Kalpa Publications in Computing

Volume 12, 2019, Pages 112–122

Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019

Privacy in wearable health devices: How does POPIA measure up?

Munyaradzi Katurura and Liezel Cilliers
University of Fort Hare, East London, South Africa
mckaturura@gmail.com, lcilliers@ufh.ac.za

Abstract

The market for wearable devices that is used for health monitoring has steadily increased over the past few years. South Africa has also seen an increase in the adoption of these wearable device. This is partly because these devices allow users to monitor their health and wellbeing in real time. However, to be efficient, the devices must collect a large amount of data. Some of the data that is collected include personally identifiable and health information which could be considered sensitive to the user. This study investigated if the Protection of Personal Information Act (POPIA) provides adequate protection to South African users of wearable health devices. The POPIA and the privacy policy of the 2 most popular wearable health devices in South Africa, the Apple watch and Fitbit, were qualitatively compared making use of Hutton et al's (2018) heuristic framework. The study found that POPIA protected the users' privacy when it came to notice, users' awareness, choice and consent, access and participation. The Act did not cover any privacy matters related to social disclosure of information by users. The study also found that Apple watch and Fitbit did well in protecting users' privacy with regards to notice and awareness as well as access and participation. The two wearables performed poorest in regards to choice and consent as well as social disclosure controls to protect users' privacy. The study recommend that users educate themselves in regard to how their data collected by wearable health devices are collected and protected.

Keywords: Personal protection of personal information act, POPIA, Wearable devices, Data privacy, Social disclosure, wearable devices

1 Introduction

The market for wearable health device has increased over the past decade with annual sales of over 113 million units sold between 2017 and 2018. The sale of these devices is predicted to increase to 222 million units by 2021. The most popular brands are FitBit, Apple watch, Xiaomi, Samsung and Garmin (Shin, Jarrahi, Karami, & Gafinowitz, 2018). Wearable health devices allow the user to track and monitor their health and fitness.

Wearable health devices is a category of technology devices designed to be worn on the human body (Peltola, 2017). Seneviratne et al., (2017) proposed that there is a distinction between wrist-worn devices, e.g FitBit, and smart watches such as the Apple watch. Typically a smartwatch will have a touchscreen display, while wrist-worn devices are mainly used for fitness tracking but do not have a

touchscreen display. Both these devices do have some form of computer with integrated sensors that can collect information relating to the user (Haghi, Thurow, & Stoll, 2017; Peltola, 2017). Due to their attentive and communicative qualities wearables devices have attracted attention from developers in various fields including health, fitness, sport, art and industrial applications (Walker, Hickey, & Freedson, 2016). Software and hardware developments in the wearables platform continue to grow due to the increased adoption of these devices for health monitoring purposes (Hutton et al., 2018). Some of the functions currently provided by wearables include step counting, sleep tracking, heart rate monitoring, workout duration and calories burnt (Cilliers, 2019).

Wearable health devices are able to collect data from the user in real-time, process the data immediately and provide instant feedback to the user (Ching & Singh, 2016). Examples of data that can be collected include location – GPS; food consumed – logged manually; activity/movements and sleep patterns – accelerometers, pedometer and altimeters; muscle function and coordination – pressure sensors; heart rate, blood pressure – heart rate sensors (Apple Inc, 2019; Charara, 2018; Cilliers, 2019; Fitbit, 2018; Genuth, 2015; Piwek, Ellis, Andrews, & Joinson, 2016). The wearable health devices also allow the user to share their information to social media or other users e.g. exercise routines, real-time mapped running routes and exercise challenges (Vitak, Liao, Kumar, Zimmer, & Kritikos, 2018). These devices continually monitor human activity for purposes of improving the efficiency, productivity and health management of the user (Cilliers, 2019). The wearable devices collect information such as demographic information of the user, health information and Personally Identifying Information (PII). PII is any information that can be used in identifying tracing or distinguishing an individual's identity (Katurura & Cilliers, 2016). PII includes information such as names, alias, date of birth, race, weight, daily activities, geographical indicators, medical information, educational information, personal identification numbers, address information, contact information, personal characteristics, photographs and other information that is linkable to any of the PII mentioned here (Botha & Grobler, 2017; Katurura & Cilliers, 2016; Parliament of the Republic of South Africa, 2013).

However, due to limited storage and processing power of wearable health devices, the device must transmit the data collected to the device manufacturer for processing and long term storage (Cilliers, 2019). The service provider also shares the information collected to partner companies for purposes of processing, marketing or other business interests of the device manufacturer (Ching & Singh, 2016; Hutton et al., 2018). The collection, sharing and transmitting of PII introduces privacy concerns to the user. The privacy of PII refers to the ability of the service provider collecting, processing and transmitting the information to keep it secure from unauthorised access, data breaches and ensuring the individual who the data identifies does not suffer any loss due to privacy breaches (Kandeh, Botha, & Futcher, 2018; Parliament of the Republic of South Africa, 2013).

A report by BusinessTech, (2018) stated that the top selling wearables in the world were Apple watch series 1 and 3, Fitbit Versa and Ionic and Amazifit BIP. In South Africa, the market for wearable health devices such as Fitbit Apple watch and Amazifit has reached $110 million between 2018 and 2019 and this amount is expected to increase to $134 million by the year 2023 (statista.com, 2019). Fitbit and Apple watch are the focus of this study due to their popularity in South Africa as reported by BusinessTech (BusinessTech, 2018). There is a need to protect the privacy of the users' information being collected from these devices. In South Africa the Protection of Personally Identifiable Information Act (POPIA) is the most applicable Act to protect the privacy of wearable health device users. However, the protection of the collected user data is the responsibility of the device manufacturer who own the data and is not located in South Africa (Cilliers, 2019; Hutton et al., 2018). The device manufacturer, in this study Apple and FitBit, do provide privacy policy statements on their website that explains how

the privacy of the user is managed. These privacy policies are largely guided by their company best practices and are not country specific (Apple Inc, 2019; Fitbit, 2018). Therefore, there is a need to compare if these generic privacy policies do protect the privacy of South African users' of wearable fitness devices when compared to the POPIA. This comparison will help highlight any privacy vulnerabilities that are introduced by the use or wearable fitness devices. It will also help lawmakers in South Africa with necessary information on how the data privacy laws can be improved to keep citizen's data safe.

2 Fitbit privacy policy

Fitbit's privacy policy deals with the information that is collect from users as well as how the information is used and shared. It also details the data retention policy and the user's right to access and control the data. It addresses international operation and data transfer, information security as well as policies for children using their devices (Fitbit, 2018).

Fitbit collects usage information as well as some PII which is either collected directly through the device or from any third party applications and social media platforms that may be linked to the Fitbit account. The collected information is used to provide, maintain, improve and develop personalised services to the user. The information is also shared to third parties who analyse and process the data on behalf of Fitbit (Fitbit, 2018).

The user is allowed access to their data as well as the ability to edit or delete their information. They are allowed to restrict the use of their information for certain purposes. However the user has to opt out of these by making use of the settings of their account. Data deletion it is not immediate and the policy states it can take between 30 and 90 days for complete deletion of data relating to a user [11]. For international users from the European Union (EU) region Fitbit commits to comply with the General Data Protection Regulation (GDPR) published in 2018. No specifications were made in the policy for non EU countries (Fitbit, 2018).

3 Apple watch privacy policy

Apple watch's privacy policy states that PII and other information is collected from users for purposes of improving service delivery to the user. The information collected may be shared to third parties who provide services, products and marketing on behalf of Apple. The privacy policy states no PII is shared with third parties for marketing purposes (Apple Inc, 2019).

The privacy policy states that data is only retained for the purpose of providing the service that it has been collected for. The user is allowed access to a copy of their data which Apple commits to keep accurate, complete and up-to-date. The user is also allowed to delete their information, however, the policy states that this action may be denied if deletion of the data undermines the legitimate use of the data (Apple Inc, 2019). For international users the policy abides by the Asia-Pacific Economic Cooperation (APEC) Cross Boarder Privacy Rules System, which provides a framework for protection of PII transferred among APEC participating economies (Apple Inc, 2019).

4 POPIA

POPIA was published in 2005 for public comment and enacted in 2013 as an Act of parliament. POPIA governs the collection, processing and sharing of personally identifiable information. The Act came into effect in 2018 and is now being enforced (Kandeh et al., 2018). A regulator has been appointed to monitor the compliance of all individuals and organisations that collect or process information (Kandeh et al., 2018; Parliament of the Republic of South Africa, 2013). The Act is generic and is meant to apply to all collection and processing of personally identifiable information (Katurura & Cilliers, 2016). The Act prescribes eight principles that must be complied with when handling personal information. The principles cover the following areas (Kandeh et al., 2018; Katurura & Cilliers, 2016):

1. Accountability – the entity collecting data must notify the user what information is collected and obtain consent from the user before any data is collected.
2. Processing limitation – the information should only be processed for purposes of providing the service it was collected for. The aim of the information processing should be to the benefit of the end user.
3. Purpose specification- only information relevant to the specific task can be collected from the user.
4. Further processing limitation – information should not be retained beyond provision of the service for which it was collected for unless the service is still ongoing.
5. Information quality- the individual or organisation collecting the information must be committed to making sure that the users information remains correct, complete and accurate at all times.
6. Openness – should a breach in privacy occur the affected user to whom the compromised data belongs must be notified and sufficient reparations proportional to the damage or loss suffered due to the loss must be paid by the entity collecting the data. Subsequently the information regulator must also be notified of the breach.
7. Security safeguards – significant security safeguards, both physical and software, must be implemented to protect the data.
8. Data subject participation- the subject to home the data relates should be allowed to view and edit their information should it not be accurate.

5 Theoretical grounding of the study

The study made use of a heuristics framework to evaluate the privacy considerations of wearable health devices by comparing individual device privacy policies and POPIA. Heuristics can be defined as a method of quickly evaluating or problem solving without external help (Nur, Sulaiman, & Aman, 2018). Hutton et al., (2018) identified a heuristic framework that can be used to evaluate the privacy of data being collected and shared through wearable health devices (Figure 1). The heuristics framework was aimed at evaluating four broad categories of privacy management which are the control of third party disclosure, informed consent to data collection, access to information collected and continued control over data collection once consent is given. After identifying these categories, the individual factors for each category were identified from four sources: privacy literature for wearable health devices; the European Union's GDPR; Inostroza, Rusu, Roncagliolo, & Rusu, (2013)study of usability heuristics for touchscreen mobile devices and the STRAP Framework, a technique that is aimed at supporting analysts in identifying privacy and security concerns during early design. Hutton et al., (2018)tested their heuristics framework against the privacy policies of 64 popular self-tracking services and wearable

devices. The results of the study indicated that the majority of the privacy policies did not provide users' full access to their own data, did not acquire sufficient consent for the use of the data, or inadequately extended controls to third parties. The study also found that services for health related data tracking were worse than other types of services at privacy compliance (Hutton et al., 2018). The heuristics framework combine the most recent mobile health privacy regulations and best practises hence they are ideal for use for this study. An illustration of how the heuristics were constructed and used in the original study is shown below as well as an indication of the focus area of this study. This study only made use of the 'Privacy Heuristics' category as indicated in Figure 1 to evaluate the privacy policies of wearable health devices against POPIA.

6 Methodology

The study made use of a literature review to investigate the research problem. A qualitative, interpretive approach was applied to critically evaluate the privacy policies of Apple watch and Fitbit against POPIA making use of Hutton et al's heuristics framework (Hutton et al., 2018). The Privacy policies of Apple watch and Fitbit were read independently by 2 researchers after which their summaries were compared on the four broad categories of the heuristics framework: notice or awareness, choice and consent, access and participation, and social disclosure. The same method was applied to POPIA. A comparative analysis of POPIA, the Fitbit and Apple watch privacy policies against the heuristics developed by Hutton et al., (2018) provided insight into the discussion in table 1.

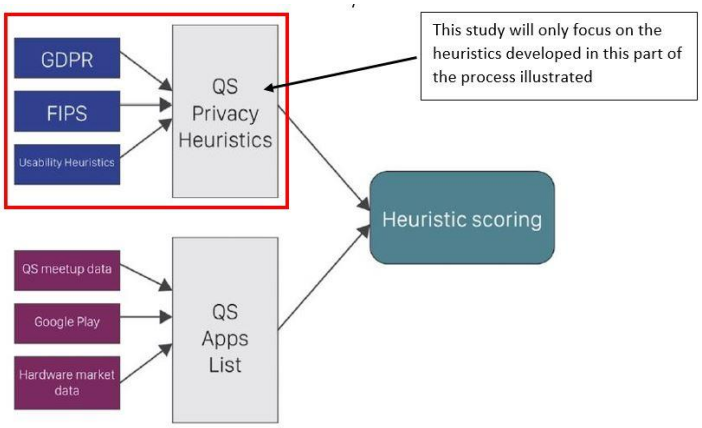

Figure 1: Heuristics framework (Hutton et al., 2018)

Table 1: Comparison of POPIA and the privacy policies of Fitbit and Apple watch

		POPIA	**Fitbit**	**Apple watch**
Notice or Awareness				

H1	Before data are shared with a remote actor, the entity collecting the data is explicitly identified.	X	X	X
H2	Before data are shared with a remote actor, the uses of the data are explicitly identified.	X	X	X
H3	Before data are shared with a remote actor, the potential recipients are explicitly identified.	X		
H4	The nature and means of the data collected are explicitly identified.	X	X	X
H5	Steps taken to ensure confidentiality, integrity, and quality of data are explained.	X		X
H6	For those of above satisfied, notice is sufficiently explicit.	X		
H7	Can control when data are used for non-operational secondary use, such as marketing or research.	X	X	X
Choice or Consent:				
H8	Consent acquired before data shared with remote actor.	X		
H9	Consent is explicitly opt-in: no preticked checkboxes, etc.	X		
H10	Can choose which data types are automatically collected from sensors or other sources, for example, connect a finance app to a single bank account or track steps but not heart rate.	X	X	X
H11	Data collection consent is dynamic: if new types of data are being collected, consent is renewed *in situ*.	X		
H12	Data processing consent is dynamic: if the purpose of processing changes, consent is renewed.	X		
H13	Data distribution consent is dynamic: if the actors' data are distributed to changes, consent is renewed.	X		
H14	Consent to store and process data can be revoked at any time: with the service and any other actors.	X		
H15	Can control where data are stored.			
Access or Participation				
H16	All raw collected data can be extracted from the service	X	X	X
H17	All data are available in standard text formats	X	X	X
H18	Data extraction is available from within the service, for example, without raising a request with support	X	X	X

H19	Programmatic access to data is possible, for example, app programming interfaces are exposed	X	X	X
Social Disclosure and Usability				
H20	Privacy controls are per-disclosure, for example, individual workouts can be published to a social networking site, not relying solely on global defaults		X	X
H21	Privacy controls allow granular sharing of data types, for example, when sharing a workout, the distance can be shared but not the pace.			
H22	Error prevention: is explicit confirmation acquired before a disclosure?			
H23	Minimize user memory load: Effects of a disclosure are visible throughout the disclosure flow (ie, memory of earlier decisions not required).		X	X
H24	Minimalist: During the disclosure flow no extraneous information (such as adverts or irrelevant user interface elements) is displayed.			
H25	Consistency: Information shown during the disclosure flow is consistent with the effect of the disclosure.		X	X
H26	Help and documentation: Contextual help with making privacy decisions is available.		X	X

The comparison found that POPIA covers all the factors under the categories of notice and awareness, choice and consent and access or participation. POPIA does not cover any factors under social disclosure and usability. Fitbit covered four out of the seven factors under notice and awareness. The policy only covered one factor under choice and consent while covering all the factors under access or participation. The policy covers four of the seven factors in the social disclosure and usability category. The Apple watch policy covered five of the seven factors in notice and awareness while only covering one of the factors in the choice and consent category. The policy covered all the factors on access and participation and but only four factors of the social disclosure and usability category.

7 Discussion

The study aimed to evaluate how the privacy of user data collected using wearables is protected under POPIA when compared the individual device privacy policies. The privacy policies were evaluated making use of the heuristics framework developed by Hutton et al., (2018). The following observations were made during the evaluation.

Notice or Awareness: POPIA covered all factors relating to notice and awareness. The main focus being the explicitness of the notice of intention to collect data, the data being collected as well as the intended use of the data. Both Fitbit and Apple watch's privacy policy made a good effort to cover all

the heuristics except explicitly identifying third parties that user data is shared with as well as an ambiguity when notifying the user when the data is shared with a third party. Apple watch and Fitbit both included in their policy that user data may be shared to external organisations for further processing or for generating marketing content (Apple Inc, 2019; Fitbit, 2018). The third parties are not identified and the user is not notified when this data is being shared or when the data they are viewing has been processed by a third party. The sharing of data to third parties exposes the user data to other privacy concerns related to data in transit such as packet sniffing where data packets are intercepted and read before reaching their intended destination (Cilliers, 2019). In addition, Fitbit and Apple may not have control over the security measures to protect data or the intent of the third party when the process the data.

Choice or Consent: POPIA covered all the factors focusing on consent being obtained before collection of any data as well as the need to seek consent if any further information is to be collected from the user (Parliament of the Republic of South Africa, 2013). Apple watch and Fitbit did seek consent before collecting data, however, the use of any of their services was dependent on the user granting consent at device setup and the user had minimal choice regarding which data to give consent over. Collection of new types of data did not always require the user's consent if the collection process did not require the use of additional hardware features like microphones and sensors. Some of the services such as diagnostic services that collect user information were automatically set to opt-in unless the user opts out manually. The extension of consent to the collection of further data as well as the setting of certain data collection to opt-in by default means that unless the user has taken care to review their device settings they may be unwittingly sharing information without being aware of what they are sharing (Hutton et al., 2018).

Access or Participation: All three policies covered the access and participation category allowing the user to participate in the management of their data. However the ambiguity of ownership of the data where the data is related to the user but owned by the service provider means in some cases the user may only have limited participation in the data management (Apple Inc, 2019; Fitbit, 2018; Hutton et al., 2018). Factor in this category aim to provide users with more control over their data to ensure the integrity of their information is maintained at all times. Control of data also allows users to evaluate and reinforce privacy controls over sensitive information (Hutton et al., 2018).

Social Disclosure Usability: This category evaluated how the interface provides adequate information to the user about the information they are about to share with others. It also evaluated the granularity of the control over which information the user chooses to share. These heuristics protect the user's privacy by ensuring the user does not accidentally share information that compromises their privacy due to lack of granular control over the data disclosure process (Hutton et al., 2018). For example a jogger should have the ability to share information about their jog without sharing geographical location data related to the jog. The category also evaluate how well the interface informs the user when PII is about to be disclosed during social disclosure (Hutton et al., 2018).

Fitbit and Apple watch's privacy policy makes some effort to allow users to socially disclose their data with other users with minimal memory load. It places the burden of privacy protection of the shared information on the user while not offering granular control of the data sharing. The aim of the factors in this category is to evaluate the controls that are given to the users when they share information from their devices to social platforms. Apple watch and Fitbit provide users with controls to share individual workout routines without relying on global settings that automate future disclosure of this information.

POPIA does not cover the category related to social disclosure of information collected through wearable health devices. As discussed earlier wearable health devices, such as Fitbit and Apple watch, affords the user the ability to share their data with other social platforms either manually or automatically (Apple Inc, 2019; Fitbit, 2018). Both Apple watch and Fitbit's privacy policies were made to be compliant with European Union (EU) data protection laws, one of which is the General Data Protection

Regulation (GDPR) of 2018 (Apple Inc, 2019; Fitbit, 2018). The GDPR covers all aspects covered by POPIA as well as social disclosure issues. The act also outlines in detail its applicability and its relevance to any information related to EU citizens regardless of where the data may be collected (Botha & Grobler, 2017). POPIA is clear on its application to South African business and organisations collecting PII relating to South African citizens as well as the relevant penalties for noncompliance however, there is no prescription of its application to international organisations from outside the country that may be collecting and processing PII relating to South African citizens (Botha & Grobler, 2017). Hence, the GDPR can be used as a substitute to evaluate the shortcomings of POPIA.

8 Recommendations

POPIA was intended to protect the privacy of PII belonging to South African citizens regardless of the methods being used to collect and process the PII. Advances in technology, increases in the ways in which data can be collected as well as the volume of the data has left the act failing to cover some privacy aspects as demonstrated in the discussion above. The study has the following recommendations of how POPIA can be updated:

Extend the application of the Act to all entities collecting PII related to South African citizens.

The EU through the GDPR has made its data privacy enforceable to all entities collecting data relating to EU citizens and in doing so it has extended the protection of its citizens' privacy beyond the borders of the EU. In response to this both Apple watch and Fitbit changed the way they collect and process data within the EU in order to stay compliant with the GDPR (Botha & Grobler, 2017; Everlytic, 2018). If South Africa where to enforce POPIA to entities outside of South Africa then there manufacturers of wearables would have to comply with the requirements of POPIA around choice and consent such as the need to reacquire consent when new data is going to be collected and the elimination of default opt in options when it comes to automated data collection.

Ensure that users of wearables are allowed granular control over consent

The study recommends that the Act creates measures to ensure that users are afforded more control over the data sharing and social disclosure process in order to allowing for data sharing without compromising the users' privacy. In cases where users opt to share PII the holder of the data must also be mandated to notify the user of the potential privacy breach consequence of sharing the data before completing the data sharing process.

Afford users of wearables the right to be forgotten.

The Act must make provisions for users to choose to have all the data relating to them deleted should they wish it. Apple watch and Fitbit do allow users to delete data however, Fitbit states it may take 90 days to delete all the data while Apple watch states that there may be residual data relating to the user after deletion on their system (Apple Inc, 2019; Fitbit, 2018). With both of these services the risk to privacy continues beyond the time that the user has decided to eliminate the risk by deleting all the data relating to them.

This study also makes recommendations to users of wearables to better acquaint themselves with the privacy policies of their products and making use of the available controls to ensure their PII privacy. While most of the wearables like Apple watch and Fitbit provide controls to restrict the amount of data collected and shared it is up to the user to make use of their controls which are by default left to opt-in users.

9 Conclusion

Wearables collect process and share large amounts of PII user data which poses a threat to users' privacy. While most of these wearables provide privacy policies to the users it is necessary to have national laws protecting the user's privacy also. South Africa has POPIA as the main Act applicable to the protection of PII. However, POPIA does not cover issues related to the protection of users' privacy when there is social disclosure of their information collected through the wearables. When users choose to share their information to certain social circles or the wearables provider chooses to share that information on behalf of the user there should be safe guards to ensure that users do not accidentally share information they do not intend to share or the shared information does not result in suffering of the user. In order to enforce this there is a need to revise POPIA to include this aspect of information privacy.

10 Acknowledgements

This research project was jointly funded by the South African Medical Research Council (SAMRC) and Forte, the Swedish Research Council for Welfare, Working Life and Welfare.

11 References

Apple Inc. (2019). Legal - Privacy Policy - Apple. Retrieved May 30, 2019, from https://www.apple.com/za/legal/privacy/en-ww/

Botha, J., & Grobler, M. (2017). *A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws*. (March).

BusinessTech. (2018). These are the most popular smartwatches in the world right now. Retrieved July 16, 2019, from https://businesstech.co.za/news/technology/268621/these-are-the-most-popular-smartwatches-in-the-world-right-now/

Charara, S. (2018). Your fitness app's privacy policy may be about to change – and that's a good thing. Retrieved May 29, 2019, from https://www.wareable.com/wearable-tech/fitness-apps-privacy-policies-gdpr

Ching, K. W., & Singh, M. M. (2016). Wearable Technology Devices Security and Privacy Vulnerability Analysis. *International Journal of Network Security & Its Applications*, *8*(3), 19–30. https://doi.org/10.5121/ijnsa.2016.8302

Cilliers, L. (2019). Wearable devices in healthcare : Privacy and information security issues Wearable devices in healthcare : Privacy and information security issues. *Health Information Management Journal*, (June). https://doi.org/10.1177/1833358319851684

Everlytic. (2018). *Popi & gdpr*. Retrieved from everlytic.co.za

Fitbit. (2018). Fitbit Legal - Privacy Policy. Retrieved May 29, 2019, from https://www.fitbit.com/eu/legal/privacy-policy

Genuth, I. (2015). All in the mind [EEG]. *Engineering & Technology*, *10*(5), 37-39(2). Retrieved from https://digital-library.theiet.org/content/journals/10.1049/et.2015.0502

Haghi, M., Thurow, K., & Stoll, R. (2017). Wearable devices in medical internet of things: Scientific research and commercially available devices. *Healthcare Informatics Research*, *23*(1), 4–15. https://doi.org/10.4258/hir.2017.23.1.4

Hutton, L., Price, B. A., Kelly, R., McCormick, C., Bandara, A. K., Hatzakis, T., … Nuseibeh, B. (2018). Assessing the Privacy of mHealth Apps for Self-Tracking: Heuristic Evaluation Approach. *JMIR MHealth and UHealth*, *6*(10), e185. https://doi.org/10.2196/mhealth.9217

Inostroza, R., Rusu, C., Roncagliolo, S., & Rusu, V. (2013). Usability Heuristics for Touchscreen-based Mobile Devices: Update. *New York:ACM Press*. https://doi.org/doi: 10.1145/2535597.2535602

Kandeh, A. T., Botha, R. A., & Futcher, L. A. (2018). Enforcement of the Protection of Personal Information (POPI) Act : Perspective of data management professionals. *South African Journal of Information Management*, *20*(1), 1–9. https://doi.org/https://doi. org/10.4102/sajim.v20i1.917

Katurura, M., & Cilliers, L. (2016). The extent to which the POPI act makes provision for patient privacy in mobile personal health record systems. *2016 IST-Africa Conference, IST-Africa 2016*, (January 2018). https://doi.org/10.1109/ISTAFRICA.2016.7530595

Nur, M., Sulaiman, S., & Aman, S. (2018). *Heuristic Evaluation : Comparing Generic and Specific Usability Heuristics for Identification of Usability Problems in a Living Museum Mobile Guide App*. *2018*.

Parliament of the Republic of South Africa. (2013). *Protection of Personal Information Act, 2013 Ensuring protection of your personal information and effective access to information*. (4). https://doi.org/10.1006/brcg.1998.0994

Peltola, O. (2017). *Introduction To Wearable Healthcare Technology*. 26.

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The Rise of Consumer Health Wearables: Promises and Barriers. *PLOS Medicine*, *13*(2), e1001953. Retrieved from https://doi.org/10.1371/journal.pmed.1001953

Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., … Seneviratne, A. (2017). A Survey of Wearable Devices and Challenges. *IEEE Communications Surveys & Tutorials*, *19*(4), 2573–2620. https://doi.org/10.1109/COMST.2017.2731979

Shin, G., Jarrahi, M. H., Karami, A., & Gafinowitz, N. (2018). *Wearable Activity Trackers , Accuracy , Adoption , Acceptance and Health Impact : A Systematic Literature Review*. (September). https://doi.org/10.13140/RG.2.2.22188.10888

statista.com. (2019). Wearables: South Africa. Retrieved July 16, 2019, from https://www.statista.com/outlook/319/112/wearables/south-africa

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10766 LNCS*, 229–239. https://doi.org/10.1007/978-3-319-78105-1_27

Walker, R. K., Hickey, A. M., & Freedson, P. S. (2016). Advantages and limitations of wearable activity trackers: Considerations for patients and clinicians. *Clinical Journal of Oncology Nursing*, *20*(6), 606–610. https://doi.org/10.1188/16.CJON.606-610