On Privacy Protection of Consumer Data Collected by e-Health Devices

Vladimir Stanisavljevic
University North, Croatia
Bruno Tekic Sauerborn
University North, Croatia

Abstract

The non-certified e-health segment is gaining momentum around the world. The trend was significantly advanced by the introduction of several sports and medical measuring devices in the form of smartwatches. There has also been a resurgence of other medical Internet of Things class devices. Several devices connect to a product or platform-specific online (Cloud) service for storing, exchanging, analysing and monitoring the customer-collected e-health data. The devices and the data collected allow the consumers to continuously track their sports achievements, movement, vital signs, essential health state, etc. while receiving some recommendations and warnings based on the measurements. As some recent examples showed, the data collected can contain sensitive information that could be used creatively and unexpectedly, either positively or negatively. Unlike professional healthcare systems, which should comply with the strict GDPR, there is much less pressure on commercial entities in the consumer technological sector to provide more privacy options for data collection through their devices. In this work, we analyse the data typically collected by consumer e-health devices and assess possible risks that commercial entities present to their customer in unauthorised use of the data for their commercial advances. They use obscure legal language to prevent users from consenting to various data usages while providing primary data storing functionality. Moreover, there is a significant risk of using the data for repression in some contexts. We analyse the sector's current state and provide some recommendations to consumers and legislation to improve consumer rights to privacy while enhancing their health. At the same time, we recommend how the professional health sector should benefit from the collected data to improve their operations.

Keywords: GDPR; Cloud services; e-Health; smart-watches; IoT
JEL classification: I11

Paper type: Research article
Received: 10 March 2023
Accepted: 1 September 2023

DOI: 10.54820/entrenova-2023-0013

Introduction

In just a few years, the rapid rise of communications and processor chips associated with ever-increasing and efficient mobile processing power and availability of cheap and reliable sensors for various purposes resulted in a much wider adoption of consumer mobile devices for monitoring health, sports achievements, and other individual wellbeing (Reeder & David, 2016). An example that is slowly but steadily gaining attraction among the general population is former sports watches that were transformed into so-called smartwatches in an analogy to mobile phones (Rawassizadeh et al., 2015). Accordingly, instead of just one sports-related function, they now have a much larger application set. In a few years of intense development, they have now been used for simple timing and organisational tasks by more serious sportspersons and for continuous casual recreational activity monitoring. Data from a device could provide new health-related benefits by providing detailed insight into preferred activities and by inspiring users to do more activities until they achieve some health-benefiting goal or motivation through interaction with other persons practising the same activity. For example, all modern mobile phones count the steps a person takes in a day, and the platform can alarm or praise users about their (in)activity. There are also similar wearable medical devices that track and log various vital signs and exchange data and user achievements with friends to inspire them and other users into other recreational activities like hiking, walking, running, cycling, swimming, rowing, tennis... The activity could even be broadcast to a much wider public.

Many health devices are extended with communication capabilities or send data to nearby mobile phones, which provides a better and larger user interface. In a way, they resemble Internet of Things (IoT) devices that are usually not much than a simple sensor equipped with a means to transfer data further, usually wirelessly, via Near Field Communication (NFC), some other specialised wireless protocol, or standard Bluetooth Low Energy (BLE) or a Wi-Fi. Some e-health sensors use ANT+ protocol to transfer data to smart-watch. Their primary goal is to provide a better analysis of the data. The whole segment of various electronic devices is sometimes called e-health and, in its mobile version, *MHealth* (World Health Organization, n.d.).

On the other side, the technological sector nowadays finds a big chunk of its income in so-called surveillance capitalism (Power et al., 2022). We witness a big initiative from companies of all sizes to collect and monetise data about users for advertising purposes. There is certainly a real concern for health data like in other medical systems (Laric et al., 2009) of many privacy breaches like for other web services that, In the end, resulted in the introduction of the EU General Data Privacy Regulation and similar legal acts in other countries. Even with that regulation in place for many years, we witness that big social networks continue to harvest user data and accept to pay fines from time to time.

Several new ideas and device categories are introduced continuously through various investment cycles and technology exhibitions. The growing number of users of various devices and the recent trend to convert them into United States Food and Drug Administration (FDA) approved devices ensure that the technology has a great future that will accelerate innovation to cover new health-related measurements by consumers.

However, there is a strong indication that besides the corporate surveillance that utilises collected data mostly for advertising, the data could be used by legislation enforcement agencies where some medical procedures that follow the indication could be punished legally (Hoel & Chen, 2018).

The structure of the work is as follows. In the first chapter, we will disseminate what health-related data is currently possible to acquire by e-health devices and platform

support by mobile operating systems, with more details on smartwatches. In the following chapter, we provide a brief introduction to basic privacy rights in accordance with the EU General Direction for Privacy Guidelines (GDPR). In the following chapter, we will examine what producers are now doing to avoid the directive and the possibility of the misuse of the user data. In the next chapter, we make an analogy to other studies for general health information systems and some possible scenarios that can be used. In conclusion, we provide some guidelines to users and producers of the equipment to avoid some illegalities.

Health Service Platforms and Smart Watches

By combining a mobile phone with a smartwatch or other wearable but wirelessly connected sensor, users can now easily continuously track walking distance, breathing, heart rate, ingestion, glucose level, blood pressure, oxygen levels in the blood, and other health and well-being-related data.

Mobile operating system support for health applications

Most contemporary smartwatches work best in association with compatible mobile OS (for example, Apple Watch integrates only with Apple iOS while Android Wear OS for smart-watches works only with Android OS). The reason for this is mobile operating systems (OS-es) which now provide elaborated *Application Programming Interfaces* (API) that can integrate various sources of health data to a unified place (combination of local but cloud synchronised storage) that can be later shared even with some medical institutions or for research. Examples of health data aggregation platforms are Google's Android Health Connect, Apple's iOS Health Connect, Garmin Health and now defunct Microsoft HealthVault. Smartwatches use a specialised operating system that is compatible with the platform through provided APIs. They can gain access to the platforms after user authorisation and later store data safely on the platform. Stored health data could be categorised into a large array of specialised groups that ease later data segmentation analysis and exchange with medical specialists.

Current measurement capabilities of smartwatches

The most significant category of wearable devices that can measure and store health data is certainly smartwatches. Besides all other computing and general purpose capabilities, these watches were initially primarily purposed to improve consumer fitness by tracking daily activities and providing historical data and thus additional motivation through gamification, social networking or simply just after achieving some goals or in interaction with other users. Garmin and Fitbit, as companies, developed various specialised lines of watches for different sporting activities and, over time, moved to more general-purpose devices while other producers chose the opposite path bonded to their own or ubiquitous Android operating system. Samsung, for its very successful line of smartwatches, started using its own OS and health platform but, over time, migrated to Google Android Wear and Google Health platform. Various devices implement a number of different techniques to measure vital signs and other activity data (mostly based on accelerometer and GPS) that can be used as health data.

Consequent device updates introduced new sensors and capabilities regularly (usually yearly). That diversity provides ample opportunities for privacy breaches for various applications that have access to the collected data. Every application can ask a user to access a particular block of data, and users are quite keen to approve that.

Table 1 summarises typical representatives of some popular producers. Readers should refer to our other works for more detailed information on a particular measurement method or device.

Table 1
Measurement capabilities of some smart-watches

Producer	Apple	Fitbit	Garmin	Samsung	Huawei	Xiaomi
Model	**Watch S7**	**Versa 3**	**Epix 2**	**Watch 4**	**Watch 3**	**Amazfit Bip U**
Pulse oximetry	+	+	+	+	+	+
Breathing rate			+	+		
HRM	+	+	+	+	+	+
EKG	+		+			
Blood pressure		+	+	+	+	
Body temperature		+				
Stress level			+	+	+	+
Sleep quality apnoea detection		+	+	+	+	+
Pedometer	+	+	+	+	+	+
Fitness tracking	+	+	+	+	+	+
Calory consumption	+	+	+	+	+	+
Menstrual cycle			+	+		
Fall detection	+					

Source: compiled by authors from various product data sheets

Other e-health devices

Smart-watches are the biggest part of e-health devices, but they are limited to their form factor and fixed position to the body that can provide only a limited set of measurements. Besides them, there is a growing market for non-medical hearing devices in the form of earbud headphones. Some of them, with their noise-cancelling capabilities, are promoted as hearing aids. It is expected that more sensors will be added to the earphones. Several applications provide some hearing tests using headphones. Many other devices for measuring weight and blood pressure almost universally have accompanied mobile apps and communicate over NFC or Bluetooth. The data is transferred and processed on the phone. Some of them provide advanced local or external data analysis through mobile phone OS or providers or third-party machine learning/artificial intelligence (ML/AI) systems. For example, they can trigger alarms or notify local emergency medical services of falls, car crashes or heart-stroke events. Coverage of all other e-devices by far exceeds the space of this article and will be skipped.

Just a few examples from a recent winner of CES (Consumer et al.) in Las Vegas is a smart toilet that analyses human excrement to provide a better understanding of gut biome and related problems. There are various new continuous glucose monitors - GCM (U.S. Department of Health and Human Services , n.d.) for continuous blood sugar level monitoring that was previously used only by diabetes but now is used much more for sports advancements like in Supersapiens that uses Abbott Freestyle Lybre sensors (**Pogreška! Izvor reference nije pronađen.**). The device uses an inserted needle a

nd transfers data by NFC. According to some published research, there is a growing interest in the development of wearable devices that will monitor glucose levels by a non-invasive method. However, accuracy is still questionable (Klonoff, 2021).

Almost all new e-health-related devices provide their service or integrate into mobile OS health services to collect, store and analyse data and eventually trigger some responses to users, medical institutions or third-party services. They mostly require the installation of a producer mobile application and agreement to their terms of service before use.

GDPR and Digital Services Act regarding e-health devices

There is a long-standing issue between internet companies that monetise user data and the European Union General Data Protection Regulation (EU-Lex, 2016). Besides GDPR, another European Union directive regarding online services and markets has been introduced (European Parliament, 2022). As they state on the introductory page: "the Digital Services Act (DSA) and the Digital Market Act (DMA) form a single set of rules that apply across the whole EU. They have two main goals:

1. to create a safer digital space in which the fundamental rights of all users of digital services are protected
2. to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally."

They intend to regulate large services for 10% of Europe's population (the limit is 45 million users), and there is little mention of e-health services. However, although many e-health devices rarely reach such a large audience (Värri, 2023), some of the existing platform services. For example, Amazon, Apple's HealthKit, Google Health, and FitBit platforms could fit the limit as a platform but not as an active user base. More specialised devices are far from the limit. Interestingly, the Act obliges service providers to provide researchers with much more insight into the data they store and the algorithms they use.

In further text, we will examine the problems consumers, producers, and regulators face in fulfilling GDPR requirements. By GDPR, personal data collected by smartwatches and other e-health devices should only be used for purposes that are clearly communicated to the user. Such consent is usually provided to a user in the form of lengthy Terms and Conditions (T&C). Some research has shown that users of websites do not read them but accept them and go on and that designers of websites use many deceiving techniques to achieve even greater acceptance ((Utz, 2019). Furthermore, data stored should not be repurposed for other unrelated activities without obtaining further consent, and this is usually hidden in the consent. Other aspects of the use of the data are equally muddied and somehow legally covered within the Terms. Our examination of some e-health devices and associated web services or mobile applications has shown that almost all do not work completely without user consent. They limit almost all services if a user restricts the use of the data in accordance with GDPR. Moreover, the consent covers various non-essential data use!

By (Shastri et al., 2016), this is like several ways information system breaks GDPR compliance. However, in the case of medical data, there is still no conclusion on how the younger generations will change their attitude towards privacy as they age, as is noted elsewhere (Laric et al., 2009). Possible privacy problems with e-health data are not as benign as targeted advertising consumers face daily. As legislation in some countries changes, some could find that just recently, perfectly legal procedures like abortion suddenly became legal offences in some US states.

Privacy concerns for e-health platforms and applications

In exchange for fulfilling the basic needs of the technological infrastructure, ethical principles and the sharing of personal data services are also needed. This mostly conflicts with an application in a hospital environment or for health institutions that are obliged to patient privacy and GDPR by legal binds. However, even in such environments, there are privacy concerns regarding health information. There is growing research in relation to how users of various online systems perceive the privacy of digitalised and online accessible medical data, and (Utz et al., 2019) describe various methods applied by sites to avoid or lure users into accepting all proposed tracking methods based on cookies simply by making a choice to complicated. They do not distinguish data stored on the device for application purposes from the user's location and other data. In the previous chapter, we showed what the devices can measure and how they could be used in health applications to detect some health issues. Moreover, the data could be used or misused. (Kenny & Connolly 2016), There are a few major categories of health information privacy concerns that patients use in health information systems. They are summarised in Table 2.

There is a growing interest in research on the consumer approach to GDPR-imposed restrictions and privacy settings. We extended the original table items with our observations about smart-watch applications and associated services. Our further intention is to do the same for the data on the device or associated cloud and other services for many popular m-health services. To start, we investigated privacy in the smartwatch, but there is no big difference when the concerns are applied to other connected medical devices in the health sector.

Usually, we can generalise that when the services are free or freemium, this is the place where the surveillance economy usually starts. However, this does not stop producers from having most of the income in selling devices to subsidise them by selling user personal data for advertising. We examined a few popular health device applications on app stores, and they state in the application manifest on the relevant App store that they collect various data without providing details about third-party data use.

Smart-watches may be the fastest growing segment of e-health devices, but they still lack the rigidity of testing of certified medical devices. Although some of them for certain measurements already have US government Food and Drugs Administration (FDA) approval, that approval has no concerns about the data use. There is a growing research interest in the use of so-called Patient-Generated Data, and the FDA certification process of many various devices is not as strict even for basic use as it is for drugs. Moreover, US FDA requirements for certifying any medical device do not specify any requirements on collected data, neither on formats or later exchange. FDA should include some restrictions on later data use as part of the certification process.

We examined a few popular health device applications on app stores, and they state in the application manifest on the relevant App store that they collect various data without providing details about third-party data use. Mobile platform APIs are much stricter in data use than individual applications. The certification could be simplified if a device is bound just to the mobile platform API. Now, they use and sometimes even seem to scam data collected by other applications, and it does not work if it is not connected to their applications.

Table 2. Major privacy concerns for health systems

Data privacy concerns	Description	Smart-watch relevance
Collection	An individual's concern regarding the collection and storage of large quantities of their health data.	In general, this is required for basic functionality, but data is much more personalised from other data sources, such as the device and associated phone and user account.
Unauthorised Secondary Use	An individual's concern is that their health data, collected for one purpose, is used for another purpose without their permission.	This is the biggest problem, as large terms and conditions usually muddy the acceptance and do not distinguish other data uses.
Improper Access	An individual's concern is that an organisation cannot prevent unauthorised individuals from accessing their health data.	There is always a problem with using the data in a wider political or law-enforcing context. Local access to data on the platform is limited, but problems arise when there is also an external service that further accesses and processes data.
Errors	An individual's concern that organisations do not have measures in place to prevent and correct errors	As for most users, this is casual data collection. They are not that concerned, but the platforms and associated cloud services have a good perception of reliability among users.
Control	Individuals are concerned that they cannot control their health data.	In the case of monitoring serious illnesses and by age, the concern increases.
Awareness	An individual's concern that they lack awareness of how their health data is used and protected.	It is valid for all internet services, and users who decide to use some service do not usually care.

Source: extended table from (Kenny & Connolly, 2016)

Conclusion

In this work, we analysed trends in the consumerisation of the collection of health and fitness-related data, as with many other things coming from big technological companies and cheap, mass-produced replicas; privacy protection lags behind the legal protection of consumers' rights. The sector uses very similar techniques in avoiding GDPR and similar techniques for forcing user consent and data sharing, as on other Websites. As the data collected contains more sensitive private data that can be used, not just by targeted advertising, but by limiting employment rights, it adds some financial burden on the da legal enforcement agencies in a totalitarian context. Our suggestion in regulating data collection is to treat them and limit exchanges, as in other medical research areas where patient-doctor confidentiality is paramount and FDA certification includes data privacy concerns. All other data use should not limit device or associated service functionality with or without consumer explicit approval. Default, in all cases, should be absolute anonymisation of the data without tracking and profiling the user and use of the data for other purposes or

sharing the data with simple data choice. Mobile OS API should guarantee the anonymisation process. As some recent examples have shown, the data collected can contain quite sensitive information that could be used creatively but also in many unexpected ways, either positively or negatively. Unlike the professional healthcare devices used for measurements in controlled environments, which should comply with strict doctor-patient confidentiality, there is a lot less pressure on commercial entities in the consumer technological sector to provide more privacy-inclined options for data collection and storage. Our further research plan is to perform a technical analysis of privacy breaches in e-device mobile applications and mobile platform-provided health API-s like in the (Liu et al., 2022).

References

1. U.S. Department of Health and Human Services, n.d. *NIH: National Institute of Diabetes and Digestive and Kidney Diseases.* [Online] Available at: https://www.niddk.nih.gov/health-information/diabetes/overview/managing-diabetes/continuous-glucose-monitoring
2. David C. Klonoff, K. T. N. N. Y. X. a. M. A. A., 2021. Noninvasive Glucose Monitoring: In God We Trust—All Others Bring Data. *Journal of Diabetes Science and Technology,* 15(6), pp. 1211-1215.
3. Hoel, T. & Chen, W., 2018. Privacy and data protection in learning analytics should be motivated by an educational maxim—towards a proposal. *Research and Practice in Technology Enhanced Learning,* 12.13(12).
4. Värri, A., 2023. The impact of the EU Digital Services Act and Digital Markets Act on health information systems. *Finnish Journal of eHealth and eWelfare,* 4.
5. European parlament, 2022. *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).* [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32022R2065
6. Tekić Sauerborn, B., 2022. *Zaštita privatnosti bio-medicinskih podataka prikupljenih pomoću pametnih satova (in Croatian).* [Online] Available at: https://repozitorij.unin.hr/islandora/object/unin:5083 [Accessed 5 2023].
7. Rawassizadeh, R., Price, B. A. & Petre, M., 2015. Wearables: Has the Age of Smartwatches Finally Arrived?. *Communications of the ACM,* January, 58(1), pp. 45-47.
8. World Health Organization, n.d. [Online].
9. Reeder, B. & David, A., 2016. Health at hand: A systematic review of smart watch uses for health and wellness. *Journal of Biomedical Informatics,* Volume 63, p. 269–276.
10. Kenny, G. & Connolly, R., 2016. *Drivers of Health Information Privacy Concern: A Comparison Study.* San Diego, s.n.
11. Shastri, S., Wasserman, M. & Chidambaram, V., 2016. *The Seven Sins of Personal-Data Processing Systems under GDPR.* s.l., s.n.
12. EU-Lex, 2016. Regulation (EU) 2016/679 Of The European Parliament And Of The Council. *Official Journal of the European Union*, 27 4.
13. Utz, C. et al., 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field.
14. Guardado, S., Isomursu, M. & Giunti, G., 2022. Health Care Professionals´ Perspectives on the Uses of Patient-Generated Health Data. In: *Challenges of Trustable AI and Added-Value on Health.* s.l.:European Federation for Medical Informatics (EFMI) and IOS Press, pp. 750-754.
15. Laric, M. V., Pitta, D. A., Baltimore & Katsanis, L. P., 2009. Consumer Concerns For Healthcare Information Privacy: A Comparison of US And Canadian Perspectives. *Research In Healthcare Financial Management,* 12(1), pp. 93-111.
16. Liu, K. et al., 2022. Evaluating the Privacy Policy of Android Apps: A Privacy Policy Compliance Study for Popular Apps in China and Europe. *Scientific Programming,* Volume 2022.

About the authors

Vladimir Stanisavljević is a senior lecturer at the University North in Croatia, and he's also the principal investigator in his private company. He earned his master's degree in computer science from the University of Zagreb's Faculty of Electrical Engineering and Computing. His teaching portfolio includes computer technology, information management, IT technologies, medical informatics, computer programming, and various operating systems. Vladimir possesses extensive research and industry expertise, particularly in computer vision systems, telecommunications, traffic management, and printing. He has worked as a researcher, system implementor, programmer, consultant, and educator. The author can be contacted at **vladost@unin.hr**.

Bruno Tekić Sauerborn was a bachelor student of Nursing at University North. Now, he is a Master of Business Administration student. He is passionate about computers, mobile devices, and wearable technology, especially video games and their development and business management. He has working experience in customer support and as a manager.