

# Chapter 33

## Wearable Devices: Ethical Challenges and Solutions

**Marc L. Resnick**  
Bentley University, USA

**Alina M. Chircu**  
Bentley University, USA

### ABSTRACT

*Today, innovation in and with Information and Communication Technology (ICT) is accelerating as consumers, companies and governments become users and designers of myriad ICT solutions whose ethical implications are not yet well understood. This chapter contributes to the growing body of research on ethical implications of one popular emerging ICT - wearable devices and associated technologies. Ethical challenges stemming from the extensive prevalence and comprehensiveness of wearable devices are related not only to the device design and use but also to the device-supported data collection and analysis and the creation of derivative products and services. Drawing from theories of ICT ethics, this chapter identifies the major ethical challenges posed by wearable devices and provides several guidelines on how these challenges can be addressed through ethically-informed design interventions.*

### INTRODUCTION

Today, innovation in and with information and communication technology (ICT) is accelerating as consumers, companies and governments become users and designers of myriad ICT solutions whose ethical implications are not yet well understood. While ICT ethicists posit that technology should be used to protect and advance core human values (life, health, happiness, security, resources, opportunities and knowledge) (Bynum, 2011), new ICTs often fail to do so. This chapter discusses wearable devices and associated technologies as one example of such ICT innovation, analyzes the ethical issues they present for individuals, organizations and societies, and proposes solutions for future designs that can help minimize the negative – intended or unintended – consequences of wearable technologies.

DOI: 10.4018/978-1-5225-8897-9.ch033

A wearable device is any ICT device which can be worn or carried by a user, and which has embedded sensors (to collect information about the user's activities), software (to enable processing of the information), and network connectivity (to enable remote data storage, synchronization, and exchange, as well as additional processing capabilities). Wearable devices include mobile phones and smartphones, activity trackers, wearable GPS trackers, smart watches, smart glasses, and sensor-enhanced objects such as passports with radio-frequency identification (RFID) chips and RFID luggage tags. Wearable devices are part of the emerging Internet of Things (IoT) – interconnected objects, devices, vehicles, and buildings that can exchange information and be controlled remotely, over the Internet. We are only starting to scratch the surface of possible developments in this area, as IoT is expected to include tens of billions of devices in a few short years.

Many companies are viewing wearables as the next growth opportunity, which will generate over \$231 billion in service revenue by 2020 (PRNewswire, 2015). Expected benefits from wearables include improved efficiency, productivity, service and engagement across a range of industries such as retail, healthcare and entertainment (PwC, 2014). According to IDC, the number of wearable units worldwide exceeded 45 million in 2015, and is expected to exceed 126 million by 2019 (Llamas, 2015). If we consider only one subset of wearables – those devoted to health self-monitoring – the number of unique commercial offerings is staggering, with over 200 wearable health sensors and almost 100,000 health applications available for purchase (or free download in many instances) (Patterson, 2013).

As the number of wearable devices and device interconnections increases, so do the associated security vulnerabilities (Goodman, 2015) and privacy threats. To analyze these challenges, this chapter draws from theories focused on the social and ethical impacts of ICT. According to a 2012 bibliometric mapping analysis, ICT ethics, also called computer and information ethics, is a relatively new but rapidly evolving field, mimicking the rapid pace of technological development over the last few decades. Technologies such as the Internet and the many Internet-enabled applications such as email, online gaming, blogs, social networking sites, and others have been extensively examined by ICT ethics researchers, especially as they relate to privacy concerns, regulations and laws, and social impacts (Heersmink et al., 2012). However, the research on ethical implications of wearable devices and associated technologies is in its infancy.

Academic researchers, industry practitioners and users alike do not yet fully understand all the emerging ethical issues posed by these emerging technologies (Chircu, 2013; Resnick, 2013). For example, privacy concerns are raised as real-time tracking and location services technologies are developed. Wearable devices such as Google Glass, a technology that allowed users, among others, to record others using head-mounted glasses, create not just privacy issues, but can lead to knowledge and opportunity disparities between adopters and non-adopters, and provide misleading information that misinterprets the context of action (Michael, 2014, 2015). We posit that these emerging ICTs are fundamentally changing the equilibriums that Western society had reached in the privacy versus safety tradeoff, and the privacy versus service tradeoff. For example, in some Western countries, the privacy versus safety equilibrium was based on the idea that law enforcement should balance individual privacy rights with the need for public safety, and obtain specific approvals for surveillance and searches needed in criminal or national security investigations. Advances in technology now create new surveillance opportunities on an unprecedented scale (Michael, 2014, 2015; Martin, 2016), which disrupt this equilibrium. Inexpensive GPS transmitters can be attached to a wide population of potential suspects' vehicles and tracked through a central database. Public cameras or unmanned aerial vehicles can be programmed with recognition

17 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/wearable-devices/228751](http://www.igi-global.com/chapter/wearable-devices/228751)

## Related Content

---

### Wearable Devices: Ethical Challenges and Solutions

Marc L. Resnick and Alina M. Chircu (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 694-712).

[www.irma-international.org/chapter/wearable-devices/228751](http://www.irma-international.org/chapter/wearable-devices/228751)

### Insider Attack Analysis in Building Effective Cyber Security for an Organization

Sunita Vikrant Dhavale (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1408-1425).

[www.irma-international.org/chapter/insider-attack-analysis-in-building-effective-cyber-security-for-an-organization/228790](http://www.irma-international.org/chapter/insider-attack-analysis-in-building-effective-cyber-security-for-an-organization/228790)

### Ethical Considerations in the Educational Use of Generative AI Technologies

Burak Tomak and Aye Yilmaz Virlan (2024). *Exploring the Ethical Implications of Generative AI* (pp. 49-62).

[www.irma-international.org/chapter/ethical-considerations-in-the-educational-use-of-generative-ai-technologies/343698](http://www.irma-international.org/chapter/ethical-considerations-in-the-educational-use-of-generative-ai-technologies/343698)

### Ethical Dimensions of the Increasing Usage of New Technologies in Virtual Education

John Nnaji (2019). *Emerging Trends in Cyber Ethics and Education* (pp. 1-21).

[www.irma-international.org/chapter/ethical-dimensions-of-the-increasing-usage-of-new-technologies-in-virtual-education/207659](http://www.irma-international.org/chapter/ethical-dimensions-of-the-increasing-usage-of-new-technologies-in-virtual-education/207659)

### Ethical and Privacy Implications of the Use of Social Media During the Eyjafjallajökull Eruption Crisis

Hayley Watson and Rachel L. Finn (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 764-777).

[www.irma-international.org/chapter/ethical-and-privacy-implications-of-the-use-of-social-media-during-the-eyjafjallajokull-eruption-crisis/228754](http://www.irma-international.org/chapter/ethical-and-privacy-implications-of-the-use-of-social-media-during-the-eyjafjallajokull-eruption-crisis/228754)