Intelligent Warning Systems: 'Nudges' as a Form of User Control for Internet of Things Data Collection and Use

Rachelle Bosua[1], Karin Clark [2], Megan Richardson [2] and Jeb Webb[1]

[1] School of Computing and Information Systems, University of Melbourne, Australia
[2] Melbourne Law School, University of Melbourne, Australia
{rachelle.bosua,karin.clark,m.richardson,jeb.webb}@unimelb.edu.au

Abstract. The modern digital world of networking and connectivity makes possible a new era of computing in which users exert greater control over the collection and use of their personal data through the Internet of Things (IoT). Our recent empirical work indicates that traditional forms of consent are inadequate and that users are looking for different levels of and greater involvement in controlling the collection and use of their personal data – with some participants voicing particular concerns about collection and use of sensitive data, such as health information, and others pointing to particular risks, such as insecure storage in the Cloud. In response to these needs we propose a new *Intelligent Warning Application* in the form of a conceptual architecture for an App that empowers users to control their IoT data collection through users: 1) identifying their own levels of risk, 2) customizing the App allowing for the setting of their identified risk levels, and 3) situated use of the App warning users of risk-averse situations through 'nudges'. We conclude with a discussion illustrating scenarios of the App's.

Keywords: Internet of Things, Privacy, Data Protection, Intelligent Warning Systems, Nudges.

1 Introduction

The uncontrolled collection of user data through the Internet of Things (IoT) is becoming a matter of particular concern in a world of more connectivity, networking and collaboration afforded by the IoT. How can individuals better control the collection and use of their personal data in an increasingly connected and digitized world of the IoT? This world enables multiple new services and the exchange of information, which promise to significantly ease and enrich our lives in many different ways. For example, the flick of a single switch can instantaneously operationalize multiple devices, invoke different devices' services and feed back information based on unique predetermined individual needs. However the mass collection, integration and use of individuals' private and personal data through modern data mining techniques and big data algorithms lead to growing privacy concerns in Australia and around the world regarding individual privacy and protection of personal data, as well as information security [1-3].

Although the open Internet-based infrastructure on which the IoT is based facilitates tremendous access to information, there are specific features that affect data protection, privacy and security [4-6]. Firstly, 'interaction' in the context of the IoT comprises data collection between multiple machines and embedded sensors without human intervention, immediate reception or control of any personal data [6]. Secondly, entities, organizations or individuals other than individual users whose data is being collected, are in control of the data being collected through IoT devices. Thirdly, without their knowledge or consent, individuals can be followed through surveillance, while their data from different data sets can be combined and processed intelligently to infer new insights based on an individual's patterns of behavior [7]. And finally, at least in Australia, there is as yet, no legal framework that responds effectively to the diverse problems that can arise in the collection, use of and protection of individuals' privacy in the context of the IoT [1-2] [7-8].

A recent Australian study on individual attitudes towards privacy, conducted by the Office of the Australian Information Commissioner, indicates that the Australian public's concern for online privacy has increased over the last five years [3]. However, despite this expressed concern, many survey participants described apparently contradictory habitual behaviors, such as not reading privacy policies (65%) or accepting default settings while using social media (50%) instead of adjusting these settings to limit who has access to their personal information. While this may seem to lay blame at the feet of the users for choosing not to engage in the learning or administrative tasks required for assuring their personal privacy, an obvious rejoinder to this argument is that these requirements may be unreasonable given the context of modern digital communications.

Modern digital communications a) present complex processes simplistically through heuristic interfaces that hide most of this complexity from the user, and b) 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 to spare users having to deal 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 or internet-connected services. The latter condition is self-evident insofar as users are routinely presented with situations that have been engineered by other parties: programs that work in certain ways and allow some forms of interaction while disallowing others. In other words, while people can engage in navigational and interactive behavior within the online environment, they often do so with limited insight or control over the implications of these behaviors. Furthermore, the providers of services typically have interests in data collection that lead them to actively obscure their interests or the 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.

In view of the above challenges and the fact that data collection through the IoT is on the increase with limited to no practical control currently exercised over individual data collection and use of this data, the question is how and to what extent individuals can be provided more support in controlling their interaction in a world of data collection enabled by the IoT? In response to this question we propose a conceptual archi-

tectural model of an Intelligent Warning Application (App) that allows users to exert more control over the collection and use of their individual data collected through the IoT. Reliant as it is on cooperation from IoT producers in providing information requested by the Intelligent Warning App, we offer this as an example of the principle of 'privacy by design' that we advocated in earlier papers based on this research [1] and [2], and which numerous privacy regulators have also endorsed. Further, based as it is on extensive user interviews and two focus groups, our proposed conceptual model also embeds a broader idea of responsive regulation i.e. regulation scaled to achieve effective regulation in response to a perceived need and with minimal intervention in preference to heavy-handed top down regulation.

This paper consists of six sections. Section 2 provides background literature that illustrates the current gap in the literature with respect to intelligent warning applications/tools. Section 3 provides background to the initial conception of our proposed Intelligent Warning App and introduces the research approach to be followed to design this tool. Section 4 presents evidence of specific user concerns and recommendations leading to a conceptual model of one view of the Intelligent Warning App design. Section 5 discusses three scenarios that illustrate instances of nudging based on a user's profile built from knowledge garnered about the user's privacy needs. The Conclusion (Section 6) elaborates on next stages of the study with some limitations and recommendations for further research.

2 Background literature

The notion of uncontrolled data collection and use of user's data is a problem that plagues many individuals in a modern world of greater connectivity and exchange of data through the Internet of Things (IoT). While the Internet is one of the most disruptive technologies of the modern age, the constant collection of data through multiple connected devices is a significant concern, especially to individuals who value their privacy. Of particular concern is the notion of *transparency* and *understanding* about how and where IoT data is collected, how IoT data is stored, and when this data is used and integrated with other data sets.

2.1 Privacy, data protection, and security in the context of IoT data collection and use

Privacy' may be treated as a broad concept covering multiple aspects of the collection and use of personal information, along with other things (for instance [9]). Alternatively, some especially European commentators may label this 'data protection' (for instance [10]), while reserving the label 'privacy' for the more particular problem of being made subject to an unwanted public gaze [11-12]. In our previous published papers we pointed out that our interviewees tended to adopt the latter view although they also considered data protection to be a pressing concern, both for them personally and also for society [1-2]. As such, this paper is concerned both with questions of

privacy and data protection and (unless otherwise specified) we treat these as overlapping and congruent concerns.

It is not just the control of personal information that is at stake here. Concerns may also extend to 'security', a term that concentrates on the protection of collected information from unwanted external access, for instance from hacking. Security principles (confidentiality, integrity and availability of information) [13] guarantee that access to collected information is restricted, open only to those who are authorized to do so, and that stored information is trustworthy and accurate. The heterogeneous nature of the IoT in combination with its wide scale of use is expected to increase security risks of the current Internet. More specifically, the limited computing power of IoT technologies violates traditional security countermeasures and enforcement calling for the need to define valid IoT security and trust models to gain full acceptance by its user base [14].

2.2 Informed consent in the context of technological artefacts

One shortcoming of the IoT is the limited support offered for the exercise of informed consent i.e. giving users the ability to concur with data collection and use techniques. Specifically, the collection of personal data through the IoT, is more than often unencrypted, uncontrolled through sensors embedded in the environment, or in the form of wearables or surveillance devices concealed in the environment.

In regard to this, 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 80's, by the 2000s individual fears about the potential abuse of personal (consumer) information have become a major concern [15]. Consumers have become concerned about the ways in which their personal information is both collected and used, with one study indicating that almost 88% of US Internet users have expressed their 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 [15]. As a result the notion of a 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. In this regard the model of informed consent for Information Systems has been introduced in 2000 [16] 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 the 'Value-Sensitive Design' framework touted by many authors [17-21] as an integral part of large-scale real world software systems. Value sensitive designs appreciate human values in a principled [18] and comprehensive way throughout the process of designing technological artefacts.

While informed consent is an attribute of many of today's modern web-based Apps and technology artefacts, ethical considerations related to providing and substantiating informed consent is considered in a modern world of technology to be inadequate,

outdated and limited [22]. More specifically, there are concerns that data collection and use practices are not clearly communicated in a responsible way to pave the way for informed consent [23]. In addition, current privacy policies are not clear and understandable by ordinary consumers in conveying how the collection and use of individuals' personal information can be protected. This problem is exacerbated in an interconnected world of the IoT.

In a world of higher levels of service delivery, enabled and facilitated by increased collection and use of personal IoT data, the notion of informed consent is therefore a major concern. Indeed, prior studies indicate that users often unknowingly 'consent' to data collection and use practices of online Apps in exchange for services, while anecdotes from our empirical research indicate that the inclusion of value-sensitive design frameworks in Internet applications as a form of gaining consent is often ignored or bypassed [1]. With the increasing collection and use of individuals' personal information, there is therefore a need for users to be more cognizant of IoT data collection and use allowing them to control these activities in a more systematic way.

2.3 Nudges as a form of control

Over the last few years the notion of 'nudges' as a form of leading or guiding individuals in certain directions while also preserving their freedom of choice, has been debated significantly (see, for instance [24-27]). Nudges as a 'soft reminder' prompting users of unacceptable online behavior have been applied in different contexts e.g to support smokers to persevere in quitting smoking, and more recently as part of the Facebook web interface nudging users to more carefully consider the content and audience of their online disclosures [28]. Being a reminder, nudges can also serve as a warning or intervention that can support users in making decisions to disclose relevant or more or less information. The notion of 'reminders' is not new, and originated as computer-based 'reminder systems' in the 90's, 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 [29].

Over time the use of computer-based reminder systems has become more mainstream as evident from their use in the form of 'nudges' in other application areas such as appointment reminder systems associated with email, audit and feedback reminders systems, costs of borrowing and workflow systems that are associated with rule-based processing of information. Reminders or recommendations that are in the form of nudges and specialized forms of nudges have emerged as a form of changing behavior. This form of behavioral changing has attracted considerable attention, often leading to concrete reforms in specific domains. Nudges exist in many different forms such as the sounding of alarms that call for human intervention (e.g. in the medical domain), or reminders in the form of animations or prompts that encourage online system users to interact though the entering of data or specific input device activity. Another form of nudging encourages users to pause and reflect prior to entering or posting information/content online (as in the case of Facebook [28]). Depending on the extent of intervention required, more interactive forms of nudging could be in the

form of online intelligent assistants that provide users 'intelligent guidance or warnings' calling for (perhaps guiding) specific user actions or behavior.

While there are deeper questions to be asked about nudges, for instance "what they signify and express for individuals and their capacity for autonomous and responsible decision-making" [26], the use of appropriate individual-centric and intelligence-based forms of 'nudging' may be instrumental in guiding users to exert more control over the collection and use of their personal information through the IoT, as proposed in the next section.

2.4 Towards intelligent warning systems

Based on our initial study of individual perceptions of privacy and concerns about control over IoT data collection and use [1-2], there is a need to design appropriate tools that enhance or supersede traditional forms of informed consent. In our follow-up focus groups conducted this year we were told that 'warnings' may be more useful to IoT users than further refining contract terms (especially where these are treated as non-negotiable). The incorporation of 'nudges' allowing users to define and select different levels of and forms of control over the legitimate collection and use of their IoT data is an attractive option. We therefore propose an Intelligent Warning App that complements IoT data collection by allowing individuals to exert control over the collection and use of their personal data through the IoT. To justify the development of such an App, we report on empirical work conducted to elicit requirements from users in this regard.

3 Research methodology and findings

3.1 Research methodology

As precursor to defining the functional requirements of our Intelligent Warning App, it is worth noting our research methodology. We followed an intense requirements elicitation phase to get a deeper understanding of IoT data collection and use practices and problems. Our overall aim was to gain specific knowledge of the issues from a group of IoT users and software engineers involved in the development of IoT software. We were specifically interested in concerns about privacy, data protection and security and wanted to hear the views of both sets of stakeholders to verify whether the identified problems can be tackled.

Following ethics approval, the first stage of our study comprised 24 interviews with 14 IoT users and 10 IoT designers/software engineers in October 2015 to January 2016. Interviews were individual one-hour face-to-face interviews conducted in Melbourne with IoT users and experienced software engineers in the 28 to 55 year age group. One of the authors conducted the interviews and transcribed the audio-recorded interview data, followed by an analysis of this data to identify key functional requirements. Three of the authors were involved 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 [1] and [2], where we argued that laws needed to provide responsive regulation of IoT privacy/data practices, including through the encouragement of minimal standards of transparency and control integrated into the design of IoT, adopting a principle of privacy by design (a principle which is partially but by no means perfectly expressed through APP 1 of the Australian Privacy Principles under the Privacy Act 1988 (Cth), which states that APP entities should "take such steps as are reasonable in the circumstances to implement practices, procedures and systems" to ensure compliance with the APPs).

Our second stage involving 2 focus groups with 4 and 7 (total 11) users and 6 IoT designers/software engineers followed in April 2017. The aim at this stage was to confirm the veracity of the findings of our first stage before moving on to obtain a more refined understanding of user requirements for privacy, data protection and security of IoT devices and compare these with options that designers thought were feasible. Both focus groups were conducted on one 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 leading the focus groups and two authors acting as observers. Focus group conversations were audio-recorded and used to confirm the key themes in the form of functional requirements outlined in the next section. 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/interest in privacy, data protection and security related to the data practices of the IoT.

3.2 Findings

As in the case of stage 1, a number of users said that they would like to have more transparency and control over their information, as one 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". Users also agreed that there might be individual and cultural variations in terms of what information was considered particularly sensitive and how it should be treated.

At the same time, users questioned the value of the standard term consent regimes that IoT systems typically employ, describing these as "extremely lengthy and full of legal jargon that a user does not understand" and essentially 'click, click, click' regimes that allowed little scope for negotiation or individual variance. In particular one of the participants indicated that this 'regime' is a result of "...the design of the 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", adding that "there is no actual conscious thought in the process".

Instead, a number of users expressed a preference for more targeted 'warnings' that would cater to particular concerns about the level of the protection and security accorded to their information and would allow them choices as to how to respond. One software engineer indicated that "I talk about notification, about different actions you take within the software system. If a software engineer designs notifications into 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 doing".

With these in mind, the next sections of this paper focus on how such warning systems might be designed and integrated into IoT devices from an architectural view, as well as how legal standards, for instance in Australia, might be drawn on by policy-makers to encourage and regulate such design features to ensure they operate to enhance rather than constrain individual capacities for autonomous and responsible decision-making.

4 Conceptual architecture of the intelligent warning app prototype

Figure 1 proposes a conceptual architectural model illustrating examples of information flows resulting from IoT data collection that the Intelligent Warning App should inform the user about. This diagram illustrates three dataflow scenarios that will nudge the user for a form of intervention depending on users' set-up preferences in respect of their data.

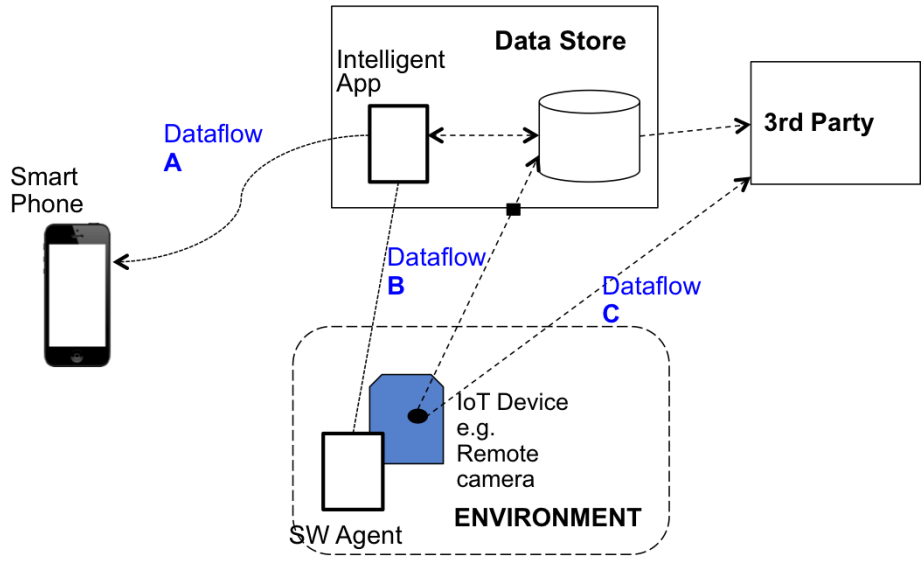

Fig. 1. Conceptual architectural model for the intelligent warning app

The above diagram represents a client server model with an IoT device and the Intelligent Warning App's intelligent agent (IA) that learns about a user's privacy and data protection requirements as set up by the user. Initially users set up their preferred protection levels, for example, control settings for i) GPS location; ii) images and iii) data movement/transfer. An initial period of use may lead to modification of the set-

ting-level knowledge stored by the Intelligent Warning App's intelligent agent. The intelligent agent is also linked to one or more sniffers (e.g. in Figure 1 represented by one small black rectangle), which monitor traffic flows in a 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, for instance in the Australian case under the Privacy Act's APPs – including APP 1, noted above). The next section describes three different 'nudging' scenarios that the Intelligent Warning App will typically alert to the user.

4.1 Description of dataflow examples that will nudge the user to either consent or request adaptation of control

- Dataflow A: as set up by 'Abigail', the Intelligent Warning App will sense or track that Abigail's fitness-monitoring IoT device which is connected to her smart phone, accesses her geolocation location data through the phone's geolocation technology and integrates this data with her fitness IoT data in order to target localized advertising about health and fitness services (in a way that if not consented to, may breach a local privacy or data protection law, for instance in the Australian case APP 2: regarding a use of sensitive health information that is not 'directly related' to the primary purpose for which the information was collected, and APP 7: direct marketing using sensitive health information). Based on controls set up in the intelligent agent by the user, this activity will either inform the user or alert the user to possible actions that include closing the port through which the geolocation data flows.
- Dataflow B: as set up by 'Beatrice', the Intelligent Warning App will assess whether images or videos of Beatrice that are collected by her security camera are encrypted prior to storing these on the server. The checking of encryption is not limited to images and videos but can also be applied to any other type of data which is being sent via one or more channels from an IoT device to a server. Users will be aware through nudging that collected data is not encrypted as this data is sent out of a specific environmental boundary (in a way that again may breach a local privacy or data protection law, for instance in the Australian case APP 11 which imposes an obligation on APP entities to 'take such steps as are reasonable in the circumstances' to protect personal information that they hold from misuse, interference, loss, unauthorized access, modification or disclosure). Once again the user can decide to take preventative actions to stop the flow of unencrypted data, for instance disconnecting the device or putting the device behind a "firewall".
- Dataflow C: in this scenario, as set up by 'Chester', the Intelligent Warning App makes Chester aware of voluminous data flowing through one or more channels to a third party server overseas (in a way that again may, if done without consent, breach a local privacy or data protection laws, for instance in the Australian case APP 8 which imposes strict standards on cross-border disclosures of personal information). Once again the Intelligent Warning App will sense or track uncontrolled movement. Hence the Intelligent Warning App should 'learn' of destina-

tions of data and by knowing this, and the setting of user controls, nudge the user of any uncontrolled movement of data through specific communi-cation channels. The user might then formally act on this by consenting or reporting inadequate behavior to an appropriate regulatory entity institution (in the Australian case, the OAIC).

5 Discussion

Our recommended architecture is considered as an initial attempt to address the gaps in individually controlled data/information collection and use through the IoT. We consider the illustrated conceptual architecture in Figure 1 as the first stage towards developing a fully functional version of our proposed Intelligent Warning App. We aim to further refine our conceptual architecture into a detailed architectural design to build a prototype of the App. The next stage of this research is therefore the capturing of more detailed requirements to identify a complete and consistent set of functional and non-functional requirements to build the App and its core intelligent agent component. More specifically, the finer details of the Intelligent Warning App's intelligent agent needs to be identified to formulate detailed design requirements of its architecture in ways that will both utilize features of machine-learning effectively, and at the same time, comply with the basic legal requirements of privacy and data protection laws in multiple jurisdictions as well as broader community norms regarding the treatment of personal data, building these safeguards into the system, see [30]. We expect that a comprehensive set of semantic processing algorithms using artificial intelligence pattern matching techniques have to be designed as the core functionality of this depends on its intelligent agent component.

6 Conclusion

Our research in progress proposes one view of an Intelligent Warning App that draws on user-selected control levels and privacy principles that are aligned with Australia's Privacy Act APPs to nudge users to better control the collection and use of their private data through the IoT. We consider the model and dataflow scenarios presented here the first in a series of models (e.g. process, domain classes, service performance and use case models) that need to be developed to illustrate different architectural views of the Intelligent Warning App. Once these models are developed, a prototype App will be designed for evaluation.

This research is limited as it is in the early stages of conceptual design and prototype development and can only proceed once all functional and non-functional requirements have been defined. An Agile SDLC development approach in combination with intelligent agent-based software design is proposed for the App development. 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. User-specific requirements need to be elicited through further interviews and discussions with our focus group members

while the more nuanced aspects of the Intelligent Warning App's design also needs to be developed in much more depth.

References

[1] Richardson M, Bosua R, Clark K, Webb J, Maynard S and Ahmad A. (2017). Towards responsive regulation of the Internet of Things: Australian perspectives, *Internet Policy Review: Journal on Internet regulation*, 6(1).

[2] Richardson M, Bosua R, Clark H, Webb J, with Ahmad A and Maynard S (2016). Privacy and the Internet of Things, *Media, Law & Arts Review*, 21(2), pp. 336-351.

[3] Office of the Australian Information Commissioner (2017). Australian Community to Privacy Attitudes report (online resources: accessed on 20 May 2017: http://www.opengovasia.com/articles/7599-australian-community-attitudes-to-privacy-survey-shows-58-of-australians-trust-state-and-federal-government-departments

[4] Babar S, Mahalle P, Stango A, Prasad N, and Prasad R (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). In: *International Conference on Network Security and Applications* (pp. 420-429). Springer Berlin Heidelberg.

[5] Kozlov D, Veijalainen J, and Ali Y (2012). Security and privacy threats in IoT architectures. In *Proceedings of the 7th International Conference on Body Area Networks* (pp. 256-262). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[6] Weber RH (2010). Internet of Things–New security and privacy challenge. *Computer Law & Security review*, 26(1), pp 23-30.

[7] Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A and Khan SU (2015). The rise of 'big data' on Cloud computing: review and open research issues *Information Systems*, 47, pp 98-115.

[8] Weber RH (2009). Internet of things–Need for a new legal environment? *Computer law & Security Review*, 25(6), pp. 522-527.

[9] Westin AF (1967). Privacy and freedom. Atheneum New York.

[10] De Hert P and Gutwirth S (2009). Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In: *Reinventing data protection?* pp. 3-44. Springer Netherlands.

[11] Gavison R (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 421-471.

[12] Austin L (2003). Privacy and the Question of Technology. *Law and Philosophy*, 22(2), 119-166.

[13] Whitman ME and Mattord HJ (2011). *Principles of information security*. Cengage Learning.

[14] Sicari S, Rizzardi A, Grieco LA and Coen-Porisini (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, pp 146-164.

[15] Friedman B, Lin P and Miller JK (2005). Informed consent by design. *Security and Usability*, (2001), 503-530.

[16] Friedman D (2000). Privacy and technology. *Social Philosophy and Policy*, 17(02), 186-212.

[17] Friedman B and Kahn Jr PH (2003). Human values, ethics, and design. *The human-computer interaction handbook*, 1177-1201.

[18] Friedman B and Nissenbaum H (1996). Bias in computer systems. *ACM Transactions on Information Systems (TOIS)*, 14(3), 330-347.

[19] Hagman J, Hendrickson A and Whitty A (2003). What's in a barcode? Informed consent and machine scannable driver licenses. In *CHI'03 Extended Abstracts on Human Factors in Computing Systems* (pp. 912-913). ACM.

[20] Nissenbaum H (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and philosophy*, *17*(5), 559-596.

[21] Friedman B, Kahn PH, Borning A and Huldtgren A (2013). CH: Early engagement and new technologies: Opening up the Laboratory, Vol 16 of the series Philosophy of Engineering and Technology (pp 55-95) Title: Value Sensitive Design and Information Systems.

[22] Rhodes SD, Bowie DA and Hergenrather KC (2003). Collecting behavioural data using the World Wide Web: considerations for researchers. *Journal of Epidemiology and Community Health*, 57(1), 68-73.

[23] Pollach I (2005). A Typology of Communicative Strategies in Online Privacy Policies, Journal of Business Ethics, 62, pp 221.

[24] Thaler R and Sunstein C (2008). Nudge: The gentle power of choice architecture. *New Haven, Conn.,Yale*.

[25] Yeung K (2012). Nudge as Fudge. *Modern Law Review*, 75(1), 122-148.

[26] Yeung K (2017). 'Hypernudge': Big Data as a Mode of Regulation by Design. *Information, Communication & Society* 20(1), 118-136.

[27] Baldwin R (2014). From regulation to behaviour change: Giving nudge the third degree. *The Modern Law Review*, 77(6), 831-857.

[28] Wang Y, Leon PG, Acquisti A, Cranor L, Forget Al and Sadeh N. (2014). A field trial of privacy nudges for Facebook. *CHI 2014,* April 26-May 01, Toronto Canada.

[29] Meddings J, Rogers MAM, Macy M and Saint S (2010). Systems Review and Meta-Analysis: Reminder systems to reduce catheter associated urinary tract infections and urinary catheter use in hospitalized patients, Clinical Infectious Diseases, 51(5), pp 550-560

[30] Agrafioti F (2015). Privacy by Design is Key to the Future of Artificial Intelligence. *Huffington Post*, 26 October, 2015.