INTERNET POLICY REVIEW
Journal on internet regulation

Volume 6 | Issue 1

Towards responsive regulation of the Internet of Things: Australian perspectives

Megan Richardson
Melbourne Law School, The University of Melbourne, Australia, m.richardson@unimelb.edu.au

Rachelle Bosua
Department of Computing and Information Systems, The University of Melbourne, Australia, rachelle.bosua@unimelb.edu.au

Karin Clark
Melbourne Law Masters, The University of Melbourne, Australia, karin.clark@unimelb.edu.au

Jeb Webb
Department of Computing and Information Systems, The University of Melbourne, Australia, jeb.webb@unimelb.edu.au

Atif Ahmad
Department of Computing and Information Systems, The University of Melbourne, Australia, atif@unimelb.edu.au

Sean Maynard
Department of Computing and Information Systems, The University of Melbourne, Australia, Sean.Maynard@unimelb.edu.au

Published on 14 Mar 2017 | DOI: 10.14763/2017.1.455

Abstract: The Internet of Things (IoT) is considered to be one of the most significant disruptive technologies of modern times, and promises to impact our lives in many positive ways. At the same time, its interactivity and interconnectivity poses significant challenges to privacy and data protection. Following an exploratory interpretive qualitative case study approach, we interviewed 14 active IoT users plus ten IoT designers/developers in Melbourne, Australia to explore their experiences and concerns about privacy and data protection in a more networked world enabled by the IoT. We conclude with some recommendations for 'responsive regulation' of the IoT in the Australian context.

Keywords: Internet of things, Innovation

Article information

Received: 02 Jun 2016 **Reviewed:** 02 Feb 2017 **Published:** 14 Mar 2017
Licence: Creative Commons Attribution 3.0 Germany
Funding: Thanks to the Melbourne Networked Society Institute at the University of Melbourne for funding our research project 'The Internet of Things (IoT) and Consumer Privacy', 2015-2016.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/towards-responsive-regulation-internet-things-australian-perspectives

Citation: Richardson, M. & Bosua, R. & Clark, K. & Webb, J. & Ahmad, A. & Maynard, S. (2017). Towards responsive regulation of the Internet of Things: Australian perspectives . *Internet Policy Review*, *6*(1). https://doi.org/10.14763/2017.1.455

This paper is part of Australian internet policy, a special issue of Internet Policy Review *guest-edited by Angela Daly and Julian Thomas.*

Acknowledgement: Thanks to the Melbourne Networked Society Institute at the University of Melbourne for funding our research project 'The Internet of Things (IoT) and Consumer Privacy', 2015-2016, and to our participants for generously sharing their experiences and concerns about the IoT. Some of the information and ideas in this article draw on Richardson et al., 2016.

INTRODUCTION

Collaboration, networking and innovation are predicted to change radically as we move into an era of the Internet of Things (IoT). One of the fastest-growing trends in computing, the IoT promises to be one of the most significant disruptive technologies of modern times, affecting multiple areas of human life including manufacturing, energy, health, automotive, retail, insurance, crime, fraud and threat detection (Dutton, 2014; Gartner, 2014; OECD, 2015; Vermesan et al., 2011). Although there are multiple definitions of the IoT (Noto La Diega & Walden, 2016), the essence is that the IoT involves computing beyond the traditional desktop, concentrated on smart connectivity of objects with existing networks and context-aware computation using network resources (Gubbi, Buyya, Marusic, & Palaniswami, 2013). Indeed, connectivity of heterogeneous objects and smart devices is a crucial part of the IoT (Atzori, Iera, & Morabito, 2010; Caron, Bosua, Maynard, & Ahmad, 2016; Gubbi et al., 2013; Noto La Diega & Walden, 2016). Interactivity and interconnectivity are therefore at the heart of the IoT, and promise to impact our lives in many positive ways.

At the same time, while the IoT holds great promise, it poses significant challenges to users' abilities to control access to and use of their personal data (Caron et al., 2016; Dutton, 2014; Weber, 2009, 2010). This challenge and the attitudes of users and designers/developers in Australia is the particular focus of this paper. In the sections that follow we commence with a brief overview of the literature on privacy, data protection and the IoT, followed by a description of our qualitative research design, key findings and discussion of the findings. We conclude with

some minimalist proposals for legal regulation of the IoT in Australia, based on an idea of responsive regulation i.e. of law responding to public concerns in fashioning legal standards (Nonet & Selznick, 1978; Nonet & Selznick, 2001).

BACKGROUND

Maintaining a desired level of privacy and data protection (or 'data privacy' as it is sometimes termed) [1] is an ever-present concern in an era of ubiquitous computing (Weber, 2015). Indeed the concerns have existed since at least the early seventies. In the mid-eighties, information management ethicist Richard Mason warned that the increased collection, handling and distribution of information posed serious threats to the privacy, accuracy and accessibility of personal information (Mason, 1986). The protection of personal information from unwanted exposure and use, as part of information security, has become prominent as a complex concept studied from many perspectives including law, economics, psychology, management, marketing and information systems (Acquisti, John, & Loewenstein, 2013; Marabelli & Newell, 2012; Pavlou, 2011). For instance, just to give a few examples of the work that has been done, a number of studies have concentrated on issues associated with desktop computing environments, particularly with respect to the internet, e-commerce and marketing (Buchanan, Paine, Joinson, & Reips, 2007; Malhotra, Kim, & Agarwal, 2004; Wang, Lee, & Wang, 1998), the building of online consumer trust (Hoffman, Novak, & Peralta, 1999; Joinson & Paine, 2007), and the effects of social networking and social media tools (Donath, 2007; Ellison, 2007; Young & Quan-Haase, 2009).

To date, however, there has been very little empirical research on the experiences and concerns of IoT users and designers/developers (although see OECD, 2015, 266-272). On the other hand, there has been considerable discussion of how the IoT affects the 'privacy' of users with observations that new and emerging IoT technologies, seamlessly woven into the fabric of everyday life, are opening up increased avenues for unauthorised access to personal information, thereby increasing risks (Atzori et al., 2010; Dutton, 2014; Weber, 2015). These arguments tap into an older literature which warns against data-mining associated with the sharing of personal data online without appropriate safeguards to look after the particular interests of the information subjects (Galkin, 1996; Hamelink, 2000). On the other hand there are those who argue for the benefits of increased information sharing, for instance in terms of the delivery of services, innovation, or improved health, etc. (Barnes, 2006; Jenkins & Boyd, 2006). As yet, there has been little to indicate whether the IoT is perceived by users to raise serious risks through the IoT's generally unobtrusive data collection and processing activities. In view of the debates currently going on, and the lack of qualitative studies that focus on user concerns about data privacy with respect to the IoT, this study sets out to explore this issue in more depth in the particular context of Australia.

RESEARCH DESIGN

We were interested in current IoT users and designers/developers' experiences of, and views about privacy and data protection with respect to the IoT, in particular, what users wanted and wished for in terms of collection, storage, processing and use of private data/information through direct or indirect surveillance in an IoT world. Due to the exploratory nature of our study, we chose an interpretive, qualitative multi case study research design (Creswell, 2007;

Neuman, 2014; Yin, 2013). This design gave us access to rich data about a contemporary phenomenon within its real-life context. In addition case studies are ideal when the boundary between the phenomenon and its context is not immediately apparent (Yin, 2013).

We wanted to hear from IT literate individuals, drawn from a range of age groups, genders and professional groupings. The main criterion was that these individuals were actively invested in different types of IoT devices (e.g., smartphones, smartcards, RFID objects, home sensors, Fitbits, etc.) and were active IoT users (at least six months), employing their devices to facilitate their lifestyle, movement, health or any aspect of their life that can be enhanced and/or supported by the IoT's connectivity. Some participants were only IoT users, and these formed our core 'user' group. Others formed a group of designers/developers of IoT devices (who might also be IoT users but had a particular perspective due to their involvement on the business side). We randomly approached university students, business professionals, retired people, and (other) members of the public to participate in our study.

Twenty-four participants (14 IoT users and ten IoT designers/developers) ultimately agreed to participate by sharing their thoughts with us in a 30-40 minutes semi-structured face-to-face interview. Questions asked of users included themes about the importance and value of privacy, concerns about the ability of IoT users to control access to their personal information as well as use of their personal information once collected. Designers/developers were also asked about the available protection of personal information by the IoT, and whether there should be more protection. Both users and designers/developers were offered opportunities to say what they thought should be done in terms of legal regulation in this regard.

Interviews were audio-recorded, transcribed verbatim and analysed using normal qualitative coding techniques that identified major themes through three different coding techniques. A first pass through the data followed a bottom-up approach to identify NVivo or 'open' codes that represent noteworthy themes aligned with aspects identified in the literature review. A second pass through the data consolidated open codes into collections of similar axial codes. A final pass through the data involved scanning of data and prior codes to identify 'selective' codes. These codes involve comparing and contrasting cases to come up with meaningful and well-developed concepts (Miles & Huberman, 1994; Strauss & Corbin, 1990). NVivo 10 was used to support the coding and analysis activities while the whole research team and later two of the researchers discussed themes and coding outcomes respectively.

RESEARCH FINDINGS

A number of themes emerged from the process of interview and data coding, as outlined above. We touch on three in particular in the following sections:

- ***Privacy continues to be valued by IoT users***

Overwhelmingly, when asked to reflect on the value of privacy, users said privacy was a matter of serious concern to them. They were pretty confident in their understanding of 'privacy' here, for the most part equating this with the limited sharing of private information, for example 'age' or information of an especially personal kind (U2, U4), and some also indicated that there are different contexts such as health, religion, work-related things and relationships that might raise particular more 'sensitive' privacy concerns (U5, U11):

> It's about keeping your… what you want kept hidden… hidden or secret. … Confidentiality. So for me, privacy is confidentiality (U2).

> I think it's my choice—who do I want to share with? If I am sharing with my friends, it means that it has to be restricted to my friends only (U4).

> People not knowing things about me that I don't want to disclose. So that could be health, it could be religion, it could be work position, it could be certain relationships that I have. So for example, at work, my work life and my private life are separate and I like that. And, I'd like to maintain that (U5).

> Ok, so this reminds me of those three circles that they used to like to use at primary school, there's the Me, and the We, and the Everybody. So within the Me, there's stuff that you might consider sensitive data… stuff that I wouldn't want to discuss with anyone other than my partner… maybe about health related stuff. Within the We, there's stuff that I'd share with people that I know well and trust (U11).

- ***Users want greater control and transparency with regard to their IoT data***

As the discussions progressed users opened up about their desires to maintain knowledge and control over access to and use of their IoT data by others. By this stage, they appear to have moved beyond the idea of 'private information' used above, voicing concerns about personal data in a broader sense – as for instance, in the following comments (of U1, U2, U7, U8):

> There is not enough transparency around [who is protecting your data] … [The service providers] hold onto the data on your behalf. I have a rough idea of how it happens from a development level, but from a user level you have no idea (U1).

> I would love to restrict what businesses can do [with my data], you've got to have that, you've got to draw the line somewhere on what they can do [with your data] (U2).

> Well, I think that you should be able to choose what's put out there… I don't expect that [my personal information] to be passed on to other people (U7).

> For me, it's about having control and having some sort of default or settings that—as far as you understand—there is security. Beyond that, you know, there's a trust. How, when and why your information is used (U8).

> I would like to understand where all my data is and where it's going (U9).

> I think that one of the major things that an individual would want from those kinds of services is transparency. So they can see where their data is, they can access it, they can have access at least (U12).

Various reasons were also offered for wanting this level of knowledge and control: ranging through protecting the self from exposure (i.e. privacy in a traditional sense), to personal image management, to other reasons of a more practical kind (such as the availability of insurance, and security risks) as reflected in the following remarks (from U2, U5, U8, U11):

> I like to project an idealised self, you know, which is what social media is famous for … I do my best to regulate what people know about me (U2).

> Access [to personal information] can create opinions that can form bias or prejudice against somebody based on what they do outside of their professional career (U5).

> [It's] 'risky' when my sensitive data is given to unfamiliar parties, I don't want people to use it incorrectly, it needs to be [controlled] (U8).

> I don't really like the idea that some faceless guy… could… work out who I am; not who I am as an individual but, you know, work out stuff about me as a person (U11).*

Interestingly, in this discussion, there seemed to be no confidence in a sufficient level of protection being offered through the terms of the privacy policies of IoT providers. Indeed, users admitted these were rarely read: as some users (U2, U6, and U9) put it:

> Who has time to read disclaimers you know? You need a law degree to get through it. I think there should actually be a law about having legal disclaimers that the average man can read (U2).

> I think that, I mean, I think that companies know that people wouldn't take the time to just read the whole terms and agreement and accept it. They just assumed that people will accept it. And I think that that's kind of unfair (U6).

> Do I want to live my life in the way that I want to live it or do I want to spend my time ticking boxes and reading small print? (U9)

• ***There is a general unawareness of current legal protective measures***

Interviewees appeared to be generally unaware about the current legal protection of private and personal information. We were struck by the fact that there was no reference made to Australian consumer protection laws (for instance provisions dealing with misleading or deceptive conduct and unfair contract terms in the Australian Consumer Law, scheduled to the *Competition and Consumer Act 2010* (Cth)). Similarly, there was no reference to privacy and data protection laws including the main source of regulation, the *Privacy Act 1988* (Cth). Yet users seemed to want to have some minimal level of legal protection here, even if just in terms of a 'legal warranty' of anonymity. As one user (U6) remarked:

> Maybe having a legal warranty or some sort of approach that might give them [IoT users] security that the information being captured is not going to be linked back to them (U6).

Another user (U12) asked for more specific legal controls of their personal information, along the lines of what the *Privacy Act* provides (for those businesses that fall within its remit): [2]

> So [in] organisations there's no specific rule that will protect individuals and the information's just being collected all the time and used for money and income purposes for organisations. I don't think there are enough regulations about this to protect individuals in Australia (U12).

The same user elaborated on the appropriate legal standards prescribing how information may be used, proper notification, and scope for individuals to access their information:

> I think one of the major things an individual would want from those kinds of services, is transparency. So they can see where their data is, can access it. We talk about other [rights], so individuals can approve [services] and also know what kind of purpose is being served there, [i.e. with] the secondary users and so on. I think from a legal perspective, if an individual uses a service that is not complying with those kinds of things they should be protected by the law (U12).

In fact, even a number of the IoT designers/developers that we interviewed revealed some concerns about the apparent lack of legal regulation. One interviewee complained that certain 'cowboys' in the field were more focussed on innovation than privacy in the design of IoT devices as a result of entrepreneurial strategies aimed at quick innovation and pushing new products or services to the market as quickly as possible, adding that 'the legal framework is always a lagging indicator into what innovation offers' (D8). Similarly, another said:

> Once you add in the digital [IoT] medium it's again a matter of some paranoia or personal suspicion. I've seen in so many cases law lags technology, I would imagine the current legal framework is not fully up to the digital world just yet (D10).

RESPONSIVE LAW AS A REGULATORY MODEL

Two ideas stand out at this stage. First, more could be done to provide IoT users with opportunities for meaningful notice and control regarding the collection, storage and use of their personal information by IoT devices, but without unduly restricting designer/developer freedom to innovate (Dutton, 2014; OECD, 2015; Wolf & Polonetsky, 2013). Second, law might serve a useful purpose in explicitly encouraging designers/developers in consultation with users to frame and adapt these standards for themselves, incorporating them into the design of their IoT devices and services from the beginning – following an approach that many have advocated (Cavoukian, 2011; Cavoukian & Popa, 2016; Dutton, 2014; OAIC, 2016) and is increasingly treated as an aspect of a modern comprehensive data protection scheme (e.g., General Data Protection Regulation 2016, article 25, and more contestably Privacy Act 1988 (Cth), APP1). [3]

This is not to say that law should abdicate its role to regulate directly for misleading and unfair trade practices and to apply its general privacy and data protection standards. In fact we argue that far more should be done along these lines in Australia, drawing on the Australian Consumer Law to offer effective regulation of misleading or deceptive conduct and unfair contracting practices associated with the IoT, complementing the data protection standards of the *Privacy Act*, which might themselves be extended further (Richardson et al., 2016). Similarly, more general legal protections of 'privacy', as with the traditional action for breach of confidence or a possible privacy tort (the second still a matter of debate and occasional legislative proposals in Australia: for instance ALRC, 2014), allowing cases to be taken to court either by individuals or groups via class actions may perform a crucial role in protecting the privacy interests of IoT users (Richardson et al., 2016). But with a potentially ubiquitous IoT – the Internet of 'a trillion things', as William Dutton puts it (2014, 18) – there can be a range of benefits associated with the delegation of responsibility away from central regulators and courts and into the hands of the party or parties best able to devise and implement the standards for themselves. In other words, there is a clear role for law to operate indirectly rather than directly in this context (Lessig, 1999; 2006), responding to the voiced desires of IoT users and some designers/developers, i.e. those who consider themselves to be the more responsible operators rather than the 'cowboys', in prescribing a minimum level of 'privacy by design' or 'data protection by design' for the IoT.

The model of IoT regulation that we are advocating here is based on a well-accepted idea of 'responsive regulation' which treats regulation as ideally a minimal but effective (and if necessary escalating) intervention in the market (Ayres & Braithwaite, 1992) and prefers a 'participatory solution' over one that is 'repressive' (i.e., top-down and coercive) or 'autonomous' (i.e. based on traditional *laissez faire* legal approaches developed by courts applying common law doctrines) (Ayres & Braithwaite, 1992; Nonet & Selznick, 1978, 2001). In the particular context of the IoT, we argue that the approach can be given a concrete application through the adoption of 'privacy by design', or 'data protection by design', as the appropriate starting point for the regulation of the IoT in the responsive regulation pyramid below. Thus, rather than privacy/data protection by design being treated as operating alongside other forms of regulation in an unstructured and unpredictable (and potentially repressive) way, or alternatively being relied on to provide the entire scope of regulation of the IoT (which leaves a great deal of control still in the hands of designers/developers, which may be insufficient to address the particular needs of IoT users in some instances), it is treated as a first and fairly minimal response. Other more stringent responses (e.g., direct enforcement of consumer protection and data protection

standards, and privacy-type doctrines developed and enforced via cases taken to court) are treated as coming in higher up the pyramid, to be actioned if the minimal protection offered through the design of a particular IoT device turns out not to be sufficient in the circumstances. As such, the protection offered by privacy/data protection by design can focus on basic things that IoT users are saying they want – including, for instance, as spelt out by our IoT users (U6, U12) above, a level of 'transparency' (so that users 'can see where their data is, can access it'), along with certain 'rights' of approval (e.g., of some services plus 'secondary users', and with knowledge of the purpose is being served), as well as ideally protection of anonymity or the like where feasible (so 'information captured is not linked back to [individuals]'). [4]

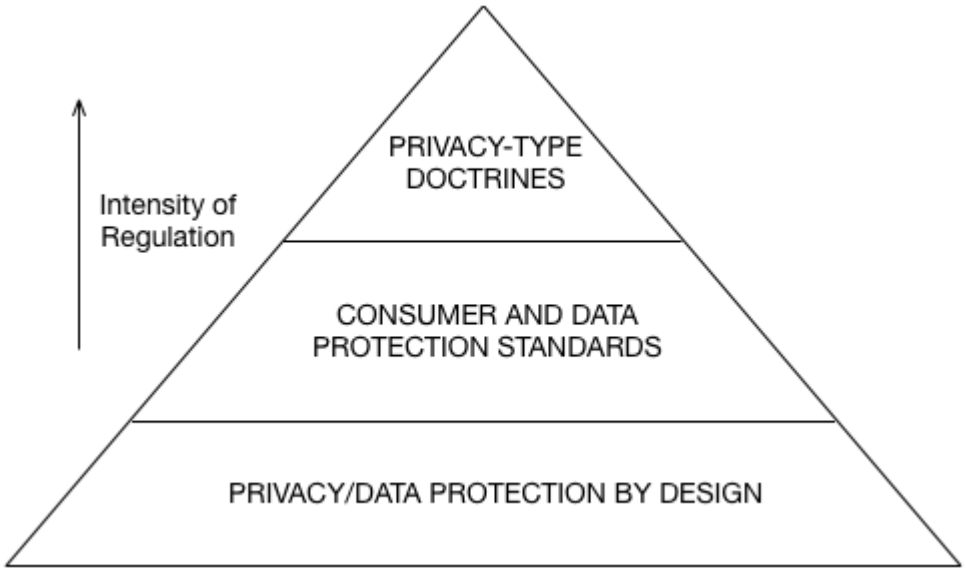

Figure 1: Responsive regulation pyramid for the IoT

FINAL REFLECTIONS

In this article, based on voiced concerns about privacy and data protection raised by a number of IoT users as well as some designers/developers in Australia, we have proposed a responsive system of privacy and data protection for the IoT beginning with privacy/data protection by design, covering basic matters such as notice and control throughout the life cycle of the data, then building up to more stringent consumer and privacy/data protection regulation provided under (*inter alia*) the Australian Consumer Law and *Privacy Act 1988* (Cth), and as a third tier actions brought by individuals in court to vindicate their claims relying on privacy-type doctrines as applied by judges (for instance, through the current action for breach of confidence, and/or a specific privacy tort if and when this becomes part of Australian law).

We note that our discussion has not touched on the question of higher levels of regulation, for instance the use of the criminal law to restrain and control the ways in which the IoT might be used for antisocial purposes, including, for instance, undesirable forms of ubiquitous surveillance. For our users, on the whole, seemed to be rather unconcerned about the dangers of surveillance by the IoT, or as Andrejevic and Burdon put it (2015, 24) 'the dimensions of a sensor society in which the devices we use to work and to play, to access information and to communicate with one another, come to double as probes that capture the rhythms of the daily lives of persons, things, environments, and their interactions', with attendant risks for human dignity and freedom. Thus users' responses to our interview questions do not offer much

support for broader reform of what might be termed Australian surveillance law. Accordingly, based on a model of responsive regulation (i.e. law responding to existing public concerns), our recommendations have centred around more limited questions of how well IoT users' private and personal information will be looked after, whether IoT users will be able to understand what is happening, and whether they can maintain control.

That is not to say that surveillance will not ultimately come to be seen more widely as a real problem of the IoT and that broader law reform measures will not be a focus of further public discussion. Indeed, already some of our interviewees argued that a coming issue will be the prospect of ubiquitous surveillance, affecting the basic structure of society (see Richardson et al., 2016). In response to this concern, law reform efforts in Australia may eventually need to be more deeply structural than the small-scale changes we have so far been contemplating.

REFERENCES

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*(2), 249-274.

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television & New Media, 16*(1), 19.

Australian Law Reform Commission (2014), *Serious invasions of privacy in the digital era*, Report No 123

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation*: New York: Oxford University Press.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165.

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review, 32*(1), 4-15.

Cavoukian, A. (2011). Privacy by Design: Origins, meaning, and prospects. *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Aspects and Standards, 170*.

Cavoukian, A., & Popa, C. (2016). Embedding privacy into what's wext: Privacy by Design for the Internet of Things. Ryerson University Privacy & Big Data Institute, April 2016.

Creswell, J. W. (2007). *Qualitative inquiry and research design: choosing among five approaches*. London: SAGE Publications.

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication, 13*(1), 231-251.

Dutton, W. H. (2014). Putting things to work: social and policy challenges for the Internet of things. *info, 16*(3), 1-21.

Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230.

Galkin, W. S. (1996). Privacy: What is it? *Computer Law Observer, 14*.

Gartner (Producer). (2014). Gartner says the Internet of Things will transform the data center. Retrieved from http://www.gartner.com/news/room/id/2684616

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7),

1645-1660.

Hamelink, C. J. (2000). *The ethics of cyberspace*. Sage.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80-85.

Jenkins, H., & Boyd, D. (2006). Discussion: MySpace and Deleting Online Predators Act (DOPA).

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. *The Oxford handbook of Internet psychology*, 237-252.

Lessig, L. (1999) (2006). *Code and other laws of cyberspace*: Basic books.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research, 15*(4), 336-355.

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: the practice perspective. *Journal of Strategic Information Systems, 21*, 18-30.

Mason, R. O. (1986). Four ethical issues of the information age. *Mis Quarterly*, 5-12.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook*. California, USA: SAGE publications.

Neuman, W. L. (2014). *Social research methods: Qualitative and quantitative approaches* (7th edition ed.). Essex, U.K.: Pearson.

Nonet, P., & Selznick, P. (1978). *Law and society in transition: Toward responsive law*: Transaction Publishers.

Nonet, P., & Selznick, P. (2001). *Toward responsive law: Law and society in transition*. Transactions Publishers, New Brunswick.

Noto La Diega, G., & Walden, I. (2016). Contracting for the 'Internet of Things': Looking into the nest. *Queen Mary School of Law Legal Studies Research Paper*.

OAIC. (2016). Office of the Australian Information Commissioner, 2015, Guide to securing personal information, January 2015.

OAIC. (2016), *Guide to big data and the Australian Privacy Principles: Consultation draft*, May 2016.

OECD. (2015). OECD Digital Economy Outlook 2015. Retrieved from doi:10.1787/9789264232440-en

Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS quarterly, 35*(4), 977-988.

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

Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: grounded theory procedures and techniques*. Thousand Oaks, CA. U.S.: SAGE publications.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., … Doody, P. (2011). Internet of Things Strategic Roadmap. In O. Vermesan & P. Friess (Eds.), *Internet of things: global technological and societal trends* (pp. 9–52). Aalborg: River Publishers.

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63-70.

Weber, R. H. (2009). Internet of things–Need for a new legal environment? *Computer law & security review, 25*(6), 522-527.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627.

Wolf, C., & Polonetsky, J. (2013). An updated privacy paradigm for the 'Internet of Things', Future of Privacy Forum, November 19.

Yin, R. K. (2013). *Case study research: Design and methods* (5th edition ed.). California: Sage Publications.

Young, A. L., & Quan-Haase, A. (2009). *Information revelation and internet privacy concerns on social network sites: a case study of facebook*. Paper presented at the Proceedings of the fourth international conference on Communities and technologies.

FOOTNOTES

1. Here we use ‘privacy’ in the particular sense of protecting the individual from the unwanted exposure and use of private information rather than in a looser sense of preserving control over personal information, treating that under the label ‘data protection’ or ‘data privacy’. We appreciate however that the concepts may be complementary and overlapping: see Richardson et al. (2016) for a fuller discussion.

2. Note that the Australian Privacy Act does not apply to ‘small businesses’ with an annual turnover of three million dollars or less, but subject to exceptions for small businesses that inter alia ‘provide a health service’ or ‘disclose personal information about another individual to anyone else for a benefit, service or advantage’: see Privacy Act 1988 (Cth), s 6D.

3. The Office of the Australian Privacy Commissioner (OAIC) takes the view that the Privacy Act’s Australian Privacy Principle 1 (‘open and transparent management of personal information’) can be drawn on to require or encourage privacy by design including for the IoT (OAIC, 2016a; OAIC, 2016b). If the idea is open and transparent (and non-contestable) standards, preferably this should be stated explicitly, as with article 25 of the European General Data Protection Regulation (2016) (‘data protection by design’).

4. Compare recital 78 EU General Data Protection Regulation on data protection by design: stating that measures might include, inter alia, ‘minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing,

enabling the controller to create and improve security features'. See also article 25.