Chapter 6
Privacy Dangers of Wearables and the Internet of Things

Scott Amyx
Amyx McKinsey, USA

ABSTRACT

This chapter identifies concerns about, and the managerial implications of, data privacy issues related to wearables and the IoT; it also offers some enterprise solutions to the complex concerns arising from the aggregation of the massive amounts of data derived from wearables and IoT devices. Consumer and employee privacy concerns are elucidated, as are the problems facing managers as data management and security become an important part of business operations. The author provides insight into how companies are currently managing data as well as some issues related to data security and privacy. A number of suggestions for improving the approach to data protection and addressing concerns about privacy are included. This chapter also examines trending issues in the areas of data protection and the IoT, and contains thought-provoking discussion questions pertaining to business, wearables/IoT data, and privacy issues.

INTRODUCTION

Data privacy concerns are not new, but they are taking on an increased urgency as more wearable and Internet of Things (IoT) devices are used in commercial, public, and private settings. While companies may be partially addressing enterprise, con-

DOI: 10.4018/978-1-5225-1016-1.ch006

sumer, and employee concerns about data privacy and collection, it is difficult to be completely prepared for the ubiquity of connected sensors that will rapidly become part of everyday life. This lack of preparedness can be seen in the innumerable data breaches that have resulted in lost consumer confidence, damaged reputations, stolen confidential business insights, identity theft, and litigation.

Technological solutions, such as firewalls and antivirus software, provide only part of the solution to the challenge of successfully managing wearables and IoT data. A change in the approach to data security on devices and on corporate servers (or in the cloud) is foundational to success: privacy must be a priority, and enterprises that engage in positive privacy practices will offer a unique differentiation in the market. As argued below, companies that are serious about protecting data need to incorporate privacy into their business models, promote a culture of privacy in the workplace, empower a Chief Privacy Officer, become involved in standards-based consortiums, and develop an enhanced privacy policy that is easy to understand. All connected devices need to have software/encryption protections and enterprise storage of data needs to be secure and maintained.

BACKGROUND

The advent of the Internet of Things (IoT), sometimes referred to as the Internet of Everything (IoE), and wearables has had a tremendous impact on consumer and enterprise concerns about privacy. The IoT consists of any object that can be connected to a network, and wearables are clothing, jewelry, or accessories that can collect and transmit data about the wearer. The IoT is driven by M2M (machine to machine) telemetry, and although some consider these two terms to be interchangeable, there are important differences (see Polsonetti, 2015). In this work, the term IoT will be used to refer to objects, in or upon which sensors can be placed, and which allows them to connect to a network.

Benefits and Drawbacks

Wearables and the IoT come with a number of benefits and drawbacks. The benefits of these devices can be seen in the data they supply. Ubiquitous connected sensors and devices constantly recording, transmitting, and sending data create an enormous opportunity for businesses to generate detailed consumer profiles to improve marketing campaigns and engender increased revenue through targeted advertising. The data derived from IoT devices can also improve productivity in the workplace, as the monitoring of certain activities can give insight to management while enhancing innovation, cooperation, and safety practices at the individual and team levels. (For