Chapter 7
Security, Privacy, and Ownership Issues with the Use of Wearable Health Technologies

Don Kerr
University of the Sunshine Coast, Australia

Kerryn Butler-Henderson
University of Tasmania, Australia

Tony Sahama
Queensland University of Technology, Australia

ABSTRACT

When considering the use of mobile or wearable health technologies to collect health data, a majority of users state security and privacy of their data is a primary concern. With users being connected 24/7, there is a higher risk today of data theft or the misappropriate use of health data. Furthermore, data ownership is often a misunderstood topic in wearable technology, with many users unaware who owns the data collected by a device, what that data can be used for and who can receive that data. Many countries are reviewing privacy governance in an attempt to clarify data privacy and ownership. But is it too late? This chapter explores the concepts of security and privacy of data from mobile and wearable technology, with specific examples, and the implications for the future.

DOI: 10.4018/978-1-5225-1016-1.ch007

Copyright ©2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

This chapter examines at the current state of play with respect to wearables and the issues that have gained a lot of press over recent years. The chapter is broken into three main sections: the first discusses the present situation and the concerns the public has with respect to security and wearable devices. The second section discusses ownership of the data and how that effects security. Questions asked in this section are related to who owns the data and who is responsible for any data breaches. The third section looks at the integrity of mobile health information. This includes the need for verification of results and trust that the personal information is safe and secure.

HISTORY OF WEARABLE TECHNOLOGY

Wearable health technology refers to technology devices that is worn by consumers to track, monitor, and gather information related to health and fitness. These can be worn around the wrist or ankle, may be clipped to the body, or worn around the neck. Wearable technologies include smart watches, sports watches, fitness trackers, smart clothing, smart jewellery, head-mounted displays and implantable technology and can be synced with a mobile device or computer. Using technologies such as GPS, accelerometers and gyroscopes, they can monitor the heart rate, temperature, perspiration, body fat composition, and muscle activity to provide information about the user's health, movement, speed, and distance.

By this definition, the first wearable technology could be tracked back 700 years ago to the first wearable glasses. In 1759, John Harrison developed the H4 longitude watch that was able to determine the longitude at sea. And the first reported hearing aid was in 1911, with Siemens & Halske releasing the Esha-Phonophor (a device for the hearing impaired) (McLellan, 2014).

Whilst there was the development of numerous wearable technologies over the years, the first wearable health technology that collected and relayed health information was the pedometer. Whilst the first accurate measurement of distance walked occurred in the 15th century by Leonardo da Vinci, it was not until the late 18th century, when Thomas Jefferson developed the first prototype of the pedometer (a manual system that allowed the user to count their steps). Today's pedometers contain a pendulum to more accurately detect movement and can capture and transmit data electronically. The first smart watch that incorporated this technology was the Garmin Forerunner, released in 2003 (McLellan, 2014).

19 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/security-privacy-and-ownership-issues-with-the-use-of-wearable-health-technologies/164308

Related Content

CHEERBOT: A Step Ahead of Conventional ChatBot
Chintan Bimal Maniyar, Chintan M. Bhatt, Tejas Nimeshkumar Panditand Dewanshi Harishankar Yadav (2019). *Next-Generation Wireless Networks Meet Advanced Machine Learning Applications (pp. 306-322).*
www.irma-international.org/chapter/cheerbot/221437

Link Failure Avoidance Mechanism (LFAM) and Route Availability Check Mechanism (RACM): For Secure and Efficient AODV Routing Protocol
Meeta Singhand Sudeep Kumar (2018). *International Journal of Wireless Networks and Broadband Technologies (pp. 1-14).*
www.irma-international.org/article/link-failure-avoidance-mechanism-lfam-and-route-availability-check-mechanism-racm/209431

Security in Pervasive Computing
Sajal K. Das, Afrand Agahand Mohan Kumar (2005). *Wireless Information Highways (pp. 421-440).*
www.irma-international.org/chapter/security-pervasive-computing/31457

Optimization Trends for Wireless Network On-Chip: A Survey
Saliha Lakhdariand Fateh Boutekkouk (2021). *International Journal of Wireless Networks and Broadband Technologies (pp. 1-31).*
www.irma-international.org/article/optimization-trends-for-wireless-network-on-chip/272049

Cryptography and Blockchain Solutions for Security Protection of Internet of Things Applications
Kamalendu Pal (2022). *Information Security Practices for the Internet of Things, 5G, and Next-Generation Wireless Networks (pp. 152-178).*
www.irma-international.org/chapter/cryptography-and-blockchain-solutions-for-security-protection-of-internet-of-things-applications/306841