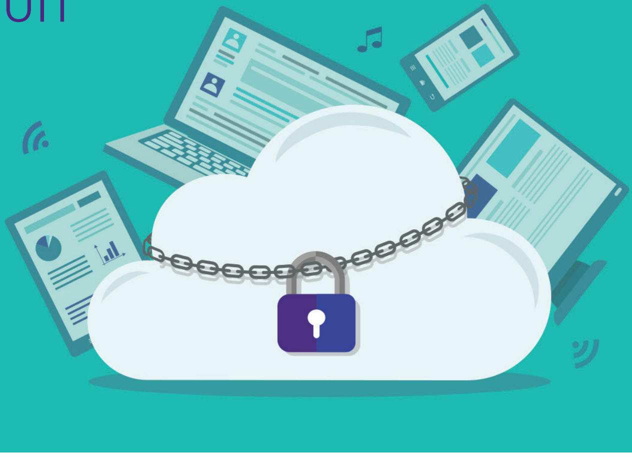
Health Wearables, Apps & Information Protection

Claire Bond-Myatt



Technology has long been an enabler of healthcare, with technological innovations bringing about new ways to deliver higher quality care to more people, for less. Wearable devices are not new, healthcare professionals have been using heart rate monitors and other hardware as a method of monitoring vital statistics, among other things, for years. What is new though, is the rate of dispersion and the variety of devices coming into the commercial market, available to both healthcare providers and, increasingly, the public.

The wearable device market, also known as the quantified self, has amassed popularity in recent years. In 2015, global retail in this market was expected to reach US$4.5 Billion, and was estimated to triple by 2019 to a whopping US$53 Billion[1].

Rapid innovations in technology, falling costs in the unit price of devices, and a general social trend toward health by tech savvy consumers, are largely held to be the drivers of the increased demand for health-related wearables.

With increased demand comes a highly competitive market with new and old entrants battling it out to produce better, more accurate and more useful wearables. The pace of innovation and demand in this space is increasingly leading to concerns over privacy and inadequate security safeguards as development outstrips legislative and regulatory requirements.

Security and Privacy

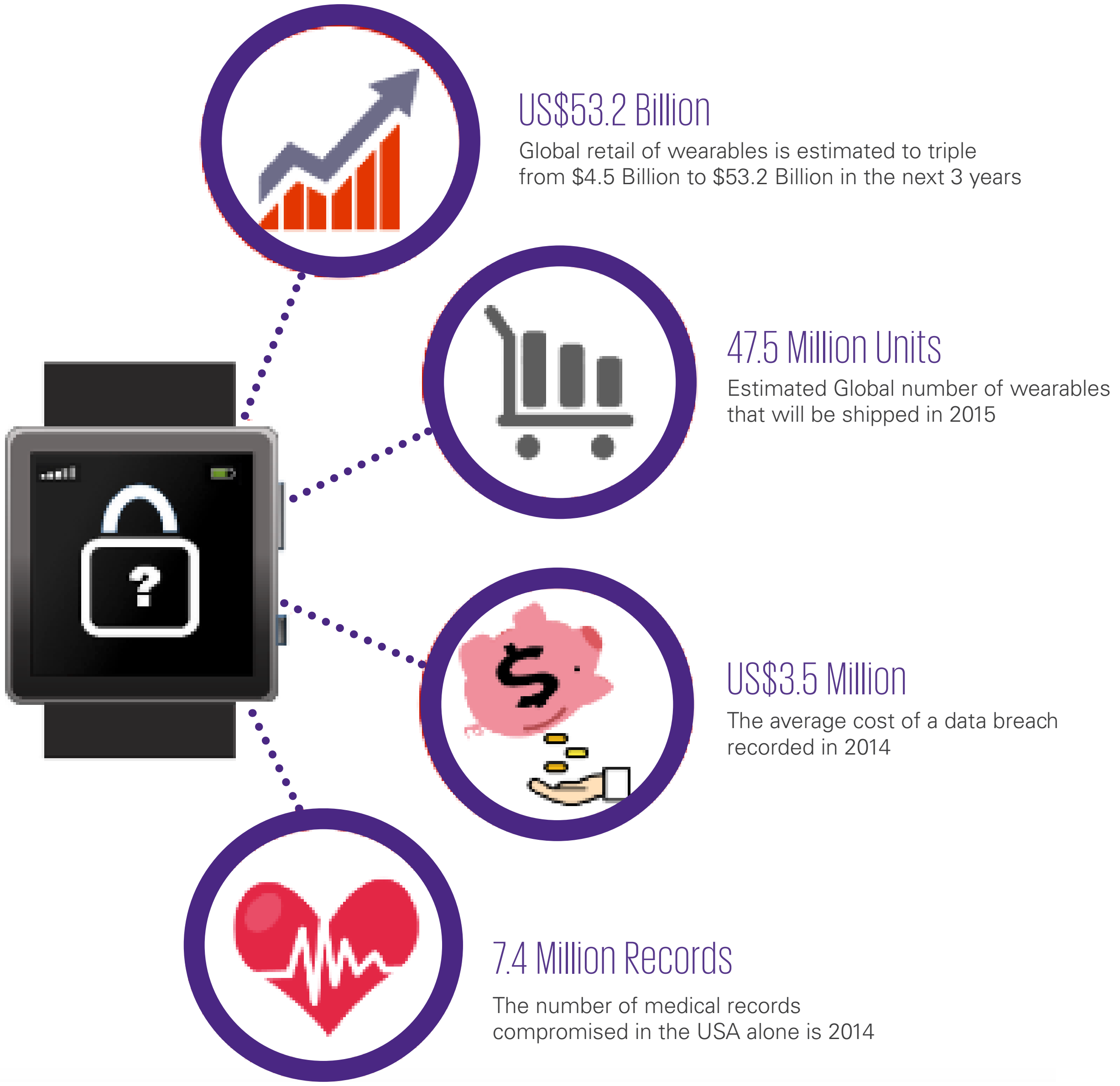
Wearables present multiple attack vectors, in that they often require data to be transmitted to a processing application typically housed on a smart device such as phones, tablets or computers. Furthermore, applications may store the data online.

Reviews by various security firms[2,3] have found multiple vulnerabilities in wearable devices and related applications, these range from exposed login credentials, network sniffing (wherein data transmitted from the device is visible to potential attackers), to being able to monitor a user's location through their device's tracking mechanism and public networking capability.

It is worth considering the security risks of wearables when linked to smart devices. Careless users may leave their wearable or smart phone unattended, where any person may pick it up and peruse the data stored thereon. Wearables themselves are not typically password protected or secured, and smartphones and other devices are only as secure as their lock screen password, if enabled.

Future concerns include the vulnerability of the Internet of Things to cyberattacks. While not currently viewed as a serious problem, it is poised to become one as smart devices, wearables and other smart appliances become more widely adopted, providing would-be thieves with a plethora of information about individuals[4].

Some statistics on wearables and data breaches in 2014



US$53.2 Billion

Global retail of wearables is estimated to triple from $4.5 Billion to $53.2 Billion in the next 3 years

47.5 Million Units

Estimated Global number of wearables that will be shipped in 2015

US$3.5 Million

The average cost of a data breach recorded in 2014

7.4 Million Records

The number of medical records compromised in the USA alone is 2014

Health wearables typically communicate with applications on smart devices

Privacy of the user is closely linked to the security considerations and concerns that are inherent to wearables. Wearables that process health-related information - which may be anything from vital statistics to sleeping patterns - and track user locations, require additional safeguards to be in place to ensure the protection and lawful processing of such information in accordance with various legislation and regulations in place worldwide.

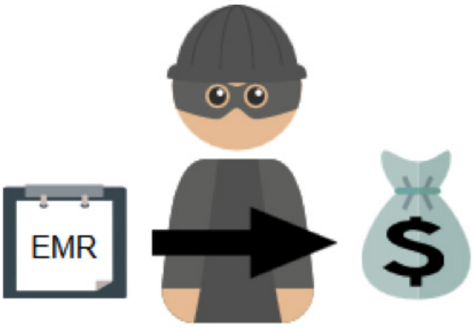
Wearables are often used with a number of applications which may be free, paid for or come with the wearable or your smart device. What is not evident, though, is who has access to the data once you have loaded it from the wearable onto the application. Even more disconcerting is that once you have done so, you may not own the data anymore. A review of 100 health and fitness apps available on the iOS and Android app stores found that more than half of the reviewed programmes did not have a Privacy Policy[5] in place, which may be an indication of their lack of commitment to ensuring the privacy of users.

Globalisation provides another facet of complexity. Wearables and applications developed in one part of the world, are quickly made available worldwide. Many countries have established privacy laws which regulate the processing of personal information, including health information, and in some counties more stringent safeguards to ensure the privacy of individuals health-related information (such as HITECH in the United States) that would need to be considered.

Furthermore, some countries require mechanisms to be in place to protect personal information that is transferred across borders. Through increased accessibility of wearables and related applications globally and the differing legal requirements for privacy between countries, challenges are presented to both users and service providers to determine the applicable legislation and regulatory framework that is to be applied.

Breaches of personal information held by organisations, especially health-related information, are also a concern. In 2014, the top 5 health-related breaches in the USA alone affected 7.4 million individuals[6]. Breaches of personal information are not only costly to the organisations responsible for the data – as highlighted in a recent IBM study which estimated the average cost of a breach to companies was $3.5 Million[7]- but also to the individual whose sensitive health information becomes public or falls into the wrong hands.

Health wearables typically communicate with applications on smart devices



Another emerging phenomenon regarding the theft of health information is medical identity theft, which is the use of stolen medical details to obtain medical care, buy drugs or submit fraudulent billing to medical aid[8]. Medical records are worth up to US$50 per record on the black market[9], which when compared to US$1 per stolen credit card record, indicates why medical identity theft is so lucrative[10]. While data coming from your fitness band or glucose meter may not be as valuable as your electronic health record on the black market, users of wearables and their related applications need to be aware of the pervasive nature of the health information being collected and stored about them, and what a breach of that information might mean.

What does it mean in a South African context?

South Africans have also been swept up in the wearable fever. Fitness bands, for example, are common features in public and in the workplace. Several medical aid schemes offer incentives to members who buy and use wearables and share the related health information with the scheme.

South African privacy awareness is still in its infancy. However, there are currently several pieces of legislation that provide a framework to understand the rights and obligations of the user, service provider and other parties, where personal information is concerned.

The Protection of Personal Information Act (POPI) is currently the most comprehensive privacy framework within the South African legislative landscape. It provides eight conditions under which personal information may be fairly and lawfully collected, used, stored, transmitted, and destroyed by both public and private organisations.

POPI requires organisations who handle personal information to ensure that personal information is processed for a specific and legitimate business purposes, limits the sharing of personal information without user consent, regulates the international transfer of personal information, and requires organisations to implement reasonable and appropriate organisational and technical security safeguards and breach notification.

The Act differentiates between personal information and special personal information, such as health-related information. Where special personal information is concerned, specific requirements need to be attained in order to process this information and may require authorisation and approval from the Information Regulator. Although POPI was enacted in November 2013, an effective date for its commencement has not yet been determined.

The Promotion of Access to Information Act (PAIA) was established to promote South Africans' right to freedom of access to information and enables individuals to request access to any information held by a public or private bodies. Under PAIA, service providers, such as app owners, will be required to inform users what data they hold, what is available for viewing and how information can be accessed.

The Electronic Communication and Transactions Act (ECTA) provides a legal framework to enable the growth of electronic commerce in South Africa, regulating the information that is shared. ECTA provides optional privacy provisions which cover information obtained through electronic transactions. Where data controllers - wearables and applications which request, collect, process and store data - subscribe to the provisions of the Act, the Act provides guidelines for the lawful processing of that information in order to provide privacy to the data subject.

ECTA also specifically offers provisions which define cybercrime, this includes unauthorised access to, interception of or interference with data (such as hacking and data theft) as well as computer-related extortion, fraud and forgery (such as medical identity left). The Act also provides penalties for cybercrime.

Other legislation which will affect the creation and use of wearables and their related applications will include the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) , the South African Constitution which offers the basic right to privacy and access to information, as well as the National Health Care Act which provides the individual the right to confidentiality.

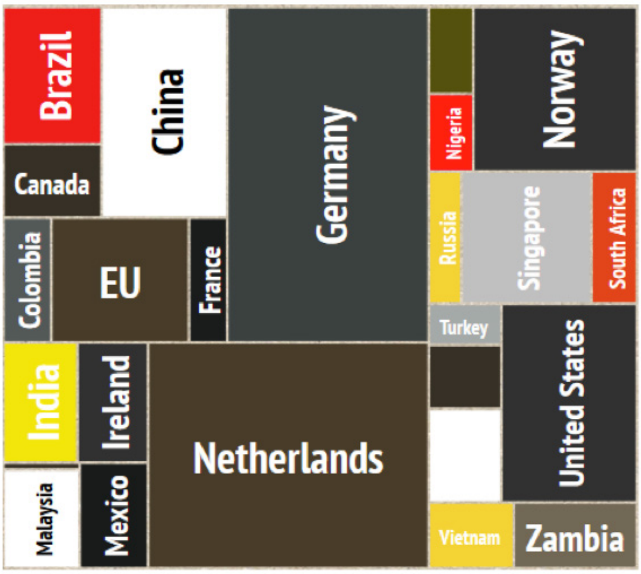
Cybercrimes in South Africa

In 2014, McAfee estimated the annual cost of cybercrime to the global economy to be US$400 Billion[11]. In the same year, cybercrime cost South Africa R5.8 Billion Rand (roughly 0.14% of national GDP)[12]. The infographic to the right provides a base for comparison of the cost of cybercrime as a percentage of GPD in countries around the world15. The majority of South African businesses and the public are not aware or ready for the sophisticated nature of cybercrime, which is only likely to worsen over the next few years. A 2013 report from Norton suggests that of all 24 countries surveyed, South Africa had the third largest number of cybercrime victims (over 1 million people affected)13.

Cybercrime is often viewed as a first world crime, and perhaps due to its remote and nonviolent nature, is an underrated crime in South African society but it is one which is seriously impacting the country's economy. Consider for the sake of comparison, that bank card fraud cost the economy R453.9 Million in 201414.

With health-related information fetching such a high price on the black market, and cybercrime already a problem, it probably will not be long before medical identity theft and other health data related crime becomes prevalent in South Africa. While ECTA and POPI legislation are in place to protect citizens and businesses, cybercrime is often difficult to detect, and apprehending the culprit even more so.

Cost of cybercrime as a percentage of GPD in countries around the world



Wearables are simply one of the many healthcare-related innovations making their way onto the market. Although concerns exist regarding how such devices are being secured, and whether user privacy concerns are being addressed, these challenges are not insurmountable to the consumer.

Discerning users may protect their data and themselves by carefully reading terms and conditions, and available privacy policies on the wearables and applications they wish to use, as well as knowing their rights under their local privacy legislation. Users can further defend their data through taking cognisance of the threat of cybercrime and following good security practices such as taking precautions to secure their devices - strong passwords, encryption and dual authentication - as well as being aware of who they are allowing to access their data and devices.

References

1 http://www.juniperresearch.com/press/press-releases/smart-wearables-market-to-generate-$53bn-hardware

2 http://www.forbes.com/sites/symantec/2014/08/19/how-safe-is-the-data-on-your-wearable-tech/

3 http://www.wickhill.com/blog/main-category/wearable-tech-just-how-secure-is-it/#.VWr61EaPMtI

4 https://securelist.com/blog/research/66439/wearable-security-present-and-future/

5 http://www.forbes.com/sites/symantec/2014/08/19/how-safe-is-the-data-on-your-wearable-tech/

6 http://www.databreachtoday.com/biggest-health-data-breaches-in-2014-a-7705

7 http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf

8 https://oig.hhs.gov/fraud/medical-id-theft/

9 http://www.medscape.com/viewarticle/824192

10 http://www.secureworks.com/assets/pdf-store/other/infographic.healthcare.pdf

11,15 http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf

12 http://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/

13 http://www.itweb.co.za/index.php?option=com_content&view=article&id=70918

14 http://www.sanews.gov.za/business/sharp-increase-bank-card-fraud