Chapter 9
Wearable Devices and Privacy Concerns: Data Collection, Analysis, and Interpretation

Ersin Dincelli
University of Colorado Denver, USA

Xin Zhou
Yale University, USA

Alper Yayla
The University of Tampa, USA

Haadi Jafarian
University of Colorado Denver, USA

ABSTRACT

Wearable devices have evolved over the years and shown significant increase in popularity. With the advances in sensor technologies, data collection capabilities, and data analytics, wearable devices now enable interaction among users, devices, and their environment seamlessly. Multifunctional nature of this technology enables users to track their daily physical activities, engage with other users through social networking capabilities, and log their lifestyle habits. In this chapter, the authors discuss the types of sensor technologies embedded in wearable devices and how the data collected through such devices can be further interpreted by data analytics. In parallel with abundance of personal data that can be collected via wearable devices, they also discuss issues related to data privacy, suggestions for users, developers, and policymakers regarding how to protect data privacy are also discussed.

DOI: 10.4018/978-1-7998-8954-0.ch009

INTRODUCTION

Wearable devices are portable computing devices that users can wear on their body or clothing. Varying from smart glasses to smart clothing, the majority of wearable devices are either stand-alone (e.g., fitness trackers) or integrated devices (e.g., a part of shoes, smartwatches, or phones). The adoption of wearable devices has been increasing steadily in recent years. The wearable market is expected to increase by 19% in the next four years and projected to reach $54 billion by 2023 (Barkho, 2019). The popularity of wearable devices is not just among the young and healthy adults anymore. 17% of Americans over 65 years old also use fitness trackers for health-related purposes (Japsen, 2016). One of the main reasons for this wide adoption is the multifunctional nature of wearable devices. Equipped with various sensors and data analytics capabilities, functionalities of wearable devices enable a variety of ways for users to manage their health. Key functionalities include tracking sleep patterns, monitoring episodes of physical activity, and measuring calorie consumption and heart rate, which can lead to informed health decision making and the formation of healthy habits (Kim & Shin, 2015; Patel, Asch, & Volpp, 2015). In addition to being a health facilitating tool, wearable devices can also be fashion accessories due to their ability to be customizable based on users' preferences towards aesthetics and self-expression (Solomon, 2018).

Be it a fitness device or fashion accessory, wearable devices have evolved over the years to an extent where they are no longer just devices that simply track users' daily activities. With the advances in sensor technologies, data collection, and data analytics capabilities, wearable devices now enable seamless interaction between users and their environment. Therefore, they not only track users' daily activities but also provide insights into their emotions, personal preferences, and health status. Such a data-driven interaction also brings concerns related to the privacy and security of highly sensitive user data.

Data privacy is one of the most challenging issues in today's data-driven society. As more users share personal information and more of their information is digitized, this challenge is becoming a central issue for both individuals, organizations, and policymakers. With the widespread increase in the adoption of wearable devices, data privacy has also become an important topic for wearable device users. Unlike other self-disclosure technologies, such as mobile applications (apps) and websites (Lowry, Cao, & Everard, 2011), sensors in wearable devices allow the collection of a wide variety of user data ubiquitously and unobtrusively on a continuum basis, and in most cases, without the explicit consent of the user. Therefore, data privacy is more challenging and unique in the context of wearable devices.

The passive and continuous data collection combined with data analytics capabilities enables interpretation of highly sensitive personal information, such as alcohol and substance use (Carreiro et al., 2018; Raij, Ghosh, Kumar, & Srivastava, 2011), sleep patterns (Sathyanarayana et al., 2016), and users' emotional states (Thapliyal, Khalus, & Labrado, 2017). Wearable devices also allow the collection of location-based data, which can be used for behavioral analytics, such as users' visit frequency of a wellness center, a hospital, or an ice cream vendor. With the increased interest in such rich consumer data and the sensitivity of the information that can be collected, consumers should treat wearable devices as a high-privacy concern product (Chen, 2013; Gao, Li, & Luo, 2015). However, users tend to underestimate the potential consequences of disclosing personal information via wearable devices (Klasnja, Consolvo, Choudhury, Beckwith, & Hightower, 2009; Raij et al., 2011).

In a broad sense, the data collected by wearable devices result in three main privacy modalities, i.e., situations that may result in privacy concerns. The first modality is related to privacy concerns that may arise due to the data collected by the device and the loss of ownership of the device. This relates to cases of losing a wearable device with personal data or an unauthorized individual accessing the device or data