Privacy Protecting Fitness Trackers: An Oxymoron or Soon to Be Reality?

Kaja J. Fietkiewicz(✉) and Maria Henkel

Department of Information Science, Heinrich Heine University Düsseldorf, Düsseldorf, Germany
{kaja.fietkiewicz,maria.henkel}@hhu.de

Abstract. The rapid technological advancements are supposed to simplify our everyday life. They are also increasingly utilized to support an active lifestyle with diverse tracking devices, like fitness trackers or smart watches. However, they do not seem to make the life of legislators and data privacy advocates easier. In contrary, with better and faster technology our (health-related) private data faces more and more threats. To better understand the current status of the intersecting domains of devices like fitness trackers and the data privacy, we have analyzed the development of general data privacy regulations in the EU as well as the data transfer modalities between EU and USA. Afterwards, we reviewed scientific publications on fitness trackers (or smart watches) and data privacy, in order to identify, whether there is interest in this topic among scholars and if so, which aspects do they investigate in particular.

Keywords: Fitness trackers · Data privacy · GDPR · Privacy Shield

1 Introduction

New technological advancements like smart and wearable devices or the Internet of Things (IoT) simplify not only our everyday life, but also "the tracking and logging of data" in order to support an active lifestyle [17]. Such fitness trackers are getting smaller and more affordable [17], while offering more and more options to track our health and activity. This is possible due to the economies of scale that drastically reduced the costs of production, whereas "concurrent advances in technology have expanded their physiological recording capabilities" [22]. In turn, they are also increasingly employed in medical field [4].

However, some of the (prospective) users are having privacy concerns and "sensitivity regarding data gathered with wearables" [17]. One could say that "personal information has never been this prone to risk given the current advancement in technologies especially in personal devices" that collect vast amounts of data, which in turn could be used to "infer sensitive personal information" [30]. Before this new technology became an integral part of many people's lives, personal health-related information was exclusively stored in hospitals or health care provider's systems [16]. One could argue that the information stored in a fitness tracker is even more thorough. The devices can meticulously record the number of steps we took, the geo-locations of where we did it, the calories we burned during this activity and how well we slept

G. Meiselwitz (Ed.): SCSM 2018, LNCS 10913, pp. 431–444, 2018.
https://doi.org/10.1007/978-3-319-91521-0_31

afterwards. The number of potential ways of utilizing all the data is rising with its amount and diversity.

The "problem" with privacy and data security is not new and is becoming more and more urgent with increasing digitalization. It is especially present in the context of the web and social media. One way to counteract or at least regulate the handling of personal data is an appropriate legislation [12]. Of course, in times of digitalization and globalization it is not enough to regulate data privacy solely in one's own country. Transnational corporations are active in many parts of the world and not every country can necessarily ensure an appropriate consumer protection. For example, smart watches or fitness trackers by Apple or Fitbit are very popular on the European market; however, their headquarters are located in the USA. How is the transitional data exchange regulated?

On May 25th, 2018, the General Data Protection Regulation (GDRP) will be implemented and might improve the current status of data security in Europe. It is intended to unify the data protection within the European Union and make it stronger as compared to the former data protection directive from almost 25 years ago. The regulation will be enforceable after two-year transition period, directly binding and applicable. The applying lex loci solutions ("law of the place of performance") means that even though the new regulation is applicable within the EU, it will also concern non-European companies, as long as their services or goods are being supplied on the European market. Ergo, it will also concern non-European fitness trackers' producers.

The increasing interest in data privacy can be recognized not only in the legal environment but in the scientific research as well. A search in the Scopus database (for peer-reviewed literature) for publications on data privacy and the Internet in general (Fig. 1) shows increasing number of publications on this topic, with a quite significant increase since 2013. Which aspects of data privacy in the context of fitness

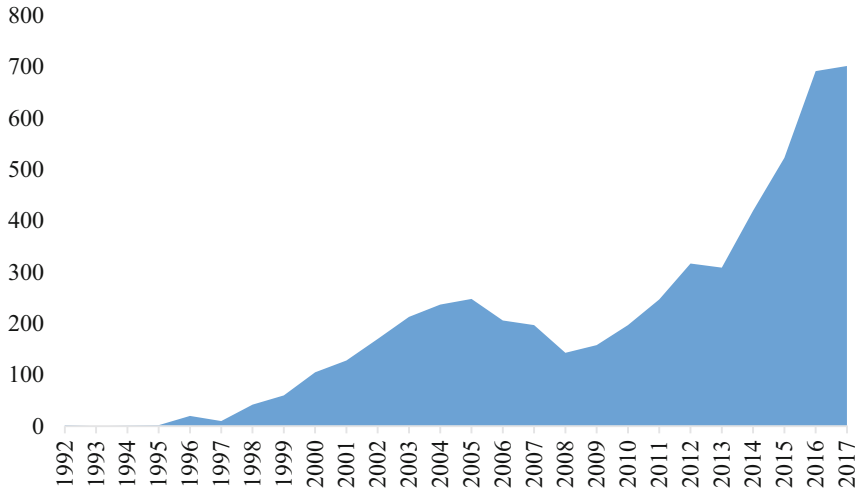

Fig. 1. Number of publications on privacy and the Internet indexed by Scopus.

trackers are the researchers interested in? What methods do they use? And, do they refer to legal sources?

This theoretical study (Fig. 2) is supposed to shed light on the status of (health-related) data privacy regulations, which also increasingly concern the manufacturers and service providers of fitness trackers. Hence, the first research question is (RQ1a): What is the legal status quo of data privacy in European Union with focus on fitness trackers? Also, since many manufacturers and services providers are located in the USA, the following question arises (RQ1b): How is the data transfer between EU and USA regulated? Finally, we want to take a look at the research trends on this particular topic and therefore formulate the final research question (RQ2): What is the state of scientific research on data privacy and fitness trackers?

Fig. 2. Scope of our theoretical research.

2 Methods

The research procedure for the first part of this paper, the legal perspective, included literature and internet research. The basis for the following discourse is composed of US-American and EU legal regulations, reports and press releases by authorities, scientific articles (focused on law and economy), and news articles by renowned news outlets.

The second part of this work includes a review of scientific literature on data privacy and fitness trackers. To identify, analyze and synthesize relevant research in this particular field, a structured literature review was conducted. Therefore, we looked for publications focusing on both, data privacy, security or protection and fitness trackers or smart watches (Fig. 3). As shown in Fig. 3, these topics have only been combined in scientific research since about 2015. There is much more scientific interest in the intersection of social media and data privacy, as well as the new General Data Protection Regulation itself (not related to fitness trackers or similar devices). Therefore, it is no surprise that our search in the two scientific databases "Web of Science" and "Scopus" yielded a total of 23 results as of February 2018.

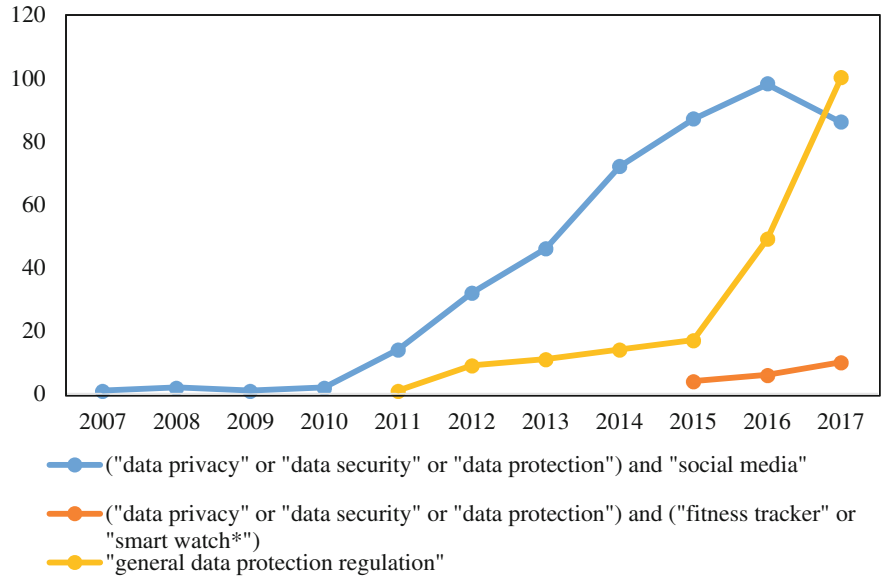

Fig. 3. Number of publications per year on privacy and social media, privacy and fitness trackers or smart watches, and on the GDPR, indexed by Scopus.

Articles included for our review had to be directly relevant to the topic and peer reviewed. We included results regardless of the age of the material, country of origin or language. We did not limit our search to theoretical, qualitative, or quantitative research as the sample was small to begin with. We excluded, however, four articles, because they were deemed irrelevant for our research question, due to either focusing on another, very specialized topic or using one of the keywords as a negative keyword, hence, expressly not talking about it. Nine articles were of a technical nature, documenting or discussing the development of a system or technical solution for data privacy in wearable technology and were excluded as well. The remaining ten articles, eight in the English, one in the German and one in the Turkish language, were analyzed regarding theories, methods and results concerning privacy and privacy protection of health data generated by wearables.

3 Results

3.1 Legal Perspective

The technological development "makes it possible for companies to collect, process and interlink data in an expanded way. They increasingly tend to use these data for various purposes, such a personalized services and marketing. As a result of technological development, along with globalization, new and increased challenges for personal data protection laws emerged" [21, 28]. The increasing privacy risks may in turn

decrease people's trust in companies that collect data for their services and this "lack of trust can slow down the development of the innovative use and adoption of new technologies" [21, 28]. Especially when such sensitive data like health information is involved, the new technology brings as many possibilities as it does bring fear about one's most intimate sphere. Great advances in Big Data technology facilitate development of personal health management, health care delivery, health-related research and population health surveillance. Until now, the legal system was lagging way behind these technological and commercial developments [18], whether we look at the countries with common or with the civil law traditions. Most of the privacy protection regulations for (health-related) data "were drafted in the twentieth century for technology available at that time (…) and are outdated in the era of Big Data" (e.g. Data Protection Directive 95/46/EC; Directive 2002/58/EC; Data Protection Act 1998) [18]. However, there is still hope that the privacy and other "fundamental rights of data subjects" can be safeguarded [18, p. 38] and many voices in the literature and in the politics see the new European General Data Protection Regulation (GDPR) as the game changer.

The focus of this research paper is set on the so-called fitness trackers or similar wearable technology that enables monitoring of physical activity, sleep pattern, heart rate etc. This data does not strictly fall into "health information" collected in the medical field, but still with its increasing spectrum (including geolocation, name, IP address, email, phone number, social network, etc.) one can create a quite accurate image of one (quantified) self. Therefore, the concerns about the data privacy, personality rights and the (imminent) danger of mass surveillance might be justified.

Legal Concerns Regarding Fitness Trackers. In 2016, Norway's Consumer Council (NCC) accused Fitbit (USA), Jawbone (USA), Garmin (Switzerland) and Mio Technology (Taiwan) of braking local laws governing the handling of consumer data [2, 33]. Even though Norway is not an EU Member State, it needs to implement some of the European directives, including the Data Protection Directive from 1995. This means that the potential data privacy violations concern, at least from the legal perspective, the whole European economic zone. According to NCC, the companies gathered too many data, did not disclose how many third parties have access to it or how long it will be kept. In general, "anyone who used them [fitness trackers] gave up data on asymmetrical and obscure terms" [2]. This way the basic privacy principles are being neglected and the accumulated information can be "exploited for direct marketing and price-discrimination purposes" [2].

The complaint was based on NCC's analysis including an examination of the functionality of the trackers, the terms and conditions, privacy policies and the degree of control provided to users over the data collected [33]. Further allegations included the lacking provision of the users with proper notice about changes in terms and conditions or insufficient explanation of how data, including sensitive personal data such as heart rate, is collected and shared with third parties [33]. In general, since this type of technology is still evolving, the NCC advises incorporating consumer-protective measures in the product design as a standard in order to enhance consumers' trust [33]. This "privacy by design" will be inevitable for companies targeting European market anyway, when the General Data Protection Regulation is in force.

The concerns about privacy and personality rights relate not only to private consumers but increasingly to the corporate environment as well. The new trend for corporate wellness or corporate health management (aiming at improved employee health and lower medical insurance premiums) could be very lucrative for fitness tracking manufacturers and service providers. However, with the new regulation in sight their business model could face some obstacles. According to the EU advisory panel, employers should not be allowed to issue workers with fitness trackers or similar monitoring devices and should "be barred from accessing data from their devices their employees wear" [14]. For the authority, even a transparency regarding the usage of the data and the possibility of opting out of any data sharing are not sufficient, since "given the unequal relationship between employers and employees, (…) workers were probably never able to give legally valid consent to have their data shared" [14]. According to the new GDPR, for any kind of employee tracking, the businesses should select the most data privacy friendly solutions available [14]. Time will tell, which of the fitness tracker providers (if any) will be the chosen one.

In 2016, the German Federal Commissioner for Data Protection and Freedom of the Information also shared some concerns about the personal data while using fitness trackers [3]. Again criticized were the terms and conditions of the manufacturers and service providers for their form and vagueness, as well as the fact that, to some extent, the data is being shared with third parties (for marketing or research purposes) and its faith does not really remain in consumers' control anymore. Finally, the consumer often does not have the possibility to autonomously erase all the accumulated data linked to his or her account. The authority also sees the new GDPR as future solution for all these concerns.

Most of the popular fitness tracker manufacturers are based in non-EU countries. Therefore, another critical point in the debate on data privacy is the data transfer outside the European Union, for example in the USA (hosting headquarters for many of the big market players). When supplying the EU-market, companies need to comply with European data protection regulations. When transferring data from EU, it must be ensured that it will be equally "protected" at the new destination. In the following, a short comparison of data privacy principles in the USA and EU will be presented to point out that such transfer, given the status quo of data protection legislature, is not unproblematic.

Data Privacy Regulations in the USA and the EU. Terry [26] argues that the current developments in consumer electronics including wearable devices are "disrupting healthcare data markets by encouraging consumers to themselves collect and curate data," which in turn reveals the shortcomings of provided healthcare data protection and, especially, the flaws of domain-limited data protection that is prevalent in the USA. This is one of the biggest differences between the US and the European data protection regulations that are not limited to one specific domain. The data privacy laws can be compared regarding three aspects: the horizontal reach (public and private domains that are being regulated), vertical attributes (what data custodian behaviors they regulated), and their enforcement (investigation and penalties) [26].

When considering the European General Data Protection Regulation, it has a very broad horizontal and vertical applicability. As for the horizontal reach, it concerns all sectors of the economy (not only, e.g. the health-related domain) and all "personal data" as well as all stakeholders controlling or processing it. As for the vertical attributes, the "Fair Information Practice Principles-like protective standards [apply] throughout the lifespan of data" [26]. Terry describes two phases of possible interaction with data—the "upstream" (when the data is being collected) and the "downstream" (the subsequent data processing and/or disclosure). The GDPR aims at protecting the personal data during both phases. The data collection (upstream) needs to be limited to a legitimate purpose and as minimized as possible. The data processing (downstream) needs to be fair, lawful, transparent, and it should follow certain storage, quality, security, and integrity as well as confidentiality limitations [26].

In comparison, most of these data protection principles are absent in the US laws, starting with a quite limited horizontal protection [26] (sector-by-sector basis regulation, with different statues for the public and private sector) [24, 28]. Furthermore, it is also very limited in its vertical reach, since most of the regulations only utilize downstream protection (hence, regulate what happens with the data after it was collected), such as confidentiality security and breach notification [26]. Terry names HIPAA (Health Insurance Portability and Accountability Act of 1996) as one of the typical US data protection laws. HIPAA is domain-specific, the domain being defined by the healthcare data custodians (the health insurers and health providers) and not by the data type (e.g., healthcare data) and provides only downstream protection [26]. This leads to a quite big gap in the protection of health-related (personal) data, since the regulation does not apply to most of the healthcare data controlled or processed by entities outside the traditional healthcare environment [26].

The need to close this data protection gap can only become more urgent, when we consider the current trends in the health/lifestyle sector. As for 2016, approx. 200,000 mobile health apps were available for smartphones, of which a not insignificant part interacts with wearables [26, 27]. However, relatively few of these products are supplied by "traditional healthcare providers" so that the data will not be protected by HIPAA's privacy rules [25, 26]. That is why the data privacy regulations in the US are not as comprehensive as they are in EU. Therefore, the question arises, how is the data transfer between USA and EU regulated? And, does it provide adequate protection? Next, a short history of trans-Atlantic agreements for data transfer and some data privacy disputes, which helped shape the GDPR, will be presented.

A Quarter Century of Data Protection Faux Pas. In May 2018 the General Data Protection Regulation will come into effect and after almost 25 years replace the Data Protection Directive. In contrast to the directive from 1995, the new regulation is immediately applicable and enforceable in every EU Member State. An EU directive only sets certain requirements and goals that need to be implemented by Member States in their legislature. With the new regulation, the data controllers and processors will be "required to emphasize transparency, security and accountability, while (…) standardizing and strengthening the right of European citizens to data privacy" [19].

The European Commission made the initial proposal of the new regulation in January 2012 [8]. "A critical observer might note that the ideas behind the Regulation and the Directive go back to 2012 and that already all circumstances within which they were drafted have in the meantime changed substantially" [7]. However, during this time the European Court of Justice ruled in several cases leading to fundamental decisions within data privacy case law (e.g., right to be forgotten, extraterritoriality, international data transfer) [7] that pointed out important data security and privacy issues and helped shape the new GDPR (Fig. 4).

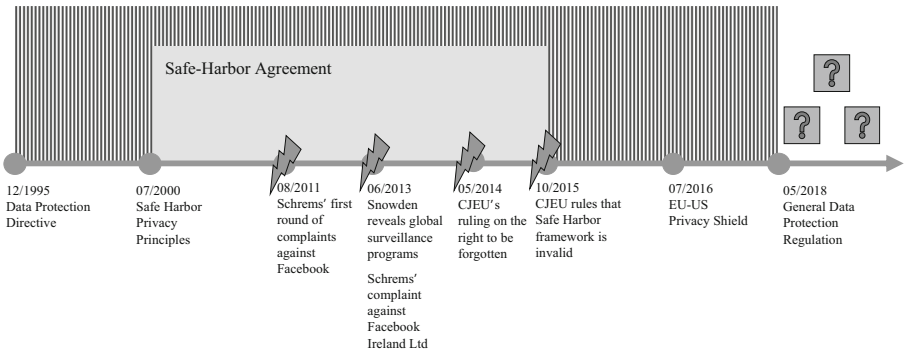

Fig. 4. Data Privacy regulations and selected disputes in the EU since 1995.

Some of the turning points were Edward Snowden's disclosure of the large-scale espionage by NSA, also targeting European personal data, or Max Schrems' campaign against Facebook, which lead to more questions about handling of European personal data by Apple, Skype, Microsoft and Yahoo! [15]. After the European Court of Justice ruled in Schrems' favor, the international Safe Harbor privacy principles (agreed upon by European Commission and the US authorities) regulating data exchanges between Europe and the US, were overturned by the European Court of Justice [15]. Apparently the agreement enabled US public authorities' interferences with the fundamental rights of persons by accessing their data [28].

The US-EU Safe Harbor program was developed in the year 2000 in order to bridge the "differences between the US and the EU data protection approaches and to provide US organizations with streamlined means to comply with" Data Protection Directive from 1995 [28]. In 2016, less than one year after the Safe Harbor agreement was overruled, the European Commission and the US Government agreed on a new framework for data exchange, the EU-US Privacy Shield. From the beginning it was challenged by civil rights organizations and privacy groups. The Privacy Shield framework includes updates of the former Safe Harbor framework to fulfill the requirements set by the CJEU's ruling [28]. Since then, USA is within the countries recognized by the European Commission as providing "adequate" protection for personal data (limited to the Privacy Shield framework) [10, 31]. Other countries that the European Commission has so far recognized are Andorra, Argentina, Canada

(commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay [10].

The GDPR requires the European Commission to regularly review its adequacy decisions. This is one of the improvements implemented due to the Schrems' case. Until Schrems' action, the Safe Harbor agreement "had never been subject to an actual review by the Commission" [31], adding up to 15 years of insufficient data transfer regulation being in force. The European Commission evaluated its adequacy decision approximately one year after the agreement was reached in an annual report and, as for October 2017, it confirmed the adequacy of the EU-US Privacy Shield [9]: "(…) the Commission concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organizations in the United States."

As for the workings of the Privacy Shield, the decision by US-based companies to join the program is entirely voluntary and leads to their public commitment to comply with the Privacy Shield Principles through (annual) self-certification (enforceable under US law) [20], which is practically the same procedure as for the Safe Harbor. Since 2016, over 2,000 companies joined the Privacy Shield program through self-certification (including, for example, the fitness tracker manufacturer Fitbit Inc.).

Still, the faith of this program remains uncertain as several actions against European Commission's decision (about the Privacy Shield) had been brought to the European Court of Justice [5, 6]. Even though the new GDPR seems to improve the data privacy situation, especially by including such upgrades as "privacy by design" or "right to be forgotten," the EU-US Privacy Shield agreement raises some questions about GDPR's adequate enforcement, e.g., when data is being transferred in the USA. The Members of European Parliament also expressed concerns about the agreement, especially after "new rules allowing the US National Security Agency (NSA) to share private data with other US agencies without court oversight [or] recent revelations about surveillance activities by a US electronic communications service provider" came to light [11]. The Parliament acknowledges "the significant improvements made compared to the former EU-US Safe Harbor, but there are clearly deficiencies that remain to be urgently resolved to provide legal certainty for the citizens and businesses that depend on this agreement" [11].

As we can see in Fig. 3, the future after the new GDPR is in force remains uncertain. Even though the regulation has the potential to significantly improve the European data protection, including health-related and personal data accumulated with wearable tracking devices, the regulation of trans-Atlantic data transfer is still raising many concerns. The question is whether the few improvements and a new name make it just a wolf in sheep's clothing, or an actual "adequate" solution. With actions against the agreement [5, 6], the concerns will be hopefully resolved by EUCJ's ruling. In the following, the outcomes of the literature review on studies concerning data privacy and fitness trackers will be summarized.

3.2 Current Research on Data Privacy and Fitness Trackers

Firstly, it should be said that only one paper [32] explicitly mentions the GDPR. They clearly state, that "[i]n most countries, laws that govern the collection, storage, analysis, processing, reuse, and sharing of data (…) fail to adequately address the privacy challenges associated with human tagging technologies" because they were "enacted decades ago" [32]. They mention the new regulation in positive light. Ghazinour et al. [13] refer to the HIPAA regulating the use of health-related data in the USA, however, as already described in our legal part of the study, this regulation only addresses medical institutions and is not applicable for wearables. Altpeter [1] mentions the E-Health Law in Germany, which regulates the data privacy in medical sector (therefore, as for its applicability, it is comparable to the HIPAA). All reviewed publications, however, are concerned about data privacy regarding the use of fitness trackers, smart watches or other wearable technology with biodata tracking functions.

Rosenbaum et al. [23] try to assess the current situation and potential future developments, benefits and risks in retail marketing. They remark that "individualized 'data mining' enables delivery of personalized product recommendations and offerings," [23] but also "may disrupt the traditional view of consumer consent" [23] to this new kind of data collection. While activity tracking surely could have many benefits for retail marketing, the authors also recognize risk, apart from health-related data breaches, identity fraud or harassment, in misinterpreting health-related information and finally endangering the costumer due to false product recommendations. They state that "consumer-oriented nutrigenomics currently does not fit neatly into existing legal categories" [23] and encourage further research into the "dark side" of these new technologies before they are utilized.

Bostanci [4] identifies malware, breach of privacy, for example when handling data in medical facilities, connection dependency, efficient data processing, and incompatibility of analysis tools and systems as ethical and technological threats and challenges for the future of wearable technologies. Meanwhile, Altpeter [1] also mentions the emotions that consumers and practitioners, who do not want their patrons to lose their trust in them, might have in the e-health sector. He emphasizes that the fear of security gaps should not hold advances of a digital health system and its advantages back.

Ghazinour et al. [13] criticize the "current binary standard" for data collection as it "leaves the user no options on selecting their privacy preferences on their data and if they do not agree to the terms, they cannot use the device" [13]. They propose a model that lets users decide about the privacy preferences for every data item.

Torre et al. [29] extend this issue by thematizing the problem of inference attacks by third parties which are granted access to health and activity data by the user. They present their idea of connecting an "Adaptive Inference Discovery Service" with personal data management functionalities to respect and take into account "the individuals' perception of privacy" [29]. In the next step of their study [30] they apply this framework in a case study with data from 49 users and predict different aspects such as weight, steps, gender and smoking with an accuracy of 50.2–99.9%. Hereby, Torre et al. show how users could be assisted in deciding which privacy settings are optimal to reduce inference risk. Of course, first of all, users need to be made aware of the risk of inference when allowing third parties to use their sensitive health and activity data.

Finally, there are also user studies which try to give insight on the opinion, perception and behavior of the users themselves. After an online survey, focus group interviews and an in-depth interview with 12 users, Yoon et al. [34] reported that power-users had fewer concerns regarding privacy ("unnecessary anxiety") than non-power-users ("vague fear") – contrary to their expectations and previous findings [34, p. 545].

Lehto and Lehto [16] asked ten participants of qualitative interviews about the sensitivity of their health data and their willingness to share data with different parties. They found that "information collected with wearable devices is not perceived as sensitive or private" while "health information stored in patient medical records is considered to be very sensitive and private" [16]. Therefore, almost all interviewees did not want to share their data with social media (9/10) but were willing to share it freely with the doctor or medical research (10/10). Eight of ten participants would share it with occupational health services and seven with the device manufacturer. Lehto and Lehto [16] conclude that handling of tracked data "needs to be described clearly and transparently to mitigate any privacy concerns from the individuals" [16] and that "[d]evice makers need to consider how and when location data is being collected as this causes many privacy concerns that can impact use and adoption of these devices" [16].

In another attempt to understand the privacy concerns of fitness tracker users, Lidynia et al. [17] conducted an online survey (n = 82). Participants preferred to keep logged data to themselves and not on external servers—sharing activity data online was not favored either. Lidynia et al. [17] admit, however, that their sample is rather small and participants were relatively young. They recommend applying their methods, the privacy paradox and the privacy calculus to a bigger and more representative sample.

4 Discussion

The legal perspective on the data privacy showed that this is an increasingly important topic, especially when such devises like fitness trackers collecting not only general personal data, but more and more health-related information, are concerned. With the new General Data Protection Regulation the European data privacy environment is changing for the better. However, is the "new" EU-US Privacy Shield agreement keeping up with this improvement? Or does it perpetuate old issues under a new name? The level and range of data privacy regulations in USA are hardly comparable to the ones in European Union. The increasing involvement of private persons in disputes about (their) personal data as well as the assistance of national data privacy authorities is somewhat reassuring that inadequate regulations violating the fundamental rights of EU citizens will be under fire. Hopefully, the decision making and emendation of these regulations will occur more quickly than it was common until now. The legislative process and formally correct execution of legal procedures take time; however, the time is running up much faster when new technologies are involved.

When compared to data privacy authorities and legislators, there is only a slight interest in data privacy and fitness trackers or similar wearables among scholars. The research on this particular topic seems to be increasing; however, it is still nascent. Very few studies address legal regulations and only one refers to the GDPR. Most of

the studies are rather theoretical, defining data privacy frameworks or summarizing benefits or challenges of wearable devices. Four of the reviewed studies were more user-oriented (case study, online survey, qualitative interviews). But still, the rather small sample sizes of user-oriented investigations and quite general studies otherwise indicate that this is an early stage of research within this domain.

5 Limitations and Future Research

For the future research on the legal perspective, we would recommend a more detailed analysis of current disputes between data privacy authorities and the European Commission (regarding the EU-US Privacy Shield) or fitness tracking manufacturers/service providers (regarding violations of data privacy regulations). In this study we only focused on the trans-Atlantic data transfer and respective agreements between EU and USA. An investigation of further bilateral agreements and data transfers as well as data privacy situation in, for example, China would be an interesting aspect to investigate in the future.

Regarding the scientific research on fitness trackers and data privacy, there appear to remain many gaps that could be closed in the future. Firstly, more reference to the legal situation would be beneficial and relevant for practice. Secondly, a more extensive user-oriented research going beyond users' privacy preferences would give scholars and practitioners more relevant insights. In this respect, such aspects as users' knowledge (or lack of it) about what happens with their data (and their respective attitudes toward it), or knowledge about what (data privacy) rights are actually due to them, would be interesting.

References

1. Altpeter, B.: E-health as a component of holistic therapy optimization. (E-Health als Bestandteil ganzheitlicher Therapieoptimierung), Diabetologe **13**(1), 29–37 (2017)
2. BBC: Privacy complaint for fitness wristband makers. http://www.bbc.com. Accessed 20 Feb 2018
3. BFDI: Datenschutz bei Gesundheits-Apps und Wearables mangelhaft. https://www.bfdi.bund.de. Accessed 20 Feb 2018
4. Bostanci, E.: Medical wearable technologies: applications, problems and solutions. In: 2015 Medical Technologies National Conference, pp. 50–53 (2015)
5. Curia: Case T-670/16, Digital Rights Ireland v. European Commission. http://curia.europa.eu. Accessed 22 Feb 2018
6. Curia: Case T-738/16, La Quadrature du Net and Others v. European Commission. http://curia.europa.eu. Accessed 22 Feb 2018
7. De Hert, P., Papakonstantinou, V.: The new general data protection regulation: Still a sound system for the protection of individuals? Comput. Law Secur. Rev. **32**, 170–194 (2016)
8. EC: Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. http://europa.eu/rapid/press-release_IP-12-46_en.htm. Accessed 21 Feb 2018

9. EC: Report from the commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield. https://ec.europa.eu. Accessed 21 Feb 2018
10. EC: Adequacy of the protection of personal data in non-EU countries. https://ec.europa.eu. Accessed 22 Feb 2018
11. European Parliament: Data Privacy Shield: MEPs alarmed at undermining of privacy safeguards in the US. http://www.europarl.europa.eu. Accessed 22 Feb 2018
12. Fietkiewicz, K.J., Lins, E.: New media and new territories for european law: competition in the market for social networking services. In: Knautz, K., Baran, K.S. (eds.) Facets of Facebook: Use and Users, pp. 285–324. De Gruyter Saur, Berlin, Germany, Boston, MA (2016)
13. Ghazinour, K., Shirima, E., Parne, V.R., Bhoomreddy, A.: A model to protect sharing sensitive information in smart watches. Procedia Comput. Sci. **113**, 105–112 (2017)
14. Kahn, J.: Fitness tracking startups are sweating due to EU privacy regulators. privacy regulators worry companies could abuse access to data, https://www.bloomberg.com. Accessed 20 Feb 2018
15. Krystlik, J.: With GDPR, preparation is everything. Comput. Fraud Secur. **7**, 5–8 (2017)
16. Lehto, M., Lehto, M.: Health information privacy of activity trackers. In: European Conference on Information Warfare and Security, ECWS, pp. 243–251 (2017)
17. Lidynia, C., Brauner, P., Ziefle, M.: A step in the right direction – understanding privacy concerns and perceived sensitivity of fitness trackers. Adv. Intell. Syst. Comput. **608**, 42–53 (2018)
18. Mendelson, D., Mendelson, D.: Legal protections for personal health information on the age of Big Data – a proposal for regulatory framework. Ethics Med. Public Health **3**, 37–55 (2017)
19. O'Connor, Y., Rowan, W., Lynch, L., Heavin, C.: Privacy by design: informed consent and internet of things for smart health. Procedia Comput. Sci. **113**, 653–658 (2017)
20. Privacy Shield Framework. https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1. Accessed 21 Feb 2018
21. Reding, V.: The upcoming data protection reform for the european union. Int. Data Priv. Law **1**(1), 3–5 (2010)
22. Reinerman-Jones, L., Harris, J., Watson, A.: Considerations for using fitness trackers in psychophysiology research. In: Yamamoto, S. (ed.) HIMI 2017. LNCS, vol. 10273, pp. 598–606. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58521-5_47
23. Rosenbaum, M.S., Ramírez, G.C., Edwards, K., Kim, J., Campbell, J.M., Bickle, M.C.: The digitization of health care retailing. J. Res. Interact. Mark. **11**(4), 432–446 (2017)
24. Schwartz, P.M.: The EU-U.S. privacy collision: a turn to institutions and procedures. Harvard Law Rev. **126**(7), 1966–2009 (2013)
25. Terry, N.: Mobile health: assessing the barriers. Chest **147**(5), 1429–1434 (2015)
26. Terry, N.: Existential challenges for healthcare data protection in the United States. Ethics Med. Public Health **3**, 19–27 (2017)
27. The Economist: Things are looking app: mobile health apps are becoming more capable and potentially rather useful, https://www.economist.com. Accessed 21 Feb 2018
28. Tikkinen-Piri, C., Rohunen, A., Markkula, J.: EU general data protection regulation: changes and implications for personal data collecting companies. Comput. Law Secur. Rev. **34**, 134–153 (2018)
29. Torre, I., Koceva, F., Sanchez, O. R., Adorni, G.: A framework for personal data protection in the IoT. In: 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, pp. 384–391 (2016)

30. Torre, I., Sanchez, O. R., Koceva, F., Adorni, G.: Supporting users to take informed decisions on privacy setting of personal devices. Personal and Ubiquitous Computing, pp. 1–20 (2017)
31. Van den Bulck, P.: Transfers of personal data to third countries. ERA Forum **18**, 229–247 (2017)
32. Voas, J., Kshetri, N.: Human tagging. Computer **50**(10), 78–85 (2017)
33. Xie, N.: Norway: Consumer Council addresses "transparency issues" in fitness wristbands. https://www.dataguidance.com. Accessed 20 Feb 2018
34. Yoon, H., Shin, D.H., Kim, H.: Health information tailoring and data privacy in a smart watch as a preventive health tool. In: Kurosu, Masaaki (ed.) HCI 2015. LNCS, vol. 9171, pp. 537–548. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21006-3_51