Chapter 83
Creepy Technologies and the Privacy Issues of Invasive Technologies

Rochell R. McWhorter
https://orcid.org/0000-0003-2053-1610
The University of Texas at Tyler, USA

Elisabeth E. Bennett
Northeastern University, USA

ABSTRACT

Technology has become increasingly invasive and corporate networks are expanding into public and private spaces to collect unprecedented data and provide new services such as artificial intelligence and through unsettling human-like personas. The term "creepy technology" is appearing in the literature along with concerns for privacy, ethical boundaries, cybersecurity, and mistaken identity but is also in news articles to inform the public about technology advances that affect consumer privacy. Invasive technology provides the impetus for external adaptation for many organizations and current trends require rapid adaption to potential threats to security. Also, usability addresses how users respond and adapt to new technology. This chapter includes the presentation of an exploratory study of how the public responded to various technology announcements (N=689 responses) and results indicated a significant response to invasive technologies and some sense of freedom to opine. This chapter also provides discussion of interventions that are critical to both public and private sectors.

INTRODUCTION

Technology is a very powerful tool that serves the interests of consumers, useful for gathering information for marketing and product development; and, increasingly used to feed prediction models and public control systems. However, as such technologies have become increasingly complex (Bennett, 2014; McWhorter, 2014a), they have also become much more invasive (Madsen, 2019; Murnane, 2017;

DOI: 10.4018/978-1-7998-8954-0.ch083

Tene & Polontesky, 2013). Due to this invasiveness, the term "creepy technology" has been appearing in the literature along with a host of concerns including privacy, ethical boundaries, cybersecurity, and mistaken identity errors (Anslow, 2007; Britt, 2015; Cumbley & Church, 2013; Johnson, 2017; Pham, 2019; Tene & Polontsky, 2013; Zhang, 2018). This chapter examines creepy technology as a new and disrupting force in the world.

For the purposes of this work, the authors of this chapter define creepy technology as: *technology that evokes a feeling or belief that individual privacy may be invaded in an unethical or discomforting manner*. The objectives of this chapter are four-fold to: (1) offer a review of relevant existing literature in this area of study for the chapter; (2) present an exploratory study regarding public responses to technology announcements; (3) present an emerging conceptual frame for processing creepy technologies; and, (4) provide a discussion on interventions for perceived invasive technologies that should be considered by both individuals and organizations. Each of these objectives are addressed in the following sections. Also, suggested additional readings and key terms and definitions will conclude the chapter.

BACKGROUND

Examples of creepy technology found in the literature are numerous (Martin, 2019; Purshouse, & Campbell, 2019; Vladimir, 2018; Wilkins, 2018). For instance, research about creepy technology includes studies at institutions of higher education that use facial recognition technology (FRT) to monitor students (see Cole, 2019; Cuador, 2017; Lieberman, 2018; Reidenberg, 2014) as well as examining trends into invasive technology (Aratani, 2019; Brown, 2019; Symanovich, 2018). Also, Wang and Kosinski's (2018) controversial research attempted to predict sexual orientation by analyzing digital pictures and the researchers remarked that "given that companies and governments are increasingly using computer vision algorithms to detect people's intimate traits, our findings expose a threat to the privacy and safety of gay men and women" (p. 246). Thus, such predictions could be harmful to people if they are identified or misidentified and subjected to discrimination, as well as discomfort about something so personal.

In addition to FRT, another type of technology that is causing concern is location sharing applications (LSAs) utilized on mobile devices (Moreau, 2019; Valentino-DeVries, Singer, Keller, & Krolk, 2018). Examples of these LSAs are Snapchat (Snapchat.com), Swarm (Swarmapp.com), Glympse (Glympse.com), and Life360 (Life360.com) that allow the user to share their location with family members and friends in real-time (Moreau, 2019). Stern (2019) noted that although these LSAs offer the benefit of peace of mind by allowing the user to keep track of friends and family members and the ability to share information with 911 call centers in cases of emergency (Magid, 2018), they also possess the creepy factor. The downside of location sharing in real-time are privacy concerns such as family members spying on the user (Navarro, 2018); or worse, when sensitive data is stolen by a third-party vendor or hackers (Boyd, 2019). For instance, it was revealed to consumers in 2018 that real-time customer location information was marketed by cell phone carriers to data brokers who in turn "sold that information to law enforcement and others, without necessarily going through time consuming formalities such as court orders" (Magid, 2018, para. 2). The hacking of real-time information was quite concerning to thousands of mobile device users who had their private information harvested. Such personal information included not only location data, but hashed passwords and logins, private Facebook messages, personal images and also confidential audio recordings that were stolen from their mobile device (Franceschi-Bicchierai, 2018, 2019).