

How Do Users of Activity Tracking Technologies Perceive the Data Privacy Environment in the EU?

Kaja J. Fietkiewicz¹ and Aylin Ilhan²

^{1,2} Heinrich Heine University Düsseldorf, Germany

¹Kaja.Fietkiewicz@hhu.de ²Aylin.Ilhan@hhu.de

Abstract. With the omnipresent digitalization and quantification of our everyday life, data privacy became an important topic in research, politics and legislation. In order to contain the possible risks of uncontrolled data collection and its possible misuse, it is important to ensure a sustainable data privacy environment. Here, one of the most important aspects is an efficient and effective legislature. In May 2018, when the General Data Protection Regulation (GDPR) came into force, the EU made an important step towards improving the European data privacy environment. In this study there are investigated both, the awareness and the perception of the GDPR by the users of fitness tracking technologies. This investigation focuses on people from the EU using a fitness tracking application as well as a fitness tracking device, which usually collect a lot of personal and health-related data. Most of the fitness tracking users are aware of the GDPR but do not believe that it will improve the reality of data privacy. Even though there appears to be limited belief in the sustainability of the European data privacy environment (in terms of a positive development of consumers' data privacy), this does not necessarily affect the everyday usage of activity tracking applications and wearables.

Keywords: GDPR, Sustainable Data Privacy Environment, Fitness Tracking Users, EU.

1 Introduction

Data privacy concerns rise with the increasing digitalization and quantification of our everyday life. What changes is also our information behavior, which now includes storing countless (personal) information pieces on the web and cloud services. These also include health information collected with activity tracking technologies, such as mobile fitness applications or fitness tracking wearables. The increasing pace of technological development is accompanied by the uncertainty about where it will lead and, especially, how all the collected data could be exploited (since it is already seen as a form of “currency” [1]). Facing these uncertain future developments, it is important to create a more sustainable data privacy environment, comprised of adequate legal framework, its effective enforcement, and compliance by the business enterprises. Fitness tracking technologies can collect diverse personal, health-related, or location-based data, therefore, this is a prominent sector to investigate in the context of data privacy environment.

Fitness tracking is also popular in the scientific field. Most studies on this topics focus on the accuracy of the trackers (see, e.g., [2, 3]) or usability, engagement, adoption, and acceptance (see, e.g., [4–10]). The number of studies on activity tracking technologies increased over the last years, which was confirmed by the systematic literature review (2013-2017) conducted by Shin et al. [11]. Based on a topic modeling analysis, Shin et al. [11] were able to detect six thematic clusters, “privacy” being one of them. Fietkiewicz and Henkel [12] conducted a literature review on fitness tracking and data privacy in the context of the GDPR. They point out several research gaps that could be closed in future studies, including a more extensive user-oriented research that goes beyond users’ privacy preferences. The scientific coverage of activity tracking and data privacy is still limited and mostly investigated from the technological point of view (e.g., encryption of health-related data, see [13–15]). Therefore, this study focuses on users’ knowledge and attitude towards European data privacy environment.

Considering data privacy in the EU, since May 2018 the GDPR plays a crucial role in regulating the consumer market, also for the fitness tracking industry. GDPR came into force in order to improve the security of personal data of the European consumers and, among others, to empower them to decide about what happens to their data. There already are few studies investigating the compliance of mobile applications with the GDPR [16–19]. Even though in these studies the focus is set on mobile health applications (mHealth), the data collected by such applications is to a certain extent similar to the data accumulated through fitness or activity tracking. The new legislation might improve the data privacy environment in EU by making it more effective and sustainable. Some of GDPR’s requirements are: explicit consent of the consumers to collect, use and move their data; the right to be forgotten; mandatory data breach notifications (within 72 hours); or privacy by design [16]. The press release of the European Commission (May, 22 2019) [20] indicates that already within about one year since GDPR came into force, “people are starting to use their new rights and more than two-third of Europeans have heard of the regulations.” However, it should not only be considered whether consumers have heard of GDPR, but also what is their perception of the regulation and its impact on data privacy. The recent research focuses only on the compliance of mobile health applications with the new legislation (which seems to be not fully satisfactory, see e.g. [17, 18]), but does not consider the perception of it by users of these applications. This rises the research questions (RQs) for the current study:

- **RQ1:** How is the awareness of the GDPR among users of activity tracking technologies in the EU?
- **RQ2:** Do the users of activity tracking technologies expect the GDPR to change the status of data protection for the better?

This research does not evaluate the sustainability of the GDPR, but rather how it is being perceived by the consumers. Given the requirement of “privacy by design” or “privacy by default,” the regulation seems to be more sustainable than the preceding Data Privacy Directive. Now, data privacy has to be considered as early as during the development stages of the technology and the amount of data collected “by default” needs to be kept to a needed minimum. However, are the European fitness tracking consumers convinced of this regulation’s effectiveness?

2 Methods

2.1 Online Questionnaire

The online survey conducted for this study included different blocks of questions, some of which were not privacy-related (e.g., socio-demographic questions, general activity and fitness level, use and duration of activity tracking applications and devices). Considering the research gaps indicated in the introduction, this study focuses only on GDPR and privacy-related aspects as well as the activity tracking technology users from the EU. The remaining study participants (non-users, or users from other regions) as well as other questions not related to privacy, which were included in the survey, will not be further elaborated from this point on.

The survey included the question about the awareness of as well as the general opinion on GDPR. As the survey was also accessible to participants from non-EU countries, the answer “I am not from EU, so it does not concern me” was added. Furthermore, three statements addressing the general opinion on online data privacy (GO1-GO3) were also included to investigate, if a positive or negative expectation of GDPR vary significantly between users with different opinions on general online data privacy. This opinion could be marked on a five-point Likert scale from ‘1—Strongly Disagree’ to ‘5—Strongly Agree’ and the neutral element ‘3—Neither agree nor disagree.’

A pretest of the survey by six participants led to minor modifications in language, formulating statements more objectively, clarifying any ambiguities, adding open questions for further comments, and making the survey more user-friendly by different positioning and segmentation of the questions. The survey distribution was non-probabilistic with a self-selected set of respondents. It distributed from February 26, 2019, until May 28, 2019, through different social media channels, scientific communities, or survey portals (e.g., SurveyCircle, Survey Tandem).

3 Results

All in all, 646 participants completed the survey, but only 235 currently use both, a fitness application and an activity tracker or smartwatch. Furthermore, 167 of these participants were from the EU (which is the relevant sample for the current study). The most represented EU-countries were Germany, U.K., Poland and Austria. In general, activity trackers and applications by the companies Fitbit, Garmin and Apple were the most popular among the study participants. The distribution by gender is very balanced (Table 1) as 49.7% of the participants are female, and 50.3% are male. Regarding the age of the participants, for further analysis a categorization into four generations, based on research on inter-generational differences in digital media usage [21], was conducted. The four generations include: Silver Surfers (at least 60 years old), Gen X (40-59 years old), Gen Y (between 24 and 39 years old), and finally, Gen Z (up to 23 years old). As for this sample, the biggest age group is Gen Y (63.5%) and Gen X (21%).

Table 1. Sample characteristics: fitness trackers and fitness applications' users from the EU.

Sample characteristics (N=167)	
Gender	Male 50.3% (n=84) Female 49.7% (n=83)
Age	Silver Surfers 6.6% (n=11) Gen X 21% (n=35) Gen Y 63.5% (n=106) Gen Z 9% (n=15)
Avg. activity level during the day	3 ("I am moderately active")
Avg. exercise level	7 ("I exercise 3 or more times per week")
Avg. usage freq. of application	7 ("Every day")
Avg. usage duration of application	4 ("For a year")
Avg. usage freq. of wearable	7 ("Every day")
Avg. usage duration of wearable	4 ("For a year")

The first research question concerned the users' awareness of the GDPR, whereas the second research question regarded their perception of GDPR's effectiveness. A total 95% of the survey participants from EU heard of the GDPR. More than half of these users (61%; N=158) do not think that it will change anything for consumers' data privacy. Interestingly, one participant mentioned that "[mainly] it would be about privacy. Although GDPR is a good thing, many companies will not obey the rules because there is a lot of money to be made in selling this data. Even the UK government is selling on confidential patient data to industry" (participant₁).

The participants' attitude towards GDPR was further analyzed in the context of their general data privacy concerns. Fig. 1 shows that all in all users from the EU are concerned about data security on the Internet and about what companies can do with their data. Even though GDPR is supposed to protect consumer data, users from the EU are still doubtful about its effectiveness.

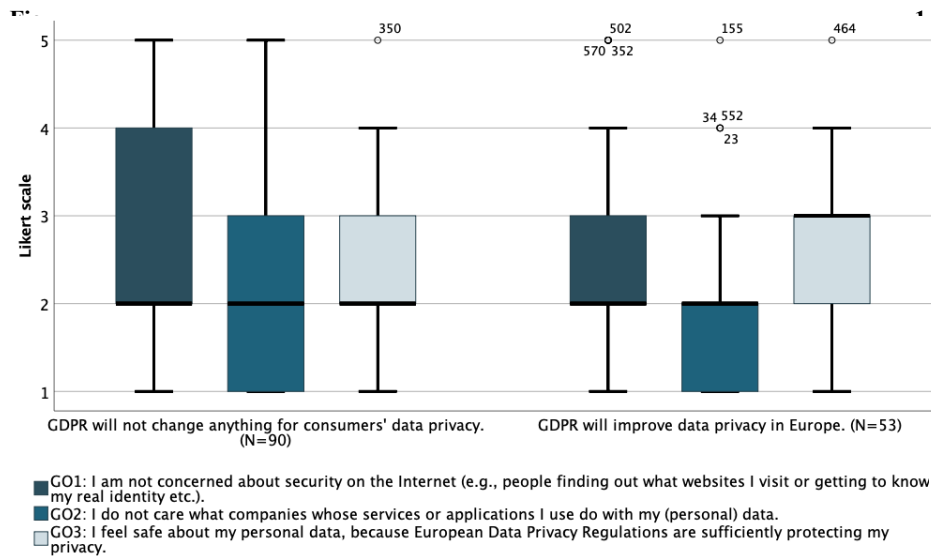


Fig. 1. General opinion on online data privacy and GDPR. Likert scale from ‘1—Strongly Disagree’ to ‘5—Strongly Agree’.

A Mann-Whitney U test was applied to determine if there were significant differences in general online data privacy concerns between EU users who believe in the effectiveness of GDPR and the ones who do not. Distributions of each statement (GO1-3) for users who think positively and negatively about GDPR were quite similar considering the median values, except for GO3. Here, the mean ranks are significantly different between users who believe in GDPR’s effectiveness (Mean Rank = 85.97) and the more skeptical ones (Mean Rank = 63.77) ($U = 3125.500$, $z = 3.243$, $p = .001$). The median of “I feel safe about my personal data, because European data privacy regulations are sufficiently protecting my privacy” (GO3) is somewhat higher for the reserved (impartial) users (Median = 3; ‘Neither agree nor disagree’) than for the skeptical ones (Median = 2; ‘Disagree’). This is a somehow expected outcome, since people who are in general skeptical about the effectiveness of European data privacy legislation have most probably some reservations towards the GDPR. Hence, the new legislation does not seem to have convinced the skeptics. Interestingly, when considering the distribution of the answers, participants who hope to see improvement due to the GDPR are partly more concerned about online data privacy than the other group.

The differences between GDPR enthusiasts and GDPR skeptics were further analyzed in the context of their socio-demographic characteristics as well as fitness (tracking) routine. In Table 2 we can see some slight differences, e.g., that more women are skeptical about GDPR than men, or that the older generations are more likely to disbelieve in its effectiveness than the younger ones. However, Pearson χ^2 revealed that there is no significant association between any of these variables and the attitude towards GDPR.

Furthermore, there appear to be no differences between these two groups regarding their activity and fitness (tracking) level. This was also confirmed by the Mann-Whitney U Test. It seems that mistrust in the data privacy environment does not get influenced by the usage of fitness tracking technologies, or vice versa, it does not influence it in any apparent way.

Table 2 Differences between GDPR enthusiasts and pessimists (n=143).

		GDPR enthusiasts (n=53)	GDPR pessimists (n=90)
Gender	Male	45.7%	54.3%
	Female	31.2%	68.8%
Age	Silver Surfers	30%	70%
	Gen X	38.2%	61.8%
	Gen Y	37.6%	62.4%
	Gen Z	53.8%	46.2%
Activity Level	During the day	3 (moderate)	3 (moderate)
	Exercise	7 (3< times/week)	6 (1-2 times/week)
Activity application	Usage freq.	7 (ever day)	7(ever day)
	Usage duration	4 (for a year)	4 (for a year)
Activity wearable	Usage freq.	7 (ever day)	7 (ever day)
	Usage duration	4 (for a year)	4 (for a year)

4 Discussion

This study showed that users of the fitness tracking applications and activity wearables from the EU are mostly aware of the GDPR. Interestingly, the results also show that more than half of these participants do not believe that it will lead to positive changes considering data protection. As one participant mentioned, one critical aspect is trust in its impact and perseverance. Users need to be able to trust in the effectiveness of the legal system and that the companies will comply. Some statements made by the users (even those who are not living in the EU) indicated that the EU has better data protection conditions than non-EU countries. Considering data scandals in the last years, it seems that users need more effective data protection regulations and their consistent execution. But, it is also not very surprising that users who believe in the effectiveness of European data privacy regulations are more likely to believe in the effectiveness of the new GDPR (or at least have a “neutral” opinion about it, as opposed to users who “disagree” with the efficacy of European legislation).

The implications of presented results are limited as the study only investigated whether participants are aware of the GDPR and whether they think it will positively change the state of data protection, but not why they think so or what impact it has on

the fitness tracking industry in particular. This could be an interesting aspect to investigate in future research.

5 Conclusion

The aim of this study was to do a first step towards closing the research gap in the domain of fitness tracking and sustainable data privacy environment, which up until now focused on the technological point of view. For this reason, we conducted a user-centered survey and gained insights into fitness tracking application users' awareness and attitude towards GDPR. Even though the participating European users are aware of the GDPR, most of them are rather skeptical as to its impact on data privacy. This however, does not appear to be impacted by socio-demographics aspects as well as the extent of the usage of fitness tracking technology.

6 References

1. Fietkiewicz, K.J., Lins, E.: New media and new territories for European law: Competition in the market for social networking services. In: Knautz, K. and Baran, K.S. (eds.) *Facets of Facenook: Use and Users*. pp. 283–322. De Gruyter (2016).
2. Evenson, K.R., Goto, M.M., Furberg, R.D.: Systematic review of the validity and reliability of consumer-wearable activity trackers. *Int. J. Behav. Nutr. Phys. Act.* 12, (2015).
3. Rosenberger, M.E., Buman, M.P., Haskell, W.L., McConnell, M. V., Carstensen, L.L.: Twenty-four Hours of Sleep, Sedentary Behavior, and Physical Activity with Nine Wearable Devices. *Med. Sci. Sports Exerc.* 48, 457–465 (2016).
4. Feng, Y., Li, K., Agosto, D.E.: Healthy users' personal health information management from activity trackers: The perspective of gym-goers. *Proc. Assoc. Inf. Sci. Technol.* 54, 71–81 (2017).
5. Fritz, T., Huang, E.M., Murphy, G.C.: Persuasive technology in the real world: a study of long-term use of activity sensing devices for fitness. *Chi.* 241–244 (2015).
6. Gouveia, R., Karapanos, E., Hassenzahl, M.: How do we engage with activity trackers? a longitudinal study of habito. *UbiComp 2015 - Proc. 2015 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput.* 1305–1316 (2015).
7. Ilhan, A., Henkel, M.: 10,000 Steps a Day for Health? User-based Evaluation of Wearable Activity Trackers. *Proc. 51st Hawaii Int. Conf. Syst. Sci.* 3376–3385 (2018).
8. Lyall, B., Robards, B.: Tool, toy and tutor: Subjective experiences of digital self-tracking. *J. Sociol.* 54, 108–124 (2018).
9. Nelson, E.C., Verhagen, T., Noordzij, M.L.: Health empowerment through activity trackers: An empirical smart wristband study. *Comput. Human Behav.* 62, 364–374 (2016).

10. Rooksby, J., Rost, M., Morrison, A., Chalmers, M.: Personal tracking as lived informatics. *Conf. Hum. Factors Comput. Syst. - Proc.* 1163–1172 (2014).
11. Shin, G., Jarrahi, M.H., Fei, Y., Karami, A., Gafinowitz, N., Byun, A., Lu, X.: Wearable activity trackers, accuracy, adoption, acceptance and health impact: A systematic literature review. *J. Biomed. Inform.* 93, 103153 (2019).
12. Fietkiewicz, K.J., Henkel, M.: Privacy Protecting Fitness Trackers: An Oxymoron or Soon to Be Reality? Presented at the (2018).
13. Abbas, A., Khan, S.U.: A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds. *IEEE J. Biomed. Heal. Informatics.* (2014).
14. Fernández-Alemán, J.L., Señor, I.C., Lozoya, P. ángel O., Toval, A.: Security and privacy in electronic health records: A systematic literature review, (2013).
15. Li, H., Wu, J., Gao, Y., Shi, Y.: Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *Int. J. Med. Inform.* 88, 8–17 (2016).
16. Braghin, C., Cimato, S., Della Libera, A.: Are mHealth Apps Secure? A Case Study. *Proc. - Int. Comput. Softw. Appl. Conf.* 2, 335–340 (2018).
17. Benjumea, J., Dorrnzoro, E., Roperio, J., Rivera-Romero, O., Carrasco, A.: Privacy in Mobile Health Applications for Breast Cancer Patients. 634–639 (2019).
18. Muchagata, J., Ferreira, A.: Mobile apps for people with dementia: Are they compliant with the general data protection regulation (GDPR)? *Heal. 2019 - 12th Int. Conf. Heal. Informatics, Proceedings; Part 12th Int. Jt. Conf. Biomed. Eng. Syst. Technol. BIOSTEC 2019.* 68–77 (2019).
19. Muchagata, J., Ferreira, A.: Translating GDPR into the mHealth Practice. *Proc. - Int. Carnahan Conf. Secur. Technol.* 2018-October, (2018).
20. European Commission: General Data Protection Regulation: one year on, http://europa.eu/rapid/press-release_IP-19-2610_en.htm.
21. Fietkiewicz, K.J.: Jumping the digital divide: How do “silver surfers” and “digital immigrants” use social media? *Netw. Knowl.* 10, 5–26 (2017).