a privacy-by-design perspective. We envisage that the type of support to be provided by the IWA, would educate users to be more cautious with respect to sharing their personal data in a more digitised and connected world.

We aim to follow an agile systems development approach to build and test the current prototype version of the IWA in order to gauge feedback about the look and feel of the app. Following this we will continue with the design and building of a more comprehensive version to test the next stages of the IWA app's design. More specifically, the finer details of the IWA's application, and interaction between the AI analytics engine utilizing machine learning and data logs representing user activity, need to be developed. For this, a comprehensive set of algorithms drawing on artificial intelligence pattern matching techniques will be designed as the AI Engine's core functionality.

Conclusion

Our research confirms that users are concerned about data management practices in a new era of IoT computing. In particular, it highlights the need for users to have more control over the personal data and emphasises the need to incorporate Value Sensitive Design principles in a new generation of control software. Our study introduces the importance of 'nudges' as a way to alert users of violations in the management of their digital personal data and proposes an architectural view of an IWA app that draws on customised user control levels, nudging users to more intelligently control the use of their personal data collected and processed through the IoT. We consider our design and dataflow scenarios a first in incorporating the notion of 'nudges' with privacy by design into an intelligent warning app.

We acknowledge that this research is work in progress and in its early conceptual design and prototyping stages. As a result, the app development can only proceed once a fully functional prototype version of the IWA has been tested with a variety of users. We plan to further the app development following an Agile development approach. Another limitation is that the actual form of nudging as a means for users to control the flow of their data, is at this stage, unspecified. We hope that user-specific requirements in this regard can be elicited through in-depth testing of our prototype and also through further interviews and discussions with focus group members to identify the more nuanced aspects of the IWA's deeper design aspects.

References

Babar, Sachin, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad. 'Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)' in *International Conference on Network Security and Applications*, Berlin/Heidelberg: Springer, 2010: 420-429.

Baldwin, Robert. 'From Regulation to Behaviour Change: Giving Nudge the Third Degree', *Modern Law Review* 77 (2014): 831.

Friedman, Batya, Peyina Lin and Jessica K Miller. 'Informed Consent by Design' in *Security and Usability 2001,* (2005): 503.

Friedman, Batya, and Peter H Kahn Jr. 'Human Values, Ethics, and Design', in Andrew Sears and Julie Jacko (eds), *The Human-Computer Interaction Handbook, Boca Raton:* CRC Press, 2003, pp. 1177-1201.

Friedman, Batya and Helen Nissenbaum. 'Bias in Computer Systems' *ACM Transactions on Information Systems (TOIS*) 14 (1996): 330.

Friedman, David. 'Privacy and Technology,' *Social Philosophy and Policy* 17 (2000): 186.

General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679, enforcement date: 25 May 2018.

Hagman, Jennifer, Ann Hendrickson and Amanda Whitty. 'What's in a Barcode? Informed Consent and Machine Scannable Driver Licenses', in *CHI'03 Extended Abstracts on Human Factors in Computing Systems*, ACM (2003): 912.

Hashem, Ibrahim, A.T., Ibrar Yaqoob, Nor Badrul Anuar, Salimeh Mokhtar, Abdullah Gani and Samee Ullah Khan. 'The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues Information Systems', *Information Systems* 47 (2014): 98-115.

Kozlov, Denis, Jari Veijalainen, and Yasir Ali. 'Security and Privacy Threats in IoT Architectures' in *Proceedings of the 7th International Conference on Body Area Networks*, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2012): 256-262.

Meddings, Jennifer, Mary AM Rogers, Michelle Macy and Sanjay Saint. 'Systems Review and Meta-Analysis: Reminder Systems to Reduce Catheter Associated Urinary Tract Infections and Urinary Catheter Use in Hospitalized Patients', *Clinical Infectious Diseases* 55 (2010): 550.

Pollach, Irene. 'A Typology of Communicative Strategies in Online Privacy Policies', *Journal of Business Ethics* 62 (2005): 221.

Rhodes, Scott D., DA Bowie and Kenneth C Hergenrather. ‚Collecting Behavioural Data using the World Wide Web: Considerations for Researchers', *Journal of Epidemiology and Community Health* 57 (2003): 68.

Richardson, Megan, Rachelle Bosua, Karin Clark, and Jeb Webb with Atif Ahmad and Sean Maynard, 'Privacy and the Internet of Things', *Media, Law & Arts Review* 21 (2016): 336.

Richardson, Megan, Rachelle Bosua, Karin Clark, and Jeb Webb with Atif Ahmad and Sean Maynard, 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives' *Internet Policy Review: Journal on Internet Regulation* 6 (2017).

Wang, Yang, Pedro G Leon, Alessandro Acquisti, Lorrie Cranor, Alain I Forget and Norman Sadeh, 'A Field Trial of Privacy Nudges for Facebook' *CHI*, Toronto Canada, 26 April-1 May 2014.

Weber, Rolf H., 'Internet of Things - Need for a New Legal Environment?', *Computer Law & Security Review* 25 (2009): 522.

_____. 'Internet of Things - New Security and Privacy Challenge', *Computer Law & Security Review* 26 (2010): 23.

Yeung, Karen. 'Nudge as Fudge', *Modern Law Review* 75 (2012): 122.

_____. '"Hypernudge": Big Data as a Mode of Regulation by Design', *Information Communication & Society* 20 (2017): 118.