Tracking or being tracked: How much do self-trackers care about their data's privacy?

Alice Floris[1]; Stefanie Astfalk[2]; Rachelle Sellung[3]; Heiko Roßnagel[4]

Abstract: The advancement of tracking technology has given people new ways to understand and rediscover themselves. These technologies provide new and unique challenges to individual privacy, particularly when privacy breaches become less apparent, and users are not adequately aware of privacy regulations and risks. Nonetheless, research on privacy concerns with self-tracking data remains inconclusive and poorly understood. Moreover, the fundamental concept of data self determination — the cornerstone of information privacy — is under attack as users fail to take the necessary precautions to protect themselves. The current study used a quantitative method to examine the overall profile of self-trackers as well as their attitudes, preferences, concerns, and hurdles to (better) privacy protection. Self-trackers, according to the findings, seek control over both their bodies (i.e., self-optimization) and their data. Additionally, people just expect to have full control over their data and are disinterested in enforcing it or devoting effort to it. This suggests that, while privacy is still associated with control, users' actions and decisions make them more susceptible to loss of data control. We contend that these findings are consistent with the privacy paradox as well as the failure of privacy self-management, as defined by [So13].

Keywords: Information privacy; data control; privacy self-management; self-tracking.

1 Introduction

How much sleep did you get last night? Did you drink enough water? How many calories did you burn today? Self-tracking is the use of digital technology to record and convert our everyday experiences and habits into data. Datafication of users' bodies has become common practice in health promotion and care [Lu16]. Health and fitness apps, for example, make up 3.50 % of all available applications in the Google Play Store globally [St22a], with over 53,000 mobile health apps [St22a]. Moreover, experts predict that digital health revenue will expand at a 10.59 % annual rate from 2022 to 2026 [St22a], resulting in a predicted market volume of $224.20 billion by 2026. This massive quantity of personal data collected opens up new opportunities for users, the healthcare system, and

[1] University of Twente, ORCID: https://orcid.org/0000-0003-4442-852X
[2] Universität Stuttgart, Institut für Arbeitswissenschaft und Technologiemanagement (IAT), ORCID: https://orcid.org/0000-0002-1926-639X
[3] Fraunhofer IAO, Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, ORCID: https://orcid.org/0000-0003-1235-030X
[4] Fraunhofer IAO, Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, ORCID ID: https://orcid.org/0000-0001-7057-8404

doi: 10.18420/sicherheit2024_008

businesses. However, studies have expressed ethical challenges about this new datafication trend due to data collection and management concerns [St22b]. This come down to a matter of control— the delicate line between tracking oneself and being tracked by others [St21c]. Users, for example, are increasingly being persuaded to share their data with their health insurance providers in exchange for benefits or perks [Ma16]. Aside from the fact that providing personal data for financial rewards blurs the line between what is voluntary and what is not [Se15], sharing personal data with third parties increases the likelihood of it being misused. Indeed, digital technologies make data collection, usage, and distribution less expensive and faster [HHG18], while the use of information technology reduces the visibility of privacy intrusions [Aj20a]. Users lose control over how much and what information they disclose because most services and networks employ automated data synchronization [Ma16]. Thus, privacy concerns are rising in light of the increasing complexity of technology and personal information becoming increasingly incorporated into broader digital networks. This observation is consistent with Mason's prediction in 1986, when the author argued that information privacy will be one of the most pressing concerns in the Information Age [Aj20a].

The present quantitative study focuses on the general self-tracker's profile as well as delves into the subject of privacy. We focused on self-trackers' privacy concerns, as well as their challenges in maintaining their data, preferences and attitudes toward (better) data protection, sharing behaviours, and knowledge of data processing and management. Finally, we wanted to see if there was any evidence of a privacy paradox. In summary, the following research questions will be addressed: RQ1.) What is the general profile of the self-tracker? RQ2.) With whom and what are self-trackers willing to share? RQ3.) Are self-trackers concerned about the privacy of their data? RQ4.) What are self-trackers' preferences and attitudes toward (better) data protection? RQ5.) Do trackers face any challenges preserving their data? RQ6.) Are self-trackers knowledgeable in data processing and handling? RQ7.) Is there any evidence for a privacy paradox?

The paper is organized as follows: The related literature on privacy, user’s knowledge and concerns about privacy, and the privacy paradox will be discussed in Chapter 2. The methodology is outlined in Chapter 3, and the results will be presented in Chapter 4. The discussion of the results follows in Chapter 5, whereas Chapter 6 demonstrates some limitations and Chapter 7 concludes the article.

2 Related Literature

As information technology evolved, privacy became inextricably linked with the concept of a personal information space [Du17]. Furthermore, this idea is linked to the principle that individuals should always retain ownership of their data, with the last say over how much and what information is disclosed [Ma86]. This control-centered perspective has become the standard in privacy research [Ge18], laying the groundwork for today's understanding of privacy regulations [We68]. This core premise, however, is under threat

when consumers fail to take the essential precautions to secure their data. Most users, for example, do not have a comprehensive understanding of data processing and management. According to Vitak et al. (2018), 73 % of trackers did not know if their provider sold their data [SMB96], 66 % did not know who could access their data, and 85 % did not know how long the tracking companies stored their data. Similarly, [Aj20b] found that 50% of trackers were unfamiliar with their devices' and applications' data regulations [Ro21]. According to [MB12], individuals become real-time “walking data generator,” unaware of how much and what type of data they generate [Vi18]. In addition, the privacy paradox demonstrated that even when users express concerns about their data privacy, they do not take the required safeguards to secure themselves and continue to interact with technology in ways that jeopardize it (for a literature overview, see [Aj20b]). For example, when users are given the option to read the terms and conditions, the great majority of them accept them without reading them properly or at all. The privacy paradox is related to the idea that users can, and therefore should, make autonomous, rational privacy decisions to protect their data [So13]. This is inspired by the traditional individual-centered approach to data privacy [St22b], which stresses personal responsibility and control over data [Ge18]. However, studies have called into question whether it is still possible and acceptable to expect individuals to have full control in an ever-changing digital environment where data management has grown extremely complicated [MB12, Ko17, Ch20, BHL21]. Focusing entirely on the individual, according to [So21], is a "losing game for both the individual and privacy legislation," since the implications of datafication extend beyond the individual's control and therefore oversimplifies the complexity of privacy [Kh22]. Similarly, [So13] contends that users' failure to preserve their privacy is a natural consequence of privacy legislation that places too much reliance on privacy self-management. The author calls for a new paradigm in which personal responsibility is no longer the primary source of data protection and privacy regulations should shift in a new direction, focusing on larger structures outside to the user. However, the question is whether users care enough about their data to hand over control to a third party, such as their service provider.

3 Method

Based on the mentioned phenomena and theoretical research, a questionnaire was developed to assess the general characteristics, motivations, various privacy related issues, personality traits and demographics among self-trackers. The current study, however, will solely focus on specific results from the general characteristics and privacy sections. In particular, we will concentrate on self-trackers’ reasons and sharing behaviours; challenges, preferences, and attitudes toward data protection; and self-trackers' knowledge of data processing and management. The questionnaire used combines existing items in the literature with own devised items. After the development process, a pre-test with a small sample size (N= 10) was performed. Hereafter the items were modified and improved to fit users’ preferences. The final questionnaire includes 26 items organised in 5 groups as follows (see also Appendix 1).

Self-Tracking Characteristics: The first component of the questionnaire focused on the person's general profile, asking users what they track, for how long, how intensively, with what devices, and for what reasons. We also asked if they shared their data and, if so, with whom and what information. Moreover, we devised our own items to assess for healthism among users. Non-trackers were asked whether they had any reasons not to track, if they had any experience with self-tracking and if so, how they felt about it.

Motivations: The framework created by [Ke22] was employed to investigate self-trackers' motivations. In this 19-item framework, self-tracking is defined by five underlying motivations: *self-entertainment*, *self-association*, *self-design*, *self-discipline*, and *self-healing*. The items were scored on a 5-point Likert scale, with 1 indicating *strongly disagree* and 5 indicating *strongly agree*.

Privacy: We split the privacy section into four subsections: (1) Privacy concerns, (2) Confidence and knowledge data management, (3) Attitudes, values and barriers privacy protection, and (4) Preferences privacy protection. To begin, we assessed privacy concerns using the 9-item MUICPC scale developed by [MC19]. We modified the items to make them appropriate for the self-tracking setting while retaining the three dimensions of perceived surveillance, perceived intrusion, and secondary use of information**.** "I feel that as a result of my using mobile apps, others know more about me than I am comfortable with," for example, is modified to "I am concerned about people knowing more about me than I am comfortable with because of the use of self-tracking devices and services". Second, we created four items to test self-trackers' knowledge of data collection, retention, ownership, and selling. We also included three elements to evaluate the user's confidence in tracking companies. Thirdly, we assessed how trackers valued their data (e.g., "I believe my tracking data is valuable enough to be used against me") and about their overall attitudes towards privacy (e.g., "Ì believe privacy concerns are overrated"). Also, we investigated if self-trackers face any challenges in appropriately securing their data. Finally, we addressed specific questions about their preferences for improved privacy protection. For instance, whether they want to learn more about privacy legislation and other privacy topics, refrain from particular behaviours that jeopardize their privacy, or even pay for a service to secure their data.

Personality Traits and Demographics: We used the Big Five Inventory-10 (BFI-10) [GNG13], a condensed version of the original 44-inventory by [Xu12]. Gender, age, educational level, marital status, and gross monthly income were gathered as demographic information.

Data Collection: 132 people completed the questionnaire. Both trackers and non-trackers were eligible to participate. Likewise, no exclusion criteria were established other than the requirement that they complete the entire questionnaire. Participation was completely voluntary, and individuals were free to leave at any time. They were not compensated for their time. The tracking ratio in the sample was about equal, with 46.9 7% self-trackers (N = 62) and 53.03 % non-trackers (N = 70). 52.27 % were female (N = 69), 45.46 % were men (N = 60), and 2.27 % identifying as other (N = 3).

4 Results

4.1 Self-Trackers' General Characteristics

Sharing Behaviors: 72.58 % did not share their self-tracking data. Of the 27.42 % who did share their data, they shared it with friends (36.59 %), other self-tracking devices and applications (19.51 %), and a (online) community (17.07 %). In addition, trackers were divided on sharing health and nutrition information, with about an equal number strongly opposing sharing and others approving. Trackers were most willing to disclose information about their progress, such as the number of steps taken and metrics linked to exercise and workouts, but not body weight and mood.

Tracking Reasons: Lack of motivation (17.45 %), disinterest in self-tracking (13.68 %), and feeling pressured by it (10.38 %) were the three main reasons for not self-tracking (see Appendix 1). 50 % of self-tracking participants did not self-track to cope with a medical condition, compared to 32.26 % who did (17.74 % indicated they did not wish to answer the question). Instead, the primary motives were self-awareness (23.81 %), self-development (19.05 %), and extra motivation (17.14 %) as shown in Appendix 2.

4.2 Privacy

Privacy Concerns: First, responses to the *perceived surveillance* items varied. Nearly an equal number strongly disagreed (16.13 %), disagreed (19.35 %), stayed undecided (20.97 %), agreed (20.97 %), and strongly agreed (20.97 %) when asked whether they are concerned about devices tracking their location, as stated in Fig 1. Similar mixed results were seen for devices collecting personal data. When asked if they were concerned about their actions being tracked, ∼46.77 % disagreed to strongly disagreed, 25.81 % were undecided, and ∼27.42 % agreed to strongly agreed.

Second, results for the *perceived intrusion* items were similar to those for the perceived surveillance, with respondents divided on whether they are concerned that people know more about them and if their information is more available to others as a result of their tracking device usage. Third, there was a clear trend toward *secondary use* items, with 54.84 agreeing or strongly agreeing to be concerned about companies using their information for other purposes and 58.06% agreeing to strongly agreeing to be concerned about companies sharing their information with third parties without permission.

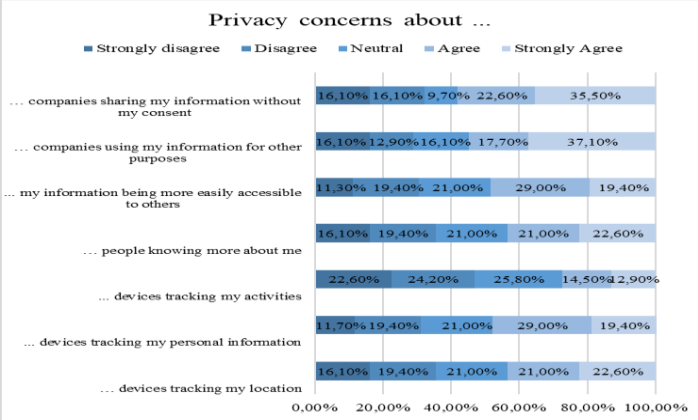

Fig. 1: Privacy Concerns Among Self-Trackers

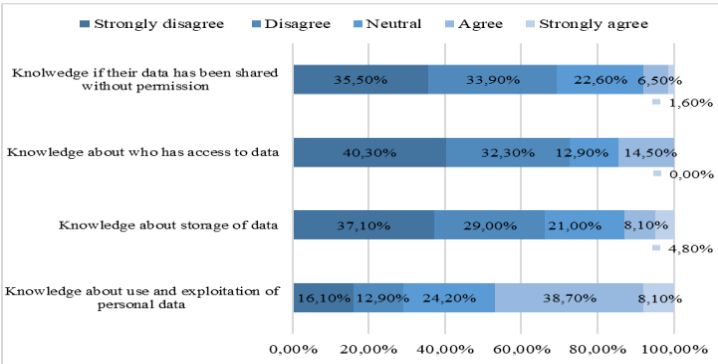

Fig 2: Self-Trackers' Knowledge Data Handling

Privacy Protection Attitudes, Values and Barriers: Self-trackers agreed to strongly agreed with 74.20 % that self-tracking data should be kept private and disagreed to strongly disagreed with 69.36 % that privacy concerns are overrated. However, 40.32 % were undecided and 37.10 % disagreed to strongly disagreed that it was their responsibility to ensure the security of their data. When asked if they feel self-tracking corporations violate their privacy by gathering their personal information, 53.22 % disagreed to strongly disagreed and 24.20 % remained undecided. Trackers disagreed to strongly disagreed with 46.77 %, agreed to strongly agreed with 29.03 %, and were undecided with 24.19 % on whether their data was valuable enough to be used against them. They did, however, agreed to strongly agreed with 48.39 % that companies exploiting their information would have an influence on them, compared to 27.42 % who disagreed to highly disagreed and 24.19 % who were undecided. 51.62 % agreed to strongly agreed that they do not have the time to be concerned about their privacy (compared to 33.87 % disagreeing to strongly disagreeing and 14.52 % undecided). 50.00 % disagreed to strongly

disagreed that they have the necessary technological skills and expertise to adequately preserve their data, as depicted in Fig 3.

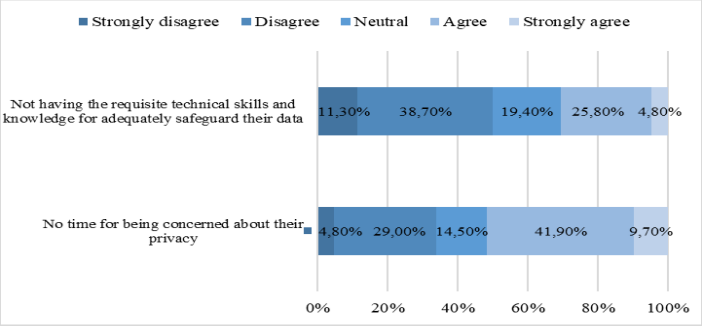

Fig 3: Barriers Privacy Protection

Preferences Privacy Protection: Trackers reported an interest in learning more about privacy regulations, data processing and storage, and how to better protect their data. Responses were divided as to whether they would effectively spend time learning more about privacy policies. They stated that they would use other applications or self-tracking devices if they believed their privacy would be better secured but were split on whether they would quit sharing if that would better protect their data.

77.97 % agreed to strongly agreed that if a self-tracking company wants to use their personal information for other purposes, they should be informed or asked permission, as illustrated in Fig 4. Similarly, 77.42 % agreed to strongly agreed that they want more say in how companies manage their personal data and that they should be notified of changes to their privacy terms and conditions (64.52 %). Users were split on whether they would pay an annual membership or delegate responsibility for protecting their privacy to a service.

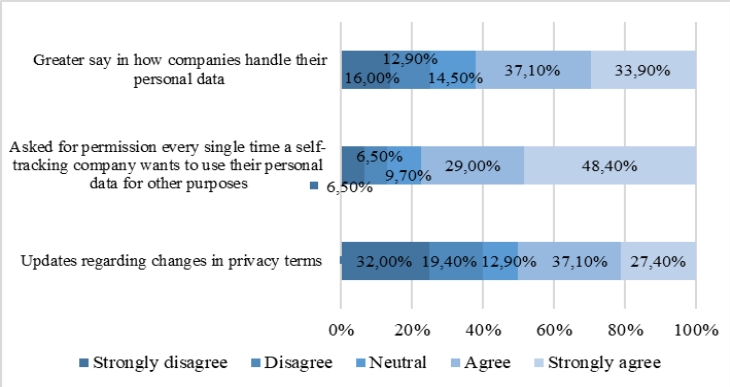

Fig 4: Self-Trackers' Preferences Privacy Protection

5 Discussion

RQ1: What is the general profile of the self-tracker? First and foremost, most trackers do not track themselves because they are dealing with a medical issue. The least mentioned motivation to track, for example, was because of a doctor's recommendation. Trackers, on the other hand, do so voluntarily because they want to be in charge of their own bodies and health. This is evident in their top three reasons for tracking: self-awareness (23.81 %), self-development (19.05 %), and extra motivation (17.14 %); but also what they track: physical activity (29.89 %), body measures (22.41 %), and general well- being (14.94 %). These findings are consistent with previous research, which has found a strong connection between self-tracking and self-optimization [GRS03, Go93, EP16]**.** People are becoming their own health entrepreneurs, as [Kr15] stated, proactively engaged in and devoted to the care of their own bodies and health.

On the other hand, the top three reasons given for not tracking were lack of motivation (17.45 %), disinterest in self-tracking (13.68 %), and feeling pressured by it (10.38 %). This indicates that self-tracking is a conscious choice made by the individual. Interestingly, privacy concerns were only the fourth most common reason for not tracking, showing that privacy concerns are not as serious enough to cause people to abandon the practice totally.

RQ2: With whom and what are self-trackers willing to share? The majority of trackers did not share their data with others, and even if they did, they were careful not to expose any sensitive information. Trackers were more likely to reveal information about their progress, exercises, and activities, but less likely to reveal information about their mood or body weight. This is not unexpected given that users primarily track themselves for self-optimization objectives. Attitudes about sharing health information were divided. This is an intriguing finding since it corresponds to the view that health information is rapidly becoming a collective benefit in an open, connected knowledge economy [7, WPG14, Sh16].

RQ3: Are self-tracking users concerned about the privacy of their data? The results for both the perceived surveillance and perceived intrusion dimensions were mixed, with approximately the same proportion of participants agreeing as disagreeing and another group remaining undecided. This is consistent with prior research by [An09] and [To21], which found that trackers are neutral to indifferent to their data. However, there was more consensus on the secondary use dimension, which includes the exploitation and sharing of self-tracking data with third parties without consent. This might be explained by the fact that, as [GS16] pointed out, secondary usage creates a sense of helplessness and vulnerability among users due to consumers' lack of information regarding data handling and management. Indeed, our findings indicated that, while trackers were aware that tracking companies gathered and used their data, they lacked the requisite data handling knowledge.

RQ4: What are self-trackers' preferences and attitudes toward (better) data protection? In terms of attitudes, trackers highly agreed that data should be kept private and strongly disagreed that privacy concerns are overblown. Moreover, trackers agreed with 64.52 % that they wanted to be alerted of changes to the privacy terms and conditions of their devices, 77.42 % said they want more say in how companies manage their personal data, and ~77.97 % want to be informed or asked permission when a company wants to use their personal information for other purposes. These data imply that trackers associate privacy with having control over one's personal information. This is not surprising given that data control has long been the central component of information privacy [Aj20a, Ma86].

RQ5: Do trackers face any challenges preserving their data? In a nutshell, yes. Half of the users stated they do not have time to be concerned about their privacy. Likewise, the same proportion of users stated that they lacked the requisite technological skills and competence to appropriately safeguard their data. In the idea that everyone should be able to secure their data for themselves, having only 50 % of users feeling capable of doing so is insufficient.

RQ6: Are self-trackers knowledgeable in data processing and handling? According to the findings, trackers had no idea how long their data was stored, who had access to it, or if it was shared without their knowledge. Similarly, what was discussed in research question 4, ~50.00 % disagreed to strongly disagreed that they have the technological skills and expertise to adequately preserve their data. These findings are consistent with earlier research indicating a lack of knowledge among self-trackers [SMB96].

RQ7: Is there such a thing as a privacy paradox? We contend that the findings support the privacy paradox. Users' privacy concerns and preferences indicate that they expect data control; nevertheless, the absence of understanding on the one hand, and a lack of willingness to invest time and effort in data security on the other, causes them to lose control over their data. Nonetheless, the findings do not refute Solove's [So13] contention that the privacy conundrum is not a paradox but rather a failed attempt at privacy self-management.

The one does not preclude the other: people demonstrate neither the ability nor the will to enforce control over their data. The latter is evident in that they indicate a want to learn more about privacy regulations and to better secure one's data (i.e., desire for control), but when asked if they would actually spend time doing so, respondents were hesitant. Similarly, when asked if they would delegate control to a service that manages their privacy, users expressed reservations. This means that people demand data control without wanting to be burdened by it; they just want it.

6 Learnings and Limitations

As self-tracking has grown more common, it is crucial that research enhance its understanding of self-tracking usage by carrying out a comprehensive assessment. One of the present study's strengths is that it takes a comprehensive approach to self-tracking behaviour by evaluating a variety of factors. To the best of our knowledge, this is the first study that examines self-tracking from such a broad perspective. In particular, we gained some valuable insights regarding individuals' challenges in preserving their data, preferences and attitudes toward (better) data protection, willingness to share data, and knowledge of data processing, trackers' concerns about data privacy as well as the privacy paradox. One limitation of this study is selection bias, since we attempted to include as many factors as possible while only included those that we considered relevant. Of course, this is biased, and it would have been interesting to explore how other factors, such as perfectionism, impact self-tracking behaviour. Prioritization, on the other hand, is crucial if one wishes to acquire a broad picture of self-tracking behaviour while keeping the questionnaire within a time constraint.

7 Conclusion

While trackers are their own health entrepreneurs [Kr15], they struggle to be their own data entrepreneurs. Trackers, on the one hand, equate data control with privacy and (better) data protection. As on the other hand, trackers expect control without necessarily wanting to exercise it or understand the complexities required for effective data management. They simply want control without being burdened by it.

In this regard, the findings are consistent with both the privacy paradox and the failed attempt at privacy self-management described by [So13]. Indeed, users' lack of knowledge and their misconception of data control reflect the in efficacy of the concept of privacy self-management, which may lead to individuals making online choices and actions that actually undermine their privacy despite their concerns. As a result, we contend that the privacy paradox does not exclude failed privacy self-management or the other way around.

So, while the control-centered approach to privacy may still be prevalent [Aj20a, Ma86], the current study indicates that demanding data control without the ability or willingness to enforce it is unsustainable. As a result, self-trackers are not only tracking themselves, but are also increasingly being tracked.

8 Appendix

Theme	Description	Reference
Characteristics	What are they tracking, what devices do they use, how intense do they track, how frequent do they track, what are they sharing and with whom, for what reasons do they track Healthism	Own devised items Health-isim [An16]
Motivations	Self-entertainment, self-association, self-design, self-discipline, self-healing	[GNG13]
Privacy	Privacy concerns Confidence and knowledge data handling; Values, attitudes and barriers data protection; Preferences privacy protection	[Xu12]
Personality traits	Big 5	[GRS03]
	Vanity	[Ne95]
Demographics	Gender, age, education level, marital status, monthly income	Own devised items

Appendix. 1: Structure of the Questionnaire given.

Reason	Count	%
Self-awareness	50	23.81
Self-development	40	19.05
Extra motivation	36	17.14
Habit change	25	11.90
Self-confirmation	22	10.48
Data collection	17	8.10
Sharing and comparing data	9	4.29
Recommendation friends and others	4	1.90
Career	4	1.90
Doctor Recommendation	3	1.43

Appendix. 2: Reasons given by Self-Trackers

Reason	Count	%
I am not motivated to do it	37	17.45
I am not interested in self-tracking	29	13.68
I get a sense of pressure from self-tracking	22	10.38
I am concerned about my privacy	19	8.96
It is too much effort	17	8.02
I do not have the time	16	7.55
Self-tracking makes me feel obsessed	15	7.08
When a goal is not met, self-tracking makes me feel guilty	12	5.66
Self-tracking bores	11	5.19

me		
Self-tracking makes me anxious	6	2.83
Self-tracking frustrates me	6	2.83
I am having trouble using its gadgets and applications	5	2.36

Appendix 3:Non-Trackers Reasoning

Note: An overview of the reasons given by non-trackers for not self-tracking.

9 References

[So13] Solove, D. J. (2013). Privacy self-management and the consent dilemma," Harv L Rev, 7, 1880.

[Lu16] Lupton, D. (2016). The diverse domains of quantified selves: self-tracking modes and dataveillance. Economy and Society, 45 (1), 101–122. https://doi.org/10.1080/03085147.2016.1143726

[St22a] Statista. (2022). Most popular Google Play app categories 2021. https://www.statista.com/ statistics/279286/google-play-android-app-categories/

[St21] Statista. (2021). Google Play: number of available medical apps as of Q1 2021.https://www.statista.com/statistics/779919/health-apps-available-google-play-worldwide/

[St22b] Statista. (2022b). Most popular Google Play app categories 2021. https://www.statista.com/statistics/279286/google-play-android-app-categories/

[St21c] Statista, 2021c

[Ma16] Mai, J.-E. (2016). Big data privacy: The datafication of personal information. The Information Society, 32 (3), 192–199. https://doi.org/10.1080/01972243.2016.1153010

[Se15] Selinger, E. (2015). How obsessive self-tracking is eroding privacy for everyone. https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0923/How-obsessiveself-tracking-is-eroding-privacy-for-everyone

[HHG18] Henkel, M., Heck, T., & Göretz, J. (2018). Rewarding Fitness Tracking—The Communication and Promotion of Health Insurers' Bonus Programs and the Use of Self-tracking Data. Lecture Notes in Computer Science, 28–49. https://doi.org/10.1007/978-3-319-91485-5\{}3

[Aj20a] Ajana, B. (2020a). Metric Culture: Ontologies of Self-tracking Practices. Emerald Publishing.

[Du17] Duch-Brown, N., Martens, B., & Mueller-Langer, F. (2017). The economics of ownership, access and trade in digital data.

[Ma86] Mason, R. O. (1986). Four Ethical Issues of the Information Age. MIS Quarterly, 10 (1), 5. https://doi.org/10.2307/248873

[Ge18] George, R. T. D. (2018). Privacy, public space, and personal information. Core concepts and contemporary issues in privacy (pp. 107–120). Springer.

[We68] Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25 (1), 166.

[SMB96] Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly, 20 (2), 167. https://doi.org/10.2307/249477

[Ro21] Rollenhagen, L. (2021). Alan Westin is the father of modern data privacy law | Articles. https://www.osano.com/articles/alan-westin

[Vi18] Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy Attitudes and Data Valuation Among Fitness Tracker Users. Transforming Digital Worlds, 229–239.https://doi.org/10.1007/978-3-319-78105-1\{_}27

[Aj20b] Ajana, B. (2020b). Personal metrics: Users' experiences and perceptions of self-tracking practices and data. Social Science Information, 59 (4), 654–678. https://doi.org/10.1177/0539018420959522

[MB12] Mcafee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. Harvard Business Review (90:10), 61–67. https://wiki.uib.no/info310/images/4/4c/McAfeeBrynjolfsson2012-BigData-TheManagementRevolution-HBR.pdf

[Ko17] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers amp; Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

[Ch20] Chakravorti, B. (2020). Why It's So Hard for Users to Control Their Data. https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data

[BHL21] de Boer, I., Herder, E., & van Lieshoud, M. (2021). The Illusion of Control in Privacy Trade-Offs: Does Familiarity Play a Role? Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization. https://doi.org/10.1145/3450614.3464471

[So21] Solove, D. J. (2021). The Myth of the Privacy Paradox. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3536265

[Kh22] Khayretdinova, A., Kubach, M., Sellung, R., Roßnagel, H. (2022). Conducting a Usability Evaluation of Decentralized Identity Management Solutions. In: Friedewald, M., Kreutzer, M., Hansen, M. (eds) Selbstbestimmung, Privatheit und Datenschutz. DuD-Fachbeiträge. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-33306-5_19

[Ke22] Kerry, C. (2022). Why protecting privacy is a losing game today—and how to change the game. https://www.brookings.edu/research/why- protecting- privacy- is- a-losinggame-today-and-how-to-change-the-game/

[MC19] Mejias, U. A., & Couldry, N. (2019). Datafication. Internet Policy Review, 8 (4). https://doi.org/10.14763/2019.4.1428

[GNG13] Gimpel, H., Nißen, M., & Görlitz, R., R. (2013). Quantifying the quantified self: A study on the motivations of patients to track their own health. Proceedings of the 34th International Conference on Information Systems (ICIS). https://core.ac.uk/download/pdf/301361222.pdf

[Xu12] Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.

[GRS03] Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five personality domains. Journal of Research in Personality, 37 (6), 504–528. https://doi.org/10.1016/s0092-6566(03)00046-1

[Go93] Goldberg, L. R. (1993). The structure of phenotypic personality traits. American psychologist, 48 (1), 26

[EP16] En, B., & Pöll, M. (2016). Are you (self-)tracking? risks, norms and optimisation in selfquantifying practices. Graduate Journal of Social Science, 12, 37–57.

[Kr15] Kristensen, D. B., Bode, M., & Lim, M. (2015). The optimizing self. Workshop on interpretive consumer research, 8.

[WPG14] Whooley, M., Ploderer, B., & Gray, K. (2014). On the integration of self-tracking data amongst quantified self-members. Proceedings of the 28th International BCS Human Computer Interaction Conference (HCI 2014) 28, 151–160.

[Sh16] Sharon, T. (2016). Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. Philosophy amp; Technology, 30 (1), 93–121. https://doi.org/10.1007/s13347-016-0215-5

[An09] Angst, C. M. (2009). Protect my privacy or support the common-good? ethical questions about electronic health information exchanges. Journal of Business Ethics, 90 (2), 169–178.

[To21] Toesland, F. (2021). How Big Data can improve population health management. https://www.techerati.com/features-hub/opinions/how-big-data-can-improve-populationhealth-management/

[GS16] Gorm, N., & Shklovski, I. (2016). Sharing steps in the workplace: Changing privacy concerns over time. proceedings of the 2016 CHI conference on human factors in computing systems, 4315–4319.

[PC21] Pinchot, J., & Cellante, D. (2021). Privacy concerns and data sharing habits of personal fitness information collected via activity trackers. JISAR14, 4.

[So06] Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154 (3), 477. https://doi.org/10.2307/40041279

[Ne95] Netemeyer, Richard G., Scot Burton, and Donald R. Lichtenstein. "Trait Aspects of Vanity: Measurement and Relevance to Consumer Behavior." Journal of Consumer Research 21, no. 4 (1995): 612–26. http://www.jstor.org/stable/2489719.

[An16] Tatiana Anisimova, "Integrating Multiple Factors Affecting Consumer Behavior toward Organic Foods: The Role of Healthism, Hedonism, and Trust in Consumer Purchase Intentions of Organic Foods," Journal of Food Products Marketing 22, no. 7 (June 14, 2016): 809–23, https://doi.org/10.1080/10454446.2015.1121429.