CHAPTER 7

Examining Privacy Disclosure and Trust in the Consumer Internet of Things: An Integrated Research Framework

Grace Fox and Theo Lynn

Abstract The Internet of Things (IoT) and the various applications it encompasses offer great potential for personalisation and convenience in all aspects of individuals' lives from healthcare to transport and smart homes. However, IoT devices collect and share large volumes of personal data leading to concerns for the security and privacy of the data. While computer science research has explored technical solutions to security issues, it is important to explore privacy from the perspective of consumers. To foster a sense of privacy and trust among consumers, IoT service providers must communicate with consumers regarding their data practices in a transparent manner. To do this, we propose that IoT service providers refine adopt transparent privacy disclosure approaches. We present a framework for testing the effectiveness of privacy disclosures in building consumers' perceptions of privacy and trust and empowering consumers to adopt IoT devices whilst retaining some level of privacy. We illustrate this framework with reference to a privacy label approach.

G. Fox (✉) • T. Lynn
Irish Institute of Digital Business, DCU Business School, Dublin, Ireland
e-mail: grace.fox@dcu.ie; theo.lynn@dcu.ie

T. Lynn et al. (eds.), *The Cloud-to-Thing Continuum*, Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-030-41110-7_7

Keywords Privacy • Trust • Privacy label • Trust label • Social contract theory • Information–Motivation–Skills Model • Research framework

7.1 Introduction

We now live in a world with more connected devices than people. In the near future, the Internet of Things (IoT) landscape will comprise of billions of connected devices and things with the ability to exchange data at any given time. IoT can be defined as

> A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these "smart objects" over the Internet, query their state and any information associated with them, taking into account security and privacy issues. (Haller et al. 2008, p. 15)

The potential value of IoT is enormous ranging from US$3.9 trillion to US$19 trillion in the coming years (Cisco 2013a, b; McKinsey Global Institute 2015). Notwithstanding this massive economic opportunity, IoT and the big data it generates further complicate the issues around privacy and security (Lowry et al. 2017). The connection of devices enabled by IoT can heighten privacy and security challenges, not least excessive monitoring and data mining techniques that may enable data to be made available for purposes for which it was not previously intended (Abomhara and Køien 2014). The risks associated with these challenges is exacerbated by the long service chains inherent in the Internet of Things involving a multitude of actors including not only IoT software vendors and device manufacturers but network operators, cloud service providers, and the software and hardware vendors and services to support the infrastructure underlying the IoT. While consumers may accept a degree of consumer surveillance from the Internet or IoT, they may be equally ignorant about the degree to which their data is being distributed to fulfil their service requirements. There is an onus on enterprises providing IoT products and services, and consuming IoT data, to both take privacy

preserving actions and to communicate with consumers on the use of their data in the Internet of Things.

While existing research has identified some solutions to security challenges in IoT, user privacy and issues around privacy in data collection, management, and dissemination must be addressed (Abomhara and Køien 2014). Indeed, privacy and trust are categorised as two of the core security challenges facing the future of IoT (Sicari et al. 2015). Chapter 6 discusses some of the technical challenges at play in relation to the security of data. In this chapter, we focus on exploring the issues of privacy and trust related to IoT from the perspective of consumers. The remainder of the chapter is structured as follows; the next section explores perspectives and theories on privacy and the Internet of Things. It is followed by a brief discussion on the nature of trust and trust in technology. Next, we discuss approaches for influencing perceptions of privacy and trust. Following on from this literature, we propose an IoT privacy trust label as a potential means to influence perceptions and trust in relation to IoT. Based on theories, constructs, and concepts discussed in earlier sections, we present a framework for testing the effectiveness of privacy disclosures in building consumers' perceptions of privacy and trust and empowering consumers to adopt IoT devices whilst retaining some level of privacy. We illustrate this framework with reference to a privacy label approach.

7.2 Privacy and the Internet of Things

Users' privacy remains an important issue in IoT environments with concerns raised around the leakage of location information and inferences from IoT device usage such as TVs (Alrawais et al. 2017). It would seem while parents were once worried about the amount of time kids spent watching television, we now need to worry about the amount of time our television spends watching us.

In the context of IoT, there are several dimensions of privacy that must be considered and protected. These include identity data or personally identifiable information (PII), location data which can reveal many forms of PII, footprint privacy, and data contained in queries (Daubert et al. 2015). Solutions have been identified for many of these dimensions, such as anonymisation (Daubert et al. 2015), but again these solutions are technical in nature and do not emphasise the user perceptions. When focusing on user privacy, there is a tendency to focus on the application layer as this is the layer closest to the consumer and the point at which privacy

perceptions can be addressed. It is also important to explore consumers' perceptions of privacy and trust as research has shown concern for privacy and absence of trust can both reduce willingness to disclose information and adopt new technologies (Li 2012).

Privacy as a phenomenon has been studied for centuries across a range of academic disciplines and perspectives such as law, sociology, marketing, and information systems (IS). This chapter focuses on privacy from the IS perspective. Privacy is defined as an individual's desire for greater control over the collection and dissemination of their personal information (Bélanger and Crossler 2011). This definition remains relevant in the context of IoT, with privacy described in this chapter as consumers' desire to be afforded a greater degree of control over the collection and use of their personal data by IoT devices and sensors. The IS literature on privacy has grown over the past three decades but privacy remains relevant today with polls continuing to find that individuals place value on their privacy. For example, Pike et al. (2017) found that 84% of consumers in the US expressed data privacy concerns, 70% of whom felt these concerns had recently increased. This may be attributable in part to growing awareness of incidences of data breaches, but it is likely to be in part influenced by the ever increasing volume of data collection facilitated by the growing proliferation of technology such as IoT devices.

Extant privacy research in the IS domain leverages a number of theoretical lenses to understand the role of privacy across different contexts and information technologies. In his review of the literature Li (2012) categorises privacy theories into five areas of theories focused on; (1) drivers of privacy concern, (2) behavioural consequences, (3) trade-offs, (4) institutional drivers and (5) individual factors. While the privacy literature in the IoT domain is in a nascent stage, the existing literature focuses on theories related to behavioural consequences, trade-offs, and individual factors to a lesser degree. In terms of behavioural consequences, many of the existing IoT studies leverage technology adoption models such as the theory of reasoned action (TRA) (Marakhimov and Joo 2017). These studies build understanding of the factors driving individuals' initial adoption decision making process, but do not enhance understanding of individuals' post-use behaviours and barriers to the use of IoT (Marakhimov and Joo 2017).

One dominant stream of the broader privacy literature focuses on the trade-offs consumers make between the benefits and risks associated with new technology use and as a result information disclosure. The relevance

of trade-offs are apparent in the IoT context. As the number of devices a user connects with increases, the convenience and perceived benefits this usage facilitates increase (Hsu and Lin 2016) enabling users to query anything from health data to weather or utility usage. The data generated from the various IoT devices and connected databases does offer benefits but also introduces undeniable risks to consumers' privacy (Bélanger and Xu 2015). The most common theory to explore these trade-offs is the privacy calculus theory, which posits that individuals will disclose their personal information or interact with a technology for as long as the perceived benefits outweigh the perceived risks or consequences (Culnan 1993). The theory assumes that individuals conduct a cognitive cost-benefit analysis, considering the benefits of disclosure and the potential negative outcomes or repercussions the individual might experience as a result of using the technology (Culnan and Armstrong 1999). PCT has been recently leveraged in the IoT context. In their study of 508 Taiwanese citizens, Hsu and Lin (2016) found concern for information privacy had a negative influence on intentions to continue use of IoT, whereas perceived benefits had a positive influence on intentions. In a study of US consumers, Kim et al. (2019) explored perceptions of trust and benefits and perceived risk on three IoT services namely healthcare, smart home, and smart transport. In terms of healthcare, privacy risk had a significant negative influence on willingness to disclosure personal data, with trust and perceived benefits positively influencing willingness. In terms of both smart transport and smart homes, trust and perceived benefits had a significant, positive effect but perceived risk was insignificant. Perceived benefits was the biggest predictor of willingness to provide information in the case of healthcare and smart transport, whereas trust was the biggest predictor in the case of smart homes. These studies provide empirical support for the use of PCT in the IoT context, illustrating that both positive perceptions (i.e. trust and benefits) influence adoption and information disclosure, and negative perceptions (i.e. risk and privacy concern) can have a negative influence.

Notwithstanding the foregoing, due to biases and cognitive limitations, consumer's perception of the benefits often outweighs perceived risks or concerns. This view has also been presented in the IoT context with Kim et al. (2019) arguing that consumers seek benefits in spite of their privacy concerns and often underestimate the risks of IoT usage to their data privacy. This contradiction is termed the 'privacy paradox'. However, research explaining the privacy paradox is still emerging. Furthermore, it is

important to consider potential knowledge gaps (Crossler and Bélanger 2017). Individuals may assume their data remains private and is not shared with other parties (Kim et al. 2019), and thus their behaviours may only seem to contradict their desire for privacy. Furthermore, we do not yet fully understand how behaviours contradict privacy concerns (Keith et al. 2015).

In terms of individual theories, protection motivation theory (PMT) is frequently leveraged in the privacy literature to explore the influence of individuals' threat and coping appraisals on their behaviours (Li 2012). In their study of 206 health wearable users in the United States, Marakhimov and Joo (2017) leverage PMT. They found that consumers' threat appraisal was significantly influenced by their general privacy concerns and their health information privacy concerns, with threat appraisals significantly influencing problem and emotion focused coping and extended use intentions as a result.

In the IoT context, no study has yet explored privacy using an institutional based-theory. However, in their early stage work, Saffarizadeh et al. (2017) leverage social reciprocity theory to propose a model which explains consumers' willingness to disclose personal data to conversational assistants. They include privacy concerns as a negative determinant on disclosure. As perceived trustworthiness leads to consumers being more likely to disclose information (McKnight et al. 2011), to foster this trust, Saffarizadeh et al. (2017) argue that in line with social reciprocity theory, disclosures from conversational assistants may encourage users to trust them. These studies provide important insights into the perceptions driving behaviour in the IoT context, but it is important to explore approaches to influence these perceptions and engender perceptions of trust and privacy as a result.

7.3 Trust, Privacy, and the Internet of Things

A consumer's willingness to trust is based on their beliefs of the trustworthiness of the organisation (van der Werff et al. 2019). These beliefs together encapsulate the assumption that the organisation will not engage in opportunistic behaviour with the individual's data (Dinev and Hart 2006) and generally relate to beliefs regarding the organisation's benevolence, integrity, and competence (van der Werff et al. 2019). Benevolence relates to the belief the organisation has the individual's best interests in mind, integrity refers to the belief in the morals and principles of the

organisation, and competence refers to the belief the organisation has the knowledge and skills to fulfil a service (Belanger et al. 2002).

Trust and privacy are often studied in tandem in many contexts including IoT, with privacy concerns negatively impacting disclosure or technology adoption and trust having the opposite influence. Generally speaking, trust in a privacy context relates to an individual's willingness to be vulnerable when transacting or sharing personal information with an organisation (McKnight et al. 2011). In the IoT context, trust can be described as consumers' willingness to be vulnerable when interacting and sharing personal data with an IoT device, the associated application, and the organisation(s) providing these. In the IoT context, there are also dimensions of trust to consider namely device trust, processing trust, connection trust to ensure data is exchanged appropriately and trust in the overall system (Daubert et al. 2015). The opaqueness of the IoT service chain makes this logistically near-impossible. While there are technical solutions in place or proposed to achieve these dimensions of trust such as trusted computing, confidentiality, certifications, and more recently, blockchain (Daubert et al. 2015; Chanson et al. 2019), there is a need to account for consumers' perceptions of trustworthiness.

7.4 Approaches for Influencing Perceptions of Privacy and Trust

As evidenced in the IoT and broader privacy literature, concern for privacy negatively impacts disclosure and willingness to use new technologies, whereas trust can positively impact adoption and disclosure behaviours (Kim et al. 2019). However, the nature of the Internet and interactions between consumers and technology or devices complicates mechanisms for building trust (van der Werff et al. 2019). It is thus important to explore mechanisms to build a sense of privacy, that is perceived control over how one's personal information is collected and used, and foster a sense of trust, that is consumers' willingness to accept vulnerability when interacting with IoT devices.

In terms of overcoming privacy concerns, prevailing suggestions in the privacy literature include increasing consumers' perceptions of control (Tucker 2014), building trust (Dinev and Hart 2006) and reducing perceptions of risk (Xu et al. 2011). In order to influence consumers' perceptions, organisations must transparently communicate with users with

regards to the controls they have over their personal data, what data is collected, and how data is used. While the efficacy of organisations' communication methods in the IoT context is yet to be tested, the need for communication prevails. For instance, in a study of smartwatch users, Williams et al. (2019) found that users who had not been primed on the risks to their personal data on smartwatches, did not perceive any risks as they hadn't learned the value of this data. Researchers have proposed that IoT providers offer users an awareness of the privacy risks, provide users with control over the collection and usage of their data by smart devices (Ziegeldorf et al. 2014; Davies et al. 2016), and control over subsequent usage by additional third-party entities and devices (Hsu and Lin 2016). This again highlights the importance of education efforts for users of IoT devices.

In terms of trust, there are no means to assess trustworthiness of IoT devices (Alrawais et al. 2017). Trust is typically developed over time as opposed to being formed based on a one-time interaction (Gefen et al. 2008). This makes trust building between consumers and online organisations or IoT devices complex. To build trust in online organisations, several approaches have been explored. Firstly the characteristics of a website such as website design, security seals or privacy policies have been examined in the literature (van der Werff et al. 2018). However, the findings on the effectiveness of these approaches have been mixed. Moreover, given that the interaction with IoT devices does not involve regular interaction with websites, many of these methods are impractical or insufficient. It is also important for the user to trust the device, as highlighted in the study by Saffarizadeh et al. (2017), and the organisation itself (IoT service provider).

The dominant method for communicating how organisations collect and use consumers' data are privacy policies. It is argued that privacy policies could reduce perceived risks, increase perceptions of control and trust (Xu et al. 2011; Pan and Zinkhan 2006) and thereby overcome any privacy obstacles. However, privacy policies tend to be quite lengthy and difficult to read (Kelley et al. 2010). Thus, when customers read privacy policies, they fail to understand the contents (Park et al. 2012) and as a result these disclosures may have the opposite to the intended impact and exacerbate concerns around control and risk. There is a need to both adjust the content of policies and develop methods which better inform consumers of how their information is used (Park et al. 2012). To combat these issues, researchers developed the privacy label based on the nutrition

Fig. 7.1 Example GDPR label (Fox et al. 2018)

label approaches and found that privacy labels could improve understanding of privacy practices (Kelley et al. 2009, 2010) and build perceptions of trust (van der Werff et al. 2019). This approach has recently been adapted to develop GDPR-based (General Data Protection Regulation) privacy labels (see Fig. 7.1) (Fox et al. 2018).

7.5 Privacy Trust Labels: Design Principles

We argue that IoT service providers should draw from this recent research on privacy and trust labels to develop an IoT based privacy label. The label should seek to build consumers' understanding of how their data is used and collected to comply with privacy regulation and build positive privacy perceptions, as well as information on the organisation to build perceptions of trustworthiness. For example, in Europe, to comply with the GDPR, the labels must include the following information (ICO 2017):

1. The identity and contact details of the data controller
2. The processing purposes for the personal data and the legal basis for the processing
3. The recipients or categories of recipients of the personal data
4. The details of the safeguards in place if transferring data to a third country
5. Data retention period
6. The data subject's rights to request: access to their data, rectification, restriction of processing, erasure of data, and data portability
7. If data processing is based on consent, the right to withdraw consent at any time
8. The right to complain to the supervisory authority
9. whether the disclosure of personal data is a statutory or contractual requirement and the consequences of non-disclosure
10. The use of automated decision-making such as profiling, the logic and impact of such processing
11. The contact details of the data protection officer
12. Information on further processing.

All information on the label should be framed in a manner, which demonstrates the benevolence, integrity, and competence of the IoT service provider with regards to protecting consumers' personal data. Traditionally, privacy labels are presented to users upon signing up to an online website or service. As IoT devices cross physical and informational boundaries, the physical security and wellbeing of citizens and their homes is intertwined in the security and privacy of the IoT devices and the network (Lowry et al. 2017). We thus, recommend the inclusion of physical privacy labels on the box of IoT devices, along with a digital label on the application presented to users at sign-up and an up to date label accessible within the application's privacy features and on the service provider's website.

7.6 Towards a Framework for Examining the Impact of Privacy Disclosures on Privacy Perceptions and Behaviours

In this section, we present a general framework for building consumers' perceptions of trust and privacy in the IoT context in Fig. 7.2 below that can be used for examine privacy and trust perceptions and behaviours in the Internet of Things. We illustrate the use of this framework in the context of the Privacy Trust Label described in Sect. 7.5 above.

With IoT technologies advancing at a faster pace than privacy regulation and practices (Lowry et al. 2017), it is important for IoT service providers to be proactive in addressing consumers' privacy concerns. Consumer perceptions of privacy are situational in nature in that they are influenced by past experience and the context in question (Li 2011). For example, individuals have perceptions of how much privacy they have in the e-commerce context, which may be influenced by past experience of a positive nature, such as convenient online shopping, and experience of a negative nature, such as a privacy invasion. Furthermore, individuals' have perceptions regarding well-known brands. These perceptions may relate to how the brand protects consumer privacy and how trustworthy the brand is with regards to protecting and fairly using personal data. For example, if a consumer perceives that Apple smartphones offer a

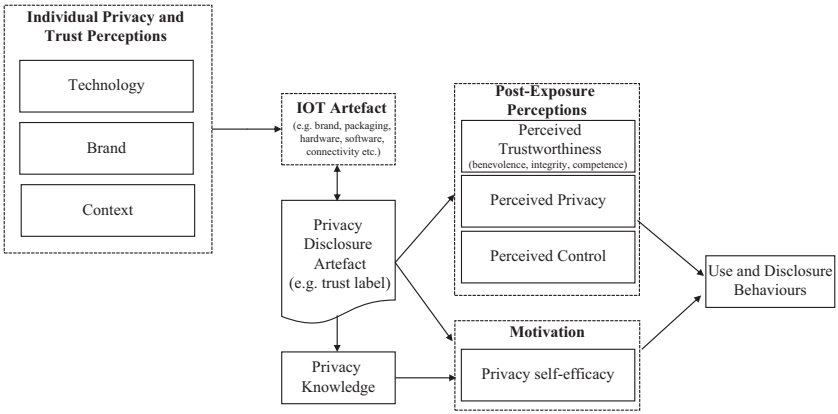

Fig. 7.2 Integrated framework to examining privacy and trust perceptions and behaviours

satisfactory level of privacy and the brand is trustworthy in terms of competence to protect data, integrity and benevolence with how that data is used, the consumer may hold positive perceptions about the trustworthiness and privacy offered by Apple products in other contexts such as the Apple watch or Apple TV. We present a framework that recognises that consumers have pre-existing perceptions and preferences regarding privacy and trust in technologies, brand and contexts (e.g. health, finance, social media, etc.). These may be general perceptions and preferences or specific to IoT. As such, these perceptions and preferences influence and are influenced by the brand, packaging, and the device hardware, software, and connectivity.

We draw from the integrative privacy framework developed by Li (2012) and the recently adapted Information–Motivation–Behavioural Skills Model by Crossler and Bélanger (2019). On the left hand of the model the IoT privacy label is presented. The label will seek to build consumers' privacy knowledge regarding how their personal data is collected and used by IoT devices. This label will in turn influence consumers' perceptions regarding the IoT device and service provider. In line with social contract theory (SCT) theory, we argue that the label will foster perceptions of control, trustworthiness, and privacy. SCT proposes that when organisations engage in transactions with customers which involve the disclosure of personal data, they enter into a social contract (Donaldson and Dunfee 1994). This contract implies that the organisation will only use the personal data in ways which align with social norms and that individuals have some level of control (Bélanger and Crossler 2011). We argue that the privacy label will form the basis of a social contract informing consumers of how their personal data is collected, stored, and disseminated in this specific context of the IoT device. Previous research has shown that privacy disclosures can enhance perceived control (Xu et al. 2011). We therefore argue that if consumers believe they retain some level of control over their personal data, they are more likely be willing to use IoT devices and disclose personal data. Similarly, privacy disclosures can potentially lead individuals to form positive perceptions related to privacy and heighten individuals' beliefs in the trustworthiness of the organisation (Culnan and Armstrong 1999). We propose a similar effect in the context of IoT devices.

Following on from perceptions and knowledge, Crossler and Bélanger (2019) discuss the privacy knowledge–belief gap and highlight the importance of contextualised privacy self-efficacy, that is individuals' perceptions

that they have the knowledge and skills needed to protect the privacy of their data as required. We argue that the privacy label will provide context-specific insights into *how* users can retain control over their data collected by IoT devices. This self-efficacy will in turn influence consumers' intentions to engage in privacy-protective behaviours such as adapting privacy settings (Crossler and Bélanger 2017, 2019). On the right hand of the model is users' usage and disclosure behaviours. We argue that the privacy label will build consumers' privacy self-efficacy and provide them with the motivation to exercise control over their privacy by modifying the privacy settings on IoT devices. We propose that consumers with high self-efficacy will adopt and continue to use IoT devices due to the high perceptions of control, privacy, and trust fostered by the label and reconfirmed through exercising control over their data. Previous research has found that privacy labels can improve privacy knowledge (Kelley et al. 2009, 2010) and foster perceptions of trust and control (Xu et al. 2011; Pan and Zinkhan 2006). Furthermore, trust is positively associated with consumers' willingness to disclose personal information (Joinson et al. 2010), whereas privacy concern has the opposite influence (Culnan and Armstrong 1999). To overcome privacy concerns, it is important to build perceptions of privacy and control. In summary, we posit that the clear transparency enabled by the privacy label approach can serve to enhance privacy knowledge, build consumers' perceptions of privacy, control and trust, and enhance privacy self-efficacy, thus empowering consumers to utilise IoT devices while retaining some level of privacy. We argue that with this knowledge, consumers can choose what personal data to disclose to IoT devices.

7.7 Concluding Remarks

In the coming years, IoT is predicted to grow exponentially generating value for consumers in all aspects of their lives. Researchers have highlighted the importance of ensuring user privacy in the IoT context, stating users' privacy 'should be guaranteed' (Sicari et al. 2015, p. 151). Furthermore, as technology continues to increase in pervasiveness, it is important to explore how trust can be engendered in and between technologies that are built upon complex data exchange infrastructures and a lack of prior experience with the technology in question (van der Werff et al. 2018). In this chapter, we present a framework for examining the effectiveness of privacy disclosures on privacy and trust perceptions and consequently, enhancing adoption and sustained usage of IoT devices.

The framework is contextualised in the broad IoT context. Empirical research is needed to determine the effectiveness of the proposed privacy label and the framework itself in different IoT contexts, applications, and other dimensions. For example, adaptation may be required for use cases such as conversational assistants where data collection occurs verbally and may require the consideration of factors outlined by Saffarizadeh et al. (2017). Moreover, there is a need for research that maps out the privacy issues across the broader IoT landscape including the device, connection, and application layers discussed in Chap. 1.

In addition to addressing consumer perceptions regarding privacy and trust related to IoT, it is important to consider technical advances such as fog computing. Fog computing can facilitate the realisation of many new applications on IoT devices, while also reducing latency, enabling mobility, location awareness and heterogeneity (Alrawais et al. 2017). In terms of security, the computational power offered by fog computing combined with the devices and sensors of the IoT could provide enhanced security to minimise attacks. However, issues related to privacy and trust are likely to be complicated by advances in fog computing (Alrawais et al. 2017). Further research, may look to adapt this framework for fog computing and other advances in technology that have privacy implications, not least artificial intelligence.

References

Abomhara, Mohamed, and Geir M. Køien. 2014. *Security and Privacy in the Internet of Things: Current Status and Open Issues.* 2014 international conference on privacy and security in mobile systems (PRISMS), 1–8. IEEE.

Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. 2017. Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Computing* 21 (2): 34–42.

Bélanger, France, and Robert E. Crossler. 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* 35 (4): 1017–1042.

———. 2019. Dealing with Digital Traces: Understanding Protective Behaviors on Mobile Devices. *The Journal of Strategic Information Systems* 28 (1): 34–49.

Bélanger, France, and Heng Xu. 2015. The Role of Information Systems Research in Shaping the Future of Information Privacy. *Information Systems Journal* 25 (6): 573–578.

Belanger, France, Janine S. Hiller, and Wanda J. Smith. 2002. Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *The journal of strategic Information Systems* 11 (3–4): 245–270.

Chanson, Mathieu, Andreas Bogner, Dominik Bilgeri, Elgar Fleisch, and Felix Wortmann. 2019. Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data. *Journal of the Association for Information Systems* 20 (9): 10.

Cisco. 2013a. Internet of Everything: A $4.6 Trillion Public-Sector Opportunity. https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf.

———. 2013b. Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion. https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-economy-insights.pdf.

Crossler, R. E., & Belanger, F. (2019). Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. *Information Systems Research* 30 (3), 995–1006.

Crossler, Robert E., and France Bélanger. 2017. *The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors*. Proceedings of the Hawaii International Conference on System Sciences.

Culnan, Mary J. 1993. How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly* 17: 341–363.

Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10 (1): 104–115.

Daubert, Joerg, Alexander Wiesmaier, and Panayotis Kikiras. 2015. *A View on Privacy & Trust in IoT*. 2015 IEEE International Conference on Communication Workshop (ICCW), 2665–2670. IEEE.

Davies, Nigel, Nina Taft, Mahadev Satyanarayanan, Sarah Clinch, and Brandon Amos. 2016. *Privacy Mediators: Helping IoT Cross the Chasm*. Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, 39–44. ACM.

Dinev, Tamara, and Paul Hart. 2006. An Extended Privacy Calculus Model for e-Commerce Transactions. *Information Systems Research* 17 (1): 61–80.

Donaldson, Thomas, and Thomas W. Dunfee. 1994. Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. *Academy of Management Review* 19 (2): 252–284.

Fox, Grace, Colin Tonge, Theo Lynn, and John Mooney. 2018. *Communicating Compliance: Developing a GDPR Privacy Label*. Proceedings of the 24th Americas Conference on Information Systems.

Gefen, David, Izak Benbasat, and Paula Pavlou. 2008. A Research Agenda for Trust in Online Environments. *Journal of Management Information Systems* 24 (4): 275–286.

Haller, Stephan, Stamatis Karnouskos, and Christoph Schroth. 2008. *The Internet of Things in an Enterprise Context*. Future Internet Symposium, 14–28. Berlin, Heidelberg: Springer.

Hsu, Chin-Lung, and Judy Chuan-Chuan Lin. 2016. An Empirical Examination of Consumer Adoption of Internet of Things Services: Network Externalities and Concern for Information Privacy Perspectives. *Computers in Human Behavior* 62: 516–527.

ICO. 2017. Privacy Notices, Transparency and Control. A Code of Practice on Communicating Privacy Information to Individuals. https://ico.org.uk/for-organisations/guide-to-dataprotection/privacy-notices-transparency-and-control/

Joinson, Adam N., Ulf-Dietrich Reips, Tom Buchanan, Carina B. Paine, and Schofield. 2010. Privacy, Trust, and Self-disclosure Online. *Human–Computer Interaction* 25 (1): 1–24.

Keith, Mark J., Jeffry S. Babb, Paul Benjamin Lowry, Christopher P. Furner, and Amjad Abdullat. 2015. The Role of Mobile-Computing Self-efficacy in Consumer Information Disclosure. *Information Systems Journal* 25 (6): 637–667.

Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. *A Nutrition Label for Privacy*. Proceedings of the 5th Symposium on Usable Privacy and Security, 4. ACM.

Kelley, Patrick Gage, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*. Proceedings of the SIGCHI Conference on Human factors in Computing Systems, 1573–1582. ACM.

Kim, Min Sung, and Seongcheol Kim. 2018. Factors Influencing Willingness to Provide Personal Information for Personalized Recommendations. *Computers in Human Behavior* 88: 143–152.

Kim, Dongyeon, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. 2019. Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services. *Computers in Human Behavior* 92: 273–281.

Li, Yuan. 2011. Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *CAIS* 28: 28.

———. 2012. Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework. *Decision Support Systems* 54 (1): 471–481.

Lowry, Paul Benjamin, Tamara Dinev, and Robert Willison. 2017. Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda. *European Journal of Information Systems* 26 (6): 546–563.

Marakhimov, Azizbek, and Jaehun Joo. 2017. Consumer Adaptation and Infusion of Wearable Devices for Healthcare. *Computers in Human Behavior* 76: 135–148.

McKnight, D. Harrison, Michelle Carter, Jason Bennett Thatcher, and Paul F. Clay. 2011. Trust in a Specific Technology: An Investigation of Its Components and Measures. *ACM Transactions on Management Information Systems (TMIS)* 2 (2): 12.

McKinsey Global Institute. 2015. The Internet of Things: Mapping the Value Beyond the Hype. McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx.

Pan, Yue, and George M. Zinkhan. 2006. Exploring the Impact of Online Privacy Disclosures on Consumer Trust. *Journal of Retailing* 82 (4): 331–338.

Park, Yong Jin, Scott W. Campbell, and Nojin Kwak. 2012. Affect, Cognition and Reward: Predictors of Privacy Protection Online. *Computers in Human Behavior* 28 (3): 1019–1027.

Pike, S., M. Kelledy, and A. Gelnaw. 2017. Measuring US Privacy Sentiment: An IDC Special Report.

Saffarizadeh, Kambiz, Maheshwar Boodraj, and Tawfiq M. Alashoor. 2017. *Conversational Assistants: Investigating Privacy Concerns, Trust, and Self-disclosure*. Thirty Eighth International Conference on Information Systems, South Korea.

Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks* 76: 146–164.

Tucker, Catherine E. 2014. Social Networks, Personalized Advertising, and Privacy Controls. *Journal of Marketing Research* 51 (5): 546–562.

van der Werff, Lisa, Colette Real, and Theo Lynn. 2018. Individual Trust and the Internet. In *Trust*, ed. R. Searle, A. Nienaber, and S. Sitkin. Oxford, UK: Routledge.

van der Werff, Lisa, Grace Fox, Ieva Masevic, Vincent C. Emeakaroha, John P. Morrison, and Theo Lynn. 2019. Building Consumer Trust in the Cloud: An Experimental Analysis of the Cloud Trust Label Approach. *Journal of Cloud Computing* 8 (1): 6.

Williams, Meredydd, Jason R.C. Nurse, and Sadie Creese. 2019. Smartwatch Games: Encouraging Privacy-Protective Behaviour in a Longitudinal Study. *Computers in Human Behavior* 99: 38–54.

Xu, Heng, Tamara Dinev, Jeff Smith, and Paul Hart. 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems* 12 (12): 1.

Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. 2014. Privacy in the Internet of Things: Threats and Challenges. *Security and Communication Networks* 7 (12): 2728–2742.