Chapter 12
Conclusions:
Where Next for Wearables?

Don Kerr
University of the Sunshine Coast, Australia

John Gammack
Zayed University, UAE

ABSTRACT

This chapter provides a contemporary example of how data from wearable devices can be used for "big data" type research. It then asked the question of data policies for the use of data generated by wearable devices. This is followed by an overview of the chapters in the book and how they fit within the general theme of the book. In addition, each chapter is categorised into whether it is social research or more technical type research. The chapter also includes concluding suggestions on the possible future research agenda for privacy and security within the subject domain of the use of wearables. In addition, insights into the future of wearables in relation to ethical considerations, privacy, security and data ownership is also given.

INTRODUCTION

Scientists announce that there is a global sleep crisis and describe how age, gender and the amount of natural light people are exposed to affects sleep patterns in 100 countries around the world (ABC News, 2016). A curious reader may well ask, "How did they get all that data?". The answer is from smartphone apps linked to wearable activity devices. While some readers may consider this to be very useful research, others may consider the information obtained to be a violation of people's

privacy. In this particular study, 6,000 people were asked to send anonymous data about their age, gender, country of residence and time zone to the researchers (ABC News, 2016). As the authors of chapters in this book have brought to light, however, new possibilities enabled by gathering data from wearables may have undesirable social and personal impacts.

Here, the asking of permission to undertake the study was merely a courtesy by the research team, since the data obtained in a study such as this can easily be obtained without any written consent. This is because it is just "out there in the cloud" and controlled by organizations who have accountability neither to its sources nor to its end users, and who can, in fact, on-sell the data to the highest bidder.

Welcome to the world of wearable devices, a world where security and privacy can be traded off against getting the latest device out to market in the quickest possible time in order to increase market share and maximize profits. As the chapters in this book have demonstrated, the use of wearable devices potentially compromises their users' security and privacy. The collected data, whether medical, geographical, or personal, and in video, audible, or other precisely specified forms, can end up being a uncontrolled resource whereby anyone can access the data for any reason. In addition to privacy concerns, there is also a range of security issues associated with smart wearable devices. These concerns are very real and have implications for end users, for enterprises, and for society as a whole.

As is understood by security experts, the machine-to-machine communication in the wearable area is not as secure as it is in other parts of the Internet. Any Bluetooth communication between devices (such as a fitness bracelet and a smartphone) can be easily accessible to third parties. At present, much of the communications between devices is not encrypted and can easily be intercepted. Moreover, as described in various chapters of this book, the privacy and security issues associated with wearables have been demonstrated to be problematic, both from a technical point of view and from a social or policy view. The dangers noted raises management problems, not just for enterprises and custodians of data but for government and lawmakers regulating society as well.

This final chapter is divided into the following sections. The next section provides an overview of each chapter and how the content of the chapter fits into the research themes of the book. The issues involved in wearables cover technical aspects, particularly around security issues, along with managerial and wider social issues, issues relevant to the privacy and freedoms of individuals, enterprises and society at large. The various chapters were selected to represent this range of research. The second section, titled, "What have we learned?", attempts to abstract lessons from all the chapters to provide a general view of what has been learned from research across these various areas. The final section discusses the issue of "What is next?" and attempts to provide an overview of possible research directions in the future.

9 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/conclusions/164313

Related Content

Web 3.0 and E-Learning: The Empowered Learner
Amit Chauhan (2016). *Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications (pp. 41-62).*
www.irma-international.org/chapter/web-30-and-e-learning/138176

Open Source for Mobile Devices and Mobile Learning
Hal Steger (2012). *Wireless Technologies: Concepts, Methodologies, Tools and Applications (pp. 1900-1908).*
www.irma-international.org/chapter/open-source-mobile-devices-mobile/58875

Exploring Value-Added Applications of Chipless RFID Systems to Enhance Wider Adoption
Ming K. Lim (2013). *Advanced RFID Systems, Security, and Applications (pp. 221-240).*
www.irma-international.org/chapter/exploring-value-added-applications-chipless/69709

Laws Associated with Mobile Computing in the Cloud
Gundars Kaupins (2012). *International Journal of Wireless Networks and Broadband Technologies (pp. 1-9).*
www.irma-international.org/article/laws-associated-with-mobile-computing-in-the-cloud/90273

Effect of Nodes Mobility on Density-Based Probabilistic Routing Algorithm in Ad-hoc Networks
Hean-Loong Ongand Essam Natsheh (2012). *International Journal of Wireless Networks and Broadband Technologies (pp. 29-48).*
www.irma-international.org/article/effect-nodes-mobility-density-based/75526