Chapter 4
Invasive and Creepy Technologies:
Challenges and Opportunities

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

Mandi M. Laurie
https://orcid.org/0000-0001-8910-5527
The University of Texas at Tyler, USA

ABSTRACT

As modern technologies have increased in sophistication and invasiveness, users have expressed concerns about confidentiality and ethical issues regarding contemporary technologies such as artificial intelligence, facial recognition, social robots, big data, and location-sharing apps. As a result, the term "creepy technologies" has been used to describe these concerns. This chapter seeks to review relevant literature for this area of study and offer interventions for individual users, teams, and organizations.

INTRODUCTION

Contemporary technologies are becoming progressively sophisticated (McWhorter, 2023) and increasingly invasive (Kelley et al., 2023; Tene & Polontesky, 2013). Due to this invasiveness, the term "creepy technology" has emerged in the literature along with concerns such as cybersecurity, confidentiality, and ethical concerns, among others (Mou & Meng, 2024; Phinnemore et al., 2023; Sharma, 2023). For this chapter, creepy technology is defined as "*technology that evokes feeling or belief that privacy may be invaded in an unethical or discomforting manner"* (McWhorter & Bennett, 2021, p. 243). This area of study can inform business professionals and stakeholders concerning the perceptions of technology by various stakeholders and likely encourage organizations to examine their technology policies.

The objectives of this chapter are two-fold to: (1) offer a review of relevant existing literature in this area of study and, (2) provide a discussion on interventions for perceived invasive technologies that should be considered by both individuals and organizations. Both objectives will be presented in

the following sections. Also, additional readings will be suggested, and key terms and definitions will conclude the chapter.

BACKGROUND

Examples of creepy technology found in the literature are numerous and are enabled by the Internet of Things (IoT). Creepy technologies include *location sharing applications* (Moreau, 2019; Phinnemore et al., 2023), *facial recognition technology* (Cuador, 2017; Reidenberg, 2014; Seberger et al., 2024; Symanovich, 2018), *always-listening voice assistants* (Ford & Palmer, 2019; Mou & Meng, 2024; Phinnemore et al., 2023), *social media* (McWhorter et al., in-press). Also found were the *convergence of big data* (Marr, 2016), the *Internet of Things* (IoT; Bennett & McWhorter, 2014; O'Hagan et al., 2023), *artificial intelligence* (AI) (Kaplan, 2016; Kjeldgaard-Christiansen, 2024; Larrey, 2017; McCarthy et al., 1955; McWhorter, 2023; Sulleyman, 2017) and *social robots* (Fitter et al., 2021; McWhorter & Bennett, 2021; Reig et al., 2021), including *AI robots* (Baldwin, 2019; Ischen et al., 2020; Mou & Meng, 2024), among others. These technologies have the capacity to evoke discomfort and human questioning about the ethical use of personal data.

INTERNET OF THINGS

The *Internet of Things* (IoT; Evans, 2011) is a term used to demonstrate the connectedness of smart devices that link the world together (Bennett & McWhorter, 2014) and Marr (2016) predicted that the term IoT would be utilized less by users as it moves into the "hype phase and quickly becomes part of everyday life" (para. 1). McWhorter and Bennett (2020) described IoT as "a phenomenon of a growing number of connected devices, and Internet-enabled services [whereby] billions of devices are now connected to one another" (p. 166) and IoT enables the sophisticated technologies that some may characterize as *creepy technology*. For example, Saliesh (2019) described a subset IoT as the "Internet of Bodies" (IoB) remarking that as the "IoT enter[s] the human body…human bodies are now connected to a network, with the potential to be remotely controlled and monitored" (para. 1). Andrea Matwyshyn, Northeastern University law professor, noted the IoB has both legal as well as policy implications when the human body is used as a technology platform (Matwyshyn, 2019). Another concerning example of the IoB is former Vice-President Dick Cheney's heart implant's wireless sensors that were intentionally inactivated due to the threat of potential hackers that proved to be a viable threat (ABC News, 2013). In 2017, roughly a half-million pacemakers were recalled due to security concerns and the devices were given a required firmware update (Garun, 2017).

SOCIAL MEDIA

Social media is very pervasive in the modern culture and is quite useful for social networking and building community, facilitating meetings in real-time, exploring new interest areas, and access to expert content, and training (McWhorter, et al., in-press). However, many users often over-share their personal information online (Shabahang et al., 2024) and organizations are reaping the financial benefits of targeted

23 more pages are available in the full version of this document, which may
be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/invasive-and-creepy-technologies/350689

Related Content

The Cloud in Education: Policy, Leadership, and Management Issues
Karl Donert (2018). *Handbook of Research on Educational Design and Cloud Computing in Modern Classroom Settings (pp. 239-261).*
www.irma-international.org/chapter/the-cloud-in-education/195275

Leveraging Educational Technology to Meet the Needs of 21st Century Learners
Gregory R. McWhorter (2021). *Handbook of Research on Barriers for Teaching 21st-Century Competencies and the Impact of Digitalization (pp. 215-233).*
www.irma-international.org/chapter/leveraging-educational-technology-to-meet-the-needs-of-21st-century-learners/280723

A Systematic Review of the Impact of ChatGPT on Higher Education
Siyi You (2024). *International Journal of Technology-Enhanced Education (pp. 1-14).*
www.irma-international.org/article/a-systematic-review-of-the-impact-of-chatgpt-on-higher-education/343528

Educational Innovation Applied to Literacy Formative Processes by Use of Artificial Intelligence
Margarita Isabel Asensio-Pastorand Juana Celia Domínguez-Oller (2025). *Transformations in Digital Learning and Educational Technologies (pp. 275-292).*
www.irma-international.org/chapter/educational-innovation-applied-to-literacy-formative-processes-by-use-of-artificial-intelligence/374819

Edu-ACoCM: Automatic Co-existing Concept Mining from Educational Content
Maitri Maulik Jhaveriand Jyoti Pareek (2019). *International Journal of Technology-Enabled Student Support Services (pp. 16-40).*
www.irma-international.org/article/edu-acocm/236072