Chapter 62
Big Data and the Internet of Things:
Current Industry Practices and Their Implications for Consumer Privacy and Privacy Literacy

Zablon Pingo
University of Technology Sydney, Australia

Bhuva Narayan
https://orcid.org/0000-0001-8852-5589
University of Technology Sydney, Australia

ABSTRACT

The privacy construct is an important aspect of internet of things (IoT) technologies as it is projected that over 20 billion IoT devices will be in use by 2022. Among other things, IoT produces big data and many industries are leveraging this data for predictive analytics to aid decision making in health, education, business, and other areas. Despite benefits in some areas, privacy issues have persisted in relation to the use of the data produced by many consumer products. The practices surrounding IoT and Big Data by service providers and third parties are associated with a negative impact to individuals. To protect consumers' privacy, a wide range of approaches to informational privacy protections exist. However, individuals are increasingly required to actively respond to control and manage their informational privacy rather than rely on any protection mechanisms. This chapter highlights privacy issues across consumers' use of IoT and identifies existing responses to enhance privacy awareness as a way of enabling IoT users to protect their privacy.

DOI: 10.4018/978-1-7998-8954-0.ch062

INTRODUCTION

Current information technology innovations such as the Internet of Things (IoT) is generating a huge amount of data popularly referred to as Big Data, which have significantly disrupted decision making in various sectors including health, manufacturing, education, agriculture, energy, retail, insurance, automotive and crime detection (Dutton, 2013; Federal Trade Commission, 2015; Richardson et al., 2017a). The IoT have increasingly become prevalent amongst consumers, promising to benefit our lives in many positive ways (Richardson et al., 2017). While the conversation around Big Data and IoT centers on the benefits, privacy and security vulnerabilities have also risen to the surface. When organizations such as service providers and data brokers collect personal information from multiple sources such including IoT devices and integrate them to create Big Data, as is often the practice under some business models (Rappa, 2003), it poses an imminent privacy and security risk to consumers. To address these privacy and security issues, several researchers have proposed technical and legal approaches, but there are limited accounts of how users of IoT respond to these privacy concerns, and about their privacy literacy. Privacy awareness is defined as individuals "cognitive ability to identify" and respond to privacy concerns in specific environments or information technology artifacts (Omoronyia, 2016). Awareness as part of literacy, thus privacy literacy is conceptualized as one's level of understanding and awareness of how information is tracked and used in online environments and how that information can retain or lose its private nature (Givens, 2015).

This chapter provides an account of how users/consumers, service providers, and regulators/policy makers need to be aware of in light of these data practices and privacy concerns. This is important as the Internet industry has a growing interest in generating value out of the Big Data both for social good and for commercial purposes. To safeguard users' privacy and personal data, various legal and structural frameworks have been proposed or put in place across many countries. However, the increased innovations of IoT and the leveraging of Big Data has opened up new challenges. These challenges also raise the question of the need to balance between regulation to protect the information privacy of users and maintaining flexibility for economic value. Thus, the data practices attract both opportunities and potential risks, particularly in how the information is collected, processed and used by the data controllers. Scholars note the challenges arise from linking users' personal information, lack of transparency, possible misuse of the data among others practices that pose risks or harm to data subjects (Crawford & Schultz, 2014; Dutton, 2013; Federal Trade Commission, 2015; Haynes & Robinson, 2015).

Increased innovation and popularity of lifelogging technologies categorized as a subset of the Internet of Things has attracted a lot of attention in research and business (Federal Trade Commission, 2015). The IoT devices have the ability to collect, process and communicate to other devices and humans. The IoT makes users both subjects and recipients of the data (Tuninetti Ferrari, 2017). Privacy is an important area for users' of IoT, for they need to be protected and have necessary awareness on how personal data collected is used by other parties, given the complexity of data sharing, business models and privacy in the technologies (boyd & Hargittai, 2010; Park, 2013; Rappa, 2003; Solove & Schwartz, 2014; Torre, Sanchez, Koceva, & Adorni, 2017). As the IoT become common and pervasive, there is a need for people to enhance their ability to evaluate the privacy/security associated with particular data practices (Zhou & Piramuthu, 2014).

Since privacy is a socially and economically negotiated concept that can be contextual, it is important for service providers to ensure an enabling environment for such negotiation to happen. Various stakeholders such as technology designers, device manufacturers, service providers, educators, privacy

Related Content