Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective

Xavier Caron [a], *Rachelle Bosua* [b,*], *Sean B. Maynard* [b], *Atif Ahmad* [b]

[a] *Price Waterhouse Coopers, Australia*

[b] *Computing and Information Systems, The University of Melbourne, Melbourne, Vic., Australia*

Keywords:
Australian Privacy Principles (APPs)
Authentication
Hacking risk
Individual privacy
Internet of Things
Privacy legislation
Security
Surveillance and ubiquity

ABSTRACT

The *Internet of Things (IoT)* heralds a new era of computing whereby every imaginable object is equipped with, or connected to a smart device allowing data collection and communication through the Internet. The IoT challenges individual privacy in terms of the *collection and use* of individuals' personal data. This study assesses the extent to which the *Australian Privacy Principles* protect individual privacy associated with data collection through the IoT. A systematic literature review identified four key privacy themes that represent issues related to the collection of individuals' data through the IoT: *unauthorised surveillance*, *uncontrolled data generation and use*, *inadequate authentication* and *information security risks*. These four themes are used to critically analyse the Australian Privacy Principle's (APPs) protection of individual data. Findings indicate that (1) the APPs do not adequately protect individual privacy of data collected through the IoT, and (2) future privacy legislation must consider the implications of *global reach* of IoT services, and *ubiquity* and *security* of IoT data collection with respect to individual privacy.

The Internet of Things (IoT), one of the fastest growing trends in computing according to Gartner (2014a), is expected to have a $14 billion economic impact by 2022 (Mahidhar and Schatsky, 2013). The IoT allows ubiquitous, unbounded connectivity of different types of devices at any time, within any place (Vermesan et al., 2011). This vision is made possible via the extensive use of sensors – objects embedded in devices that have the ability to link the digital world with the real world (Atzori et al., 2010). Examples include the collection and integration of data from one or more sources such as: patient vital signs including heart rate and body temperature, individual patterns of movement through global positioning in cities, home sensors that track power and electricity consumption, and devices that track vehicle routes and driver behaviour. As more data from different sources are collected using these devices, the IoT may have significant impact on individuals' privacy with the additional potential for widespread 'surveillance' of individuals without their knowledge or consent (Oriwoh et al., 2013).

Gibbs (2008) defines privacy as the "limitation of others' access to an individual" and mentions that this limitation is based on three elements: *secrecy* (the control of information), *anonymity* (acting without attention from others) and *solitude* (limiting physical access to an individual). In addition, Gibbs (2008) mentions the importance of balancing personal privacy needs against other individual rights and against collective social good. More specifically, *individual privacy* involves what information individuals should (1) be required to divulge about themselves to others, and (2) keep strictly to themselves (Mason,

* *Corresponding author.* Computing and Information Systems, The University of Melbourne, Melbourne, VIC, 3010, Australia. Tel.: +61 3 8344 1398.
E-mail address: rachelle.bosua@unimelb.edu.au (R. Bosua).

http://dx.doi.org/10.1016/j.clsr.2015.12.001

1986; Strickland and Hunt, 2005; Westin, 1968). Considering the increased digitisation of personal information and networking of technologies through the IoT, there is a growing concern that individuals may be unaware of legal consequences related to data collection through the IoT. More specifically, there are often unclear guidelines with respect to how and where individuals' collected data are stored, and ultimately used by those collecting or trading the data.

From an information privacy perspective, the IoT involves multiple stakeholders: individuals (the subject of data collection), organisations (who are responsible for processing individuals' collected data) and third parties (e.g. users who benefit from or use the collected or processed data). The IoT promises multiple benefits to all these stakeholders. For individuals, providing value such as health and wellbeing benefits. For organisations and third parties, providing information to deliver improved services to individuals and the society at large. However, considering the growing trend to gather increasingly more individual and personalised data, IoT data collection, handling and processing practices arguably raise many questions regarding the impact on an individual's privacy from a legal perspective.

Weber (2009) indicates that the purpose of the IoT is to facilitate information exchange about 'things' in a secure and reliable manner. 'Secure' and 'reliable' in this context are key concerns that impact on individual data protection, particularly when considering aspects such as unintentional and ethical use of collected IoT data, and the role of third party users. In March 2014, Australia announced an updated set of 13 privacy principles that govern the handling of personal information (Office of the Australian Information Commissioner, 2014a). Although these principles are supposed to broadly protect individual privacy, they were originally developed for a narrow purpose. Hence, the Australian Privacy Principles (APPs) do not address individual privacy in the context of the IoT. Therefore the research question posed by this research is: *To what extent does the Australian Privacy Principles protect an Australian individual's privacy with respect to data collected via the Internet of Things?*

In answering this question, this paper does not offer a legal analysis, but verifies whether the current Australian Privacy Principles (APPs) effectively protects an individual's privacy from an IoT perspective. A two-phase research approach was followed, motivated by the concern that the IoT may give service providers the ability to gather a large amount of data about individuals, without individuals knowing how these data are used in terms of privacy and legislation. The first phase of this research consisted of a systematic literature review to identify key privacy themes or issues deemed important from an individual privacy perspective. The second phase critically analysed the extent to which the 13 APPs address each of the individual privacy issues identified in phase one.

This paper is structured as follows. Section 1 provides background literature on the *Internet of Things* and *Information Privacy*, followed by an introduction of the 13 APPs. Section 2 describes the research methodology followed. Section 3 highlights key privacy themes that emerged as a result of the literature review phase of the research methodology. Section 4 describes results from a critical comparison of the privacy themes with the 13 APPs, with a conclusion in Section 5 that highlights limitations, aspects of the APPs that can be improved, and avenues for future research.

1. Background literature

1.1. *The Internet of Things*

The Internet of Things (IoT) represents one of the most significant disruptive technologies of this century, consisting of an emerging global Internet-based technical architecture (Gubbi et al., 2013; Weber, 2010). Described by Atzori et al. (2010) as a *novel technology that is rapidly gaining ground*, the major enabling element of the IoT is the integration of several collaborative and communication technologies allowing for comprehensive data collection. Examples include tracking and identification technologies that are integrated through wired and wireless actuator and sensor networks, allowing enhanced communication protocols between distributed, intelligent smart sensor objects in the form of wearables or smart objects embedded in the environment, devices or even humans (Atzori et al., 2010; Berinato, 2014). More formally the IoT is defined as "*. . .the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment*" (Gartner, 2014b).

The IoT allows organisations and third parties to collect and analyse data about the environment and individuals' attributes offering new personalised and reality-augmented services that involve little human or no interaction (Vermesan et al., 2011). A typical example from the healthcare industry includes the collection of, monitoring and transmission of patient medical and wellbeing data to a central cloud-based system. Subject to processing, illuminating insights into the patterns and conditions associated with an individual's health can emerge as medical professionals interact with and access these data. Another example includes the collection of and integration of different domestic data sets to predict utility usage patterns of individual households, or include predictions for households to the extent of indicating the degree of human intervention when necessary (e.g. automatic turning off of a household's water system in the event of hazardous leaks).

IoT technology consists of a web of interacting sensors that can detect and measure changes in variables such as positioning, temperature, light and movement, even to the level of reporting on the status of individuals or objects. In some cases sensors can interact with the environment (Bauer et al., 2014). Expectations are that the IoT may have a significant impact on the everyday-life of individuals, users and the society at large from service-related industries to the detection of dangerous conditions, the retail industry and the tracking of an entire supply chain (Bauer et al., 2014). The US National Intelligence Council includes the IoT in the list of six 'Disruptive Civil Predictions' which indicates that by 2025, the IoT may form an integral part of everyday things such as household furniture, food packaging, clothing and paper documents. Table 1 summarises potential areas of application that may benefit from