Internet Privacy

4

Nathan John Rodriguez
Weber State University, USA

INTRODUCTION

Technological innovations have fundamentally altered communication patterns during the past three decades. Smartphones have become widely adopted in recent years, and offer the allure of convenient access to news content, entertainment, retailers, weather information, and other people. In a practical sense, users sacrifice information regarding their online activity in exchange for content that is deemed relevant to their interests. There have been slightly different iterations of the axiom, "If the service is free, you are the product" over the past few decades, as it has come to signify the dangers of popular online platforms collecting consumer data (Oremus, 2018).

This entry examines internet privacy through four complementary, overlapping perspectives. It is argued that the most significant threats to internet privacy come through user activity, corporate data collection, governmental surveillance, and malevolent actors. To be sure, these are not discrete categories, but are frequently interrelated. For example, consumers frequently submit private information to corporate entities in exchange for access to online content. Before delving into further explanations and examples of these perspectives, it is necessary to begin with a discussion of what is meant by the notion of privacy and internet privacy.

BACKGROUND

Privacy Theories

One of the earliest definitions of privacy is "the right to be let alone" (Warren & Brandeis, 1890). The notion of privacy encompasses territorial privacy, personal privacy and informational privacy (Rosenberg, 1992). There are a variety of potential dimensions to informational privacy, but a broader definition of these concerns has been characterized as the unauthorized use of personal information. (Smith, Milberg, & Burke, 1996).

Online privacy studies have focused on the motivation for privacy protection as well as the behavior related to privacy protection. Internet privacy research frequently relies upon protection motivation theory (PMT), which posits that individuals engage in a rational thought process, and protect themselves based on the perceived severity of a negative outcome, the probability of that event occurring, and the efficacy of a potential solution (Rogers, 1975). PMT has undergone several iterations in recent years, and an extended parallel process model (EPPM) emerged to address these deficiencies by explaining why—even in the face of a high-perceived threat—a user may not change their behavior. Recent studies have shown that internet users "tend to ignore privacy risks until they encounter monetary loss online in person" (Chen, Beaudoin, & Hong, 2017, p. 300).

DOI: 10.4018/978-1-5225-9715-5.ch049

The Privacy Paradox describes the incongruent way in which users frequently express a theoretical interest in protecting their privacy, yet do not engage in behaviors that would protect their privacy (Norberg, Horne, & Horne, 2007; Brown, 2001). A thorough review of Privacy Paradox literature concluded that decision-making regarding privacy may be a rational calculation of risk and reward, a biased and irrational risk assessment, or a situation that involves virtually no calculation (Barth & de Jong, 2017). The authors concluded that decision-making tends to occur more frequently on an irrational rather than a rational level, as individuals tend to follow their intuition with little regard to privacy risks.

Attitudes Regarding Online Privacy

Sharing personal information online has become routine and more embedded in everyday social interactions (Zafeiropoulou, Millard, Webber & O'Hara, 2013). Privacy concerns were perhaps more prominent in the early days of the internet, but a rising percentage of people today are less concerned about potential risks due to "a growing internet population, constantly changing areas of use, and increasing security awareness" compared to earlier in the 21st century (Bergstrom, 2015, p. 425). Some internet users are fully aware of the risks they face online, and willingly accept those risks for access to certain services, thus engaging in a cost-benefit analysis (Park, Campbell, & Kwak, 2012; Preibusch, 2013). Consumers have been shown to willingly forego certain online privacy protections to access more customized content (Martin & Murphy, 2017; Sundar, Kang, Wu, Go & Zhang, 2013). It is quite possible that many users experience what Choi, Park, and Jung refer to as "privacy fatigue," an umbrella term for concepts ranging from security fatigue (Furnell & Thompson, 2009), to consent fatigue (Schermer, Custers, & van der Hof, 2014), and breach fatigue (Kwon & Johnson, 2015), in which users experience a "psychological state of tiredness with the issue of online privacy" (2018, p. 43).

It has been shown that people with a more sophisticated apprehension of the internet, who are better able to perceive privacy threats, are no better off than laypersons with respect to acting to secure their privacy online (Kang, Dabbish, Fruchter, & Kiesler, 2015). An over-reliance upon self-reporting studies could account for part of the discrepancy as there is a demonstrated tendency for internet users to be overly confident in their own competence. Jensen, Potts, and Jensen (2005) asked participants if they were familiar with technological solutions to enhance their privacy, and less than 25 percent of participants who answered in the affirmative were able to answer basic follow-up questions about the technology.

Concerns related to online privacy develop from personal experience, and include discussions with friends and family and hearing reports about data breaches through media channels that resulted in financial losses (Brandimarte et al., 2013, Bryce and Fraser, 2014). Simply put, many people may have become inured to the notion of their personal data being exposed online, and may appreciate those risks only after a negative experience. In 2016, there were more than 4,000 data breaches that affected more than 4.2 billion records (Risk-Based Security, 2017). These data breaches, in turn, often result in user information being sold on the dark web (Ablon, Libicki & Golay, 2014).

In the past few years, consumers have become more knowledgeable about the ways in which their data is being used (Morey, Forbath & Schoop, 2015). It has been argued that 2018 is the year in which consumers grew more informed and cynical about the ways in which their personal data is used (Ng, 2018), as a recent poll indicates a majority of Americans reported changing their privacy settings in the past 12 months (Perrin, 2018).