Privacy in a world of the Internet of Things
A Legal and Regulatory Perspective
Research Paper 6
Privacy in a world of the Internet of Things
A Legal and Regulatory Perspective
Networked Society Institute Research Paper 6
December 2017

Authors
Rachelle Bosua, Megan Richardson, Karin Clark, Sean Maynard, Atif Ahmad and Jeb Webb
1. School of Computing and Information Systems
2. Melbourne Law School
University of Melbourne

Contact
Rachelle Bosua – rachelle.bosua@unimelb.edu.au

Acknowledgements
The authors would like to thank all the participants who generously gave their time to participate in our study.

ISBN
978-0-7340-5325-1

Licence
Creative Commons Attribution-ShareAlike – creativecommons.org/licenses/by-sa/4.0/

Cover Image
iStock

Networked Society Institute
The University of Melbourne's Networked Society Institute catalyses interdisciplinary research to understand and create the connected future. The Institute provides a focal point enabling the University of Melbourne to address the impact and realise the opportunities of connectivity on society.
networkedsociety.unimelb.edu.au
Executive Summary

The world of digital connectivity is changing rapidly as a result of the emergence of the Internet of Things (IoT). Representing one of the most disruptive technologies of our time, the IoT is an emerging global internet-based architecture that seamlessly integrates multiple data collection devices that collect, interchange and process data. Examples of IoT devices include wearables that monitor and track our wellbeing based on daily physical activities such as running or walking, medical devices that monitor and track intake of and responses to medication, and surveillance devices that track and monitor movement related to patient rehabilitation following accidents or age-related degeneration.

While the IoT holds great promise in terms of facilitating the collection and processing of data to improve and customise service delivery, there is a need to rethink what ‘privacy’ means to individuals and IoT designers/developers in the realm of increasing digital connectivity, and more generally how personal information should be collected, stored, transmitted and used. Moreover, what are legal perspectives on data privacy in an increasingly connected world enabled by the IoT?

Considering these challenges, we share our findings aiming to answer the following questions:

- How do IoT users (or consumers) perceive ‘data privacy’ in a connected world of greater connectivity enabled by the IoT?
- What are specific individuals’ IoT-related data privacy concerns?
- What can be done from a regulatory perspective to address individuals’ data privacy concerns?

In response to the above questions, an exploratory qualitative research design was followed. We collected data from 24 IoT users and designers/developers in the 22 - 65 age group to hear more about their feelings and perceptions of data privacy and legal regulation with respect to IoT data collection, processing and use.

Our study highlights four recommendations:

1. Data privacy is important in a more connected world enabled by the IoT.
2. Forms of consent for IoT data collection needs to be adapted to cater for today’s modern IT user requirements.
3. Incorporation of ‘privacy-by-design’ in the IoT development process may improve data privacy-related concerns.
4. A responsive regulation approach that includes ‘privacy-by-design’, consumer and data protection standards, and privacy type doctrines may enhance IoT privacy/data protection.
1 Privacy in a world of the Internet of Things

1.1 The Internet of Things (IoT)

The Internet of Things (IoT) represents one of the most disruptive technologies of modern times and holds many promises and advantages in terms of interweaving technologies in our everyday lives. The Internet of Things as a global emerging Internet-based information architecture represents a network of physical and virtual devices, objects and sensors embedded in other objects and the environment with specialized electronics, software and processing power enabling these objects to freely collect, process, exchange and distribute data (Weber, 2010). With predictions that this new era of computing will involve computing beyond the traditional desktop, this trend is already a reality with new developments in Virtual Reality (VR) and Augmented Reality (AR), 5G networking technologies, Cyber Physical Systems (CPS), machine learning, artificial intelligence, and new developments in infrastructure such as the cloud. Examples of the IoT include smart objects interacting through sensors embedded in homes and home devices (e.g. thermostat and lighting controls, smart refrigerators, televisions and washing machines), smart cities (e.g. secure building access, smart objects controlling traffic congestion, crime, pollution, and connected cars) and wearables (e.g. smart watches and wristbands for workouts, monitoring of mobility, people’s health conditions, remote health and the administering of medication).

Emerging IoT objects will contribute unimagined richness to our lives that will impact the way we interact socially, medically and technologically. As we move into a world of greater connectivity and networking enabled through the Internet of Things (IoT), we are also moving into an era of increased data collection related to our individual lives, movements, interactions with the world, others and sensory objects, and behavior-related data through surveillance devices and objects. Hence, the power of intelligent computing combined with new networking technology features and improved technological infrastructures to distribute and process data hold great promise to customise, focus and tailor service delivery for our daily living, wellbeing, social and medical needs.

1.2 Data privacy in the world of the IoT

The IoT challenges conventional understanding of what may be expected in terms of individual ‘privacy’ in a new hyper networked sensory environment. With an increase in cyber security threats, new measures are required to ensure and establish resilience to architectural attacks, data authentication and management, access control and user privacy needs related to this (Webber, 2010). In addition, user’s may have unique privacy requirements that need to be addressed not only in relation to the collection and processing of their data, but also through the design of IoT objects. Over the years, mutual appreciation has developed between software engineers and human-computer interface (HCI) designers to better understand the interdependent relationship between privacy, technology and situated technology use. In a new world of IoT artefact design it is necessary to follow an intensive participatory design approach that actively involves the data privacy needs of multiple users and stakeholders in the IoT design process.
1.3 Law, regulation and the IoT

New technological developments such as semantic web technologies and autonomous computing predict an era of linked open data enabling the sharing and re-use of virtual objects as a service through cloud infrastructures. Moreover, the open and ubiquitous nature of the IoT may increase its vulnerability to malicious attacks aiming to obtain private data or controlling physical environments in which IoT objects operate. These elements challenge the privacy of individuals collected and stored IoT data. Hence, new legal models, policies and frameworks are required to guarantee identity trust and liability management associated with individuals’ data and information privacy related to the design, development and contextual use of IoT objects.

2 Research methodology: data collection and analysis

We followed an exploratory qualitative research design as we were interested to hear how users and software developers/designers feel about privacy and regulation in a more connected world of the IoT. We also wanted to hear more of their hopes and fears and the kind of legal regulation they might expect of this world. We were interested in recruiting both active IoT users and software designers/developers to identify what they thought were happening in the field. Ultimately 24 participants in the 22 – 65-year age group, all from Melbourne, consented to participate and contributed to our study.

2.1 Participant profiles

We recruited participants through emails followed by snowballing whereby participants invited others and brokered links to potential participants that we ultimately followed up. Our participants were all IT literate, some more than others (classified on the low, medium and high scale). Fourteen participants were male and 10 were females while all our participants were active IoT users. Twelve of the participants were also software engineers (SEs) who were involved in software design/development activities of IoT artefacts.

Our participants came from multiple sources, including academia and private and public organisations. Our final set of participants were all professional and experienced and consisted of a cohort of eight university students, with our other participants as working professionals or consultants/employees in large, medium and small industries or government organisations. Table 1 gives a background summary of our participants in terms of gender, age group, professional work life and whether they were both experienced IoT users and/or designers/developers.
2.2 Data collection and analysis

Ethics clearance to conduct the study was granted in August 2015, after which we started to recruit participants. One of the researchers commenced data collection through semi-structured face-to-face interviews each lasting 30 to 40 minutes from mid-November 2015 to mid-March 2016.

Interview questions concentrated on the following:

- Knowledge and experience of the IoT (i.e. what IoT objects individuals used)
- Confidence in and concerns associated with IoT data collection and handling from a privacy and legal perspective,
- Individual perspectives on risks associated with the giving out of sensitive data/information in a more connected world
- Perspectives about informed consent and privacy
- Concerns about privacy and the processing, dissemination and storage of individual’s data collected through the IoT data
- Privacy concerns related to the design of IoT objects and devices
- IoT privacy aspects individual users felt could be improved
- The future of customer privacy from a legal and regulatory perspective.

All interviews were audio-recorded and transcribed verbatim. Transcribed interviews were collectively incorporated in the NVivo11 data analysis tool to support the analysis of interview transcripts. Coding followed a thematic approach concentrated on identifying user perceptions and feelings about privacy in terms of the collection, processing and dissemination of IoT data. In particular we wanted to identify user concerns about privacy in a world of more data collection. We were also conscious of software designers/developers’ comments on aspects that need to be considered to refocus privacy concerns in an increasingly connected IoT world. We also wanted to hear how the design of IoT artefacts could be improved in view of individuals’ data privacy concerns.

Table 1: Summary of study participant’s background

<table>
<thead>
<tr>
<th>Interviewee number</th>
<th>User Classification</th>
<th>Gender</th>
<th>Age</th>
<th>IT literacy (IoT use or development)</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1 - U2</td>
<td>User</td>
<td>Male</td>
<td>22-39</td>
<td>Med to High</td>
</tr>
<tr>
<td>U3- U6</td>
<td>User</td>
<td>Female</td>
<td>22-39</td>
<td>Med to High</td>
</tr>
<tr>
<td>U7 - U9</td>
<td>User</td>
<td>Male</td>
<td>40-61</td>
<td>Med to High</td>
</tr>
<tr>
<td>U10 - U12</td>
<td>User</td>
<td>Female</td>
<td>51-61</td>
<td>Low to Medium</td>
</tr>
<tr>
<td>D1 - D4</td>
<td>Designer &amp; User</td>
<td>Male</td>
<td>22-39</td>
<td>Med to High</td>
</tr>
<tr>
<td>D5 - D7</td>
<td>Designer &amp; User</td>
<td>Female</td>
<td>22-39</td>
<td>Med to High</td>
</tr>
<tr>
<td>D8 – D12</td>
<td>Designer &amp; User</td>
<td>Male</td>
<td>40-61</td>
<td>High</td>
</tr>
</tbody>
</table>
3 Findings: Individual perspectives on privacy and IoT

Our data analysis yielded key findings presented in two categories that describe user concerns about data privacy (Section 3.1) and IoT designer/developer concerns about data privacy (Section 3.2).

3.1 IoT user concerns about data privacy

3.1.1 IoT users value data privacy

Even though the proliferation and use of social media tools and technologies give the impression of a world devoid of privacy, most of our interviewees (both users and designers) felt that they valued their personal information and wanted to keep it under their control. Initial discussions concentrated on the meaning of privacy and evidence indicated clarity in understanding ‘privacy’ as a concern about limiting exposure of personal information considered sensitive. Most participants felt there was a clear boundary delineating what others need to know about oneself as summed up by one of the participant’s comments:

*Privacy means there are things I don’t want people to know about me, and there are things that I’m happy for people to know about me and I like to think that I project the things that I want people to know, and then don’t project the things that I don’t want people to know (U1)*

*Privacy] is about keeping your… what you want kept hidden or secret… confidentiality. So for me, privacy is confidentiality’ (U2)*

*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 (U7)*

Hence, IoT users had a clear understanding of privacy adopting a traditional language of privacy as essentially a ‘concern over our accessibility to others’.
3.1.2 Users want greater transparency and control of IoT data

As privacy discussions with participants proceeded, it became clear however that IoT users were especially concerned about the control they had over their collected personal data and knew very little about how their collected data was being used. Even though they did not use the term ‘privacy’ to describe this concern one user’s comment succinctly echoed this concern:

There is not enough transparency around [who protects your data]. [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 (D1).

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 (U10).

Others indicated they wanted ‘to understand where all my data is and where it’s going’, while another participant indicated that s/he would ‘love to restrict what businesses can do [with my data]...you’ve got to draw the line somewhere on what they can do [with your data]’. Others indicated reasons why they wanted more control that varied from limited self-exposure (‘I don’t want some faceless guy...work out who I am, not who I am as an individual, or work out stuff about me as a person’) to personal image management (‘I like to project an idealized self you know, which is what social media is famous for’) and self-regulation (‘I do my best to regulate what people know about me’). Another participant expressed concern that his current health insurance might be jeopardized stating (‘If you took my [rewards cards] and you analysed my food buying pattern and saw that is was horrendous – and then you saw that I was doing less than 2,000 steps a day and I have a resting heart rate of 180, I’d be in the worst case for [health] insurance’). These expressions indicated that IoT users were concerned about their personal data and others’ ability to control and understand their patterns of behaviour stemming from their personal information. (For ease of reference we will term this particular concern one about ‘data privacy’.)
3.1.3 Suggestions to improve transparency and control

Participants gave practical suggestions on mechanisms to improve their understanding of and control of their personal data collected through the IoT. A range of responses indicated ideas such as ‘reporting on everything that is held on you’ to ‘allow for the deletion of information’ when desired, and even having the ability to ‘lock [my personal data] right down’ or ‘I want to release it [my personal data], to a more arduous demand of having a ‘me’ online portal allowing individuals to ‘see the top services that I have signed up for’ allowing that ‘...I could break those [online] links, delete those silos of information’.

IoT users mistrusted providers’ privacy policies and felt the terms and conditions were cumbersome to read through as one user indicated:

*We have to agree to the terms and conditions of services in order to use them [IoT objects]. And nobody pays any attention to that… even if you do, unless you agree to the conditions, you can’t use the service. That is a ‘by default opt in’ [situation] and you have no ability to opt out. It’s not true consent’ (U7).*

Giving consent to data collection was considered onerous and complex with an overwhelming number of boxes to be ticked taking time, as one participant stated: ‘who has time to read disclaimers?’. Another participant compared the complexity of giving consent to ‘… 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’. In addition, IoT users felt they were uncertain as to not knowing ‘when they [IoT providers] are going to change their privacy settings and you don’t know when they’re going to change their policies and give away your data to anyone’. Most, if not all of the IoT users admitted to not reading IoT privacy policies, while they mistrusted IoT provider’s claims that a large part of their information would be kept anonymous with their identities kept separate.
3.1.4 Perceptions of lawlessness

For the most part, IoT users did not comment on legal aspects related to data privacy, e.g. existing legal proscriptions on misleading or deceptive conduct, unfair contract terms in the Australian Consumer Law and the relatively low level of privacy protection standards in the Australian Privacy Act (1988). However, users seemed to want to have some minimal protection levels from a legal perspective even just in the form of a ‘legal warranty’ of anonymity as one user indicated:

Maybe having a legal warranty or some sort of approach that might give [IoT users] security that the information being captured is not going to be linked back to [IoT users] (D1).

There was also uncertainty as to what effective legal measures could be taken in the event of a data privacy breach, as one user put it succinctly:

And if there is a breach in your privacy, in your personal data, then which jurisdiction or how do you actually pursue a legal claim? Because its not a matter of whether or not the law exists, but how do you actually [know] which law is breached and how do you apply or enforce that breach of law (U1).

Another user expressed also some ignorance about legal aspects stating that ‘I'm not aware what legal implications are’ and later, as the discussion unfolded, admitted:

‘I think [it] is a very big issue [the legal protection of data] but I’m relying on other people to be concerned of it on my behalf. And what would get me to take action about it would require awareness raising by those people [responsible for] raising alarm bells and say something’ (U11).
3.2 IoT designer/developer concerns about data privacy

3.2.1 Uncertainty around legal perspectives and IoT data protection

One designer/developer indicated uncertainty surrounding data privacy from a legal perspective by saying ‘It’s very hard to put your finger on what [the laws on data privacy] exactly means’ (U14), while another designer/developer indicated ‘I don’t think my [personal data] is protected from a legal perspective’ (D12).

3.2.2 Legal responsibility related to privacy

One designer/developer felt strongly that the responsibility for data privacy was not to be handled by designers/developers at a technical level, but an aspect to be dealt with by others, as in his case the owners of the IT artefacts being developed:

‘I’m not the adjudicator of good or bad science, or good or bad security. I’m the tech guy and my job is to implement the IT systems that reflect the needs of users and at some points in time their needs has to be balanced with societal needs and the legal framework’ (D3).

He continued stating that there is a gap in policies and legal frameworks that guide the work of designers/developers:

‘The problem right now is we’ve gone too far, far further on the tech side than anything else, what policies apply? I have data from [other countries], tons and tons of different places. What’s the ethics that applies on the access and use of that data, when the data is actually hosted in Australia? People are very unsure what to apply and where… does the privacy legislation in Victoria apply? And I guess there is not one solution, each one has their own particular nuances of trust’ (D3).

3.2.3 An apparent lack of legal regulation

A few designers/developers interviewed revealed they felt there was a lack of legal regulation, with one interviewee complaining that young IT developers, whom he called ‘cowboys’, were more focused on innovation than data privacy with respect to the design of IoT artefacts. He based his argument on entrepreneurial strategies aimed at quick innovation and pushing new products and services to the market rather than considering policies and regulatory aspects related to the design of IoT artefacts:

‘In terms of innovation, the legal framework is always a lagging indicator into what innovation offers. The joke I heard recently was ‘in your life you will be entitled to 15 minutes [of] privacy’. Well it’s essentially a revelation of the world we live in now’ (D4).

Once you add in the digital [IoT] medium its again a matter of some paranoia or personal suspicion. I’ve seen in so many cases law lags technically. I would imagine the current legal framework is not fully up to the digital world just yet (D4).
4  Data privacy in a world of IoT

Our study revealed two key aspects related to privacy and data protection (or data privacy as we have termed it) in a new connected world enabled by the IoT.

**Privacy is important to individuals**

Privacy as a principle is still important for individuals and is particularly surprisingly so in a world of increased social media use. Information most interviewees considered sensitive, such as intimate health information, should be treated as private i.e. kept inaccessible so far as feasible. More generally, when it comes to data privacy, individuals wish to exercise more control on what they share and with whom. In particular, individuals wish to exercise more control over the collection and storage of their sensitive data/information and would value more transparency by external entities who collect and use their data. In particular they wish to be informed how their collected data is used and protected. In particular multiple use-scenarios of their data need to be relayed back to them so that they are aware of the actual use of their data, particularly in instances where collected data is integrated and used for purposes other than initially planned or signed up for. Users want absolute assurance that they cannot be identified and that their data is actually stored securely taking into consideration individual protection requirements.

**Forms of consent can be improved**

Almost all interviewees expressed frustration and impatience with the sign-up and consent procedures to agree to IoT services and data collection (in cases where this was required). Consent procedures were overall perceived to be out of touch with modern IT users, and interviewees felt that forms and mechanisms to consent needed revamping to fit today’s modern online user society. Suggestions were made to have multiple points of consent with the ability to revoke earlier forms of consent or opt out if necessary along the data use life-cycle. In addition, users admitted that they did not read lengthy consent forms and felt that from a legal perspective, consent forms were unclear, creating uncertainty about what one signs up for. Hence, there are multiple opportunities to provide IoT users with more meaningful notice and consent opportunities that relate to the collection, storage and use of their IoT data, without restricting designer/development innovation.

We have found the above comments about consent to be among the most interesting and useful outcomes from our research. In April this year (2017), we followed up with in-depth focus group meetings where we spent longer discussing problems of consent and ways these might be addressed with some of our interviewees and a selection of other IoT users and developer/designers. In the next stage of our work we will be developing ideas for designing technologies that can be programmed to deliver timely warnings in order to address the significant consent deficit in the current system.
References

