Self-Tracking & Running a Marathon: Is your Privacy in Danger?

Jelizaveta Gordejeva[1], Andreas Mayer[2], Monika Pobiruchin[3]

Abstract: Running has become one of the most popular workout activities in the past years. Runners track themselves during training and big events like marathons races with dedicated wearable devices or smartphones. We analyzed freely accessible and supposedly anonymous respectively pseudonymous tracking data of three marathon events. Tracking data were collected by a single live GPS tracking provider, here Racemap. All data were publicly available. Thereby, we found out that it is possible to link these data sources with other public online resources to re-identify a person and to gather further sensible personal information (e.g., private or working addresses). Furthermore, we propose measures that participants, providers and organizers could carry out in order to ensure data privacy.

Keywords: self-tracking; data privacy; GDPR; wearables

1 Introduction

Beginning with the 1960s, running and jogging have become one of the most popular workout activities [SBB15]. In 2010, more than 800 marathon events were held worldwide [DT10] and one can assume that this number even increased. Today's world is dominated by technology and many runners use wearables, fitness trackers or smart watches to track their activity. Surveys among runners report that a vast majority (e.g. 73% for the Trollinger Marathon event [Wi18], 83% for the Half Marathon in Eindhoven [Ja17]) of race participants use technology to track their activities. Applications – mostly smartphone apps – designed for saving and displaying collected data do not fall behind on popularity, either.

In the context of European legislation, such tracking data falls under the Rules of General Data Protection Regulation (GDPR) [Eu16] as it is being gathered from and by natural persons. This means that individuals (data subjects) have – among others – the right of access (Art. 12, 15, 46 GDPR) to the stored personal data, the right to be informed (Art. 12-14 GDPR), and the right to erasure of personal data (Art. 17, 19 GDPR). Furthermore, some data collected by wearable devices, such as heart rate or electrocardiogram, is considered

[1] Department of Medical Informatics, Heilbronn University, Heilbronn, Germany, jelizaveta.gordejeva@hs-heilbronn.de
[2] Department of Medical Informatics, Heilbronn University, Heilbronn, Germany, andreas.mayer@hs-heilbronn.de
[3] GECKO Institute for Medicine, Informatics and Economics, Heilbronn University, Heilbronn, Germany & Consumer Health Informatics Special Interest Group, German Association for Medical Informatics, Biometry and Epidemiology, Cologne, Germany, monika.pobiruchin@hs-heilbronn.de

doi: 10.18420/sicherheit2024_009

health data and thus falls under special categories of personal data and requires special protection (see Art. 9 of the GDPR).

GPS tracking data generated during sports events like Marathons is often published online. Examples for this are various providers for live GPS tracking for endurance events, e.g., Follow My Challenge, Open Tracking, Racemap, ShareMyRun, and many others. These services are offered for event participants to track and record their run. The activity is often shared publicly via the provider's or the event's website. In general, the tracking is visible even after the date of the event. In a similar context, in 2018, The Guardian released an article about how the fitness tracking application Strava was inadvertently giving away locations of secret U.S. army bases [He18].

The release of personal health and fitness data can be dangerous for the data subjects and is – unless informed consent has been given – prohibited. Thus, the organizations and companies have to anonymize the data sets prior to publication. This is frequently done by removing explicit identifiers such as name, address and telephone number. However, even if the published data is said to be anonymous and key identifiers have been removed, there is still a possibility of re-identification. Users are often not aware of the "Fitness-Print" they leave in the digital world by entering their real name or allowing applications to track their location outside of race tracks and events.

This study aims to answer the following questions: (1) Is it possible to re-identify a person using publicly available and presumably anonymous or pseudonymous tracking information provided during marathon events? (2) Is it possible to gather further sensitive personal, e.g., (private) addresses, photos? (3) Based on question (1) and (2) for how many participants could a re-identification be conducted?

2 Related Work

In terms of health-related data research was conducted that shows the possibilities and dangers of re-identifications in medical datasets [Em11a; Em11b; Je20]. Prior to this in 2002, L. Sweeney showed that it is possible to establish a personal reference from supposedly anonymous data, and presented a model for the protection of such personal data [Sw02]. To prevent this possibility, L. Sweeney proposed the principle of K-Anonymity: a data set (e.g. organized as a table) with supposedly anonymous data is considered. The table consists of attributes which, in combination with an external source of information, can be linked in order to re-identify the persons concerned. If K-Anonymity is taken into account, each set of quasi-identifiers, e.g., gender, zip code, year of birth, etc., is repeated at least k-times. This makes it potentially more difficult to establish the personal reference by linking different data, since no subset of attributes matches fewer than k persons. In essence, the higher k, the "more anonymous" the data. Moreover, it is possible to improve or extend k-Anonymity by using e.g. l-diversity [Ma07] or t-closeness [LLV07].

The data privacy risk of fitness data collected with popular fitness platforms like Strava was addressed by [HHB18]. They "discover[ed] that 95.1% of moderately active users are at risk of having their protected locations extracted by an attacker". However, to the best of the authors' knowledge no similar study using live GPS tracking data of a public (marathon) event and related publicly available data sources was conducted before.

3 Methods

3.1 Data Sources & Analysis

We used data from four publicly available Internet resources to evaluate, if a personal reference can be established through linking said data: (1) Recorded maps by Racemap, (2) official race results lists, (3) Google Maps, (4) official photo services' websites, see Figure 1. All data was freely accessible without prior registration or authentication.

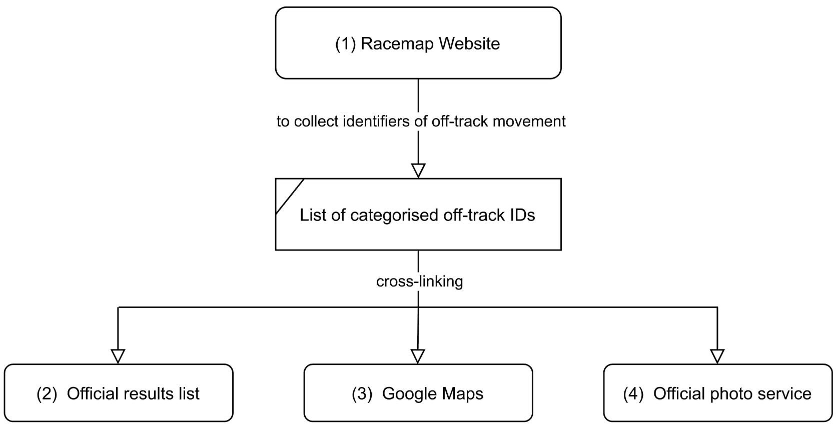

Fig. 1: Flowchart depicting the process of data analysis and the sources used.

The primary data source was the Racemap service [Ra21a]. The recorded data is displayed on a live tracking map, which is accessible via their website or smartphone application. Any interested person without prior registration or other special access can view those. Usually, the maps remain visible to the public even after the event has ended. The recording period of the tracking maps usually starts and ends several hours before and after the official start time of the race.

The collection of real-time data is voluntary. Participants decide for themselves if they want to use the tracking app during the race. If the participant decides to use this application, s/he must provide a name and the race number. Then the participant is visible on the live map (see Figure 2). During the race, viewers have the possibility to follow the participants in real time. Furthermore, viewers can search for a particular participant via the name or race number.

Fig. 2: Visualization of a single runner (identified by F5442) during the live map of the Trollinger Marathon 2019 event. Every white dot visible represents a recorded runner. The blue line denotes the official race track.

We considered three maps of regional and national marathon events provided by Racemap: Trollinger Marathon 2018 and 2019, Dresden Marathon 2019 [Ra18; Ra19a; Ra19c]. Each of this map was examined by one of the authors. Every data point that represents a single runner was followed throughout the entire recording period of the map. Every data point was assigned a number in ascending order. Off-track activity of relay runners such as driving to their respective starting points was not considered as this is intentional. If data points were recorded off the official race track or in the hours before or after the race they were classified into three categories:

- **A: Before the race.** An event that had occurred before the runner reached the track.
- **B: After the race.** An event that occurred after the runner had left the track.
- **C: Other.** An event that is difficult to describe because the speed of location change and distance traveled are too great. Presumably caused by technical difficulties, such as loss of GPS signal.

Different off-track recordings found in the categories A, B, C are grouped based on their location (see Figure 3), e.g., train station, parking lot, hospital, or specific activity of the person, e.g., driving on highway.

The official results lists of the marathon events [mi21a; mi21b; mi21c] that are published on the events' website were used for cross-linking. These lists contain information about name, surname, race number, age group, and association or organization a participant belongs to.

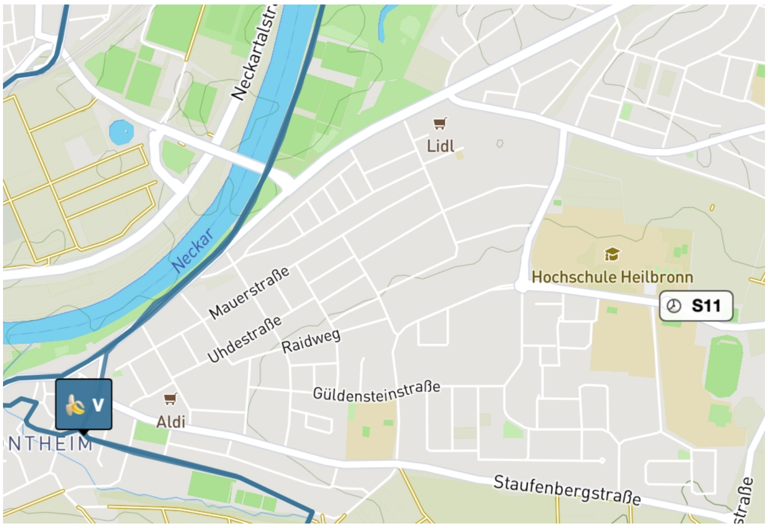

Fig. 3: Visualization of a single off-track (relay) runner (identified by S11) during the live map of the Trollinger Marathon 2019 event. The blue line denotes the official track.

Google Maps was used for address research. As Racemap does not provide the possibility to determine the exact address of a place, their maps are detailed enough to find the matching address using Google Maps.

Official event websites were accessed to look for photos of the race participants. Photos can be found through search function by entering the race number. All photos can be searched for without any additional authentication.

All data sources were accessed and analyzed between 01-06-2020 and 31-07-2020.

3.2 Ethics

The authors are well aware of the ethical and especially the data privacy issues of this research. Therefore, no offline/online download or storing of any personal information that might have occurred during the analysis was conducted. During the analysis, the authors only accessed publicly available data. Findings are only reported in an aggregated manner or with pseudonyms. Therefore, single persons cannot be identified. Racemap GmbH, the primary data source, was contacted prior the analysis and the aim of the study and study's purpose were described. Furthermore, we responsibly disclosed our findings to Racemap GmbH.

4 Results

4.1 Principal Findings

We analyzed the tracking data from the participants of three marathon events. For the events Heilbronn Trollinger Marathon 2018 and 2019, a full analysis of all participants was carried out. For the Dresden 2019 marathon, we investigated ten randomly chosen participants.

It was possible to re-identify persons using publicly available and presumably anonymous or pseudonymous tracking information. Moreover, it was possible to gather further personal data: addresses (private and work) and photos. Out of 11,169 Trollinger Marathon (in years 2018 & 2019 combined) participants, 501 (4.5%) used Racemap to track their activity. Among them, 15.4% (77/501) have recorded activity off-track. Out of those, 12.4% (62/501) have provided their surname and first name to Racemap service, which made the re-identification using other data sources possible, and 11.8% (59/501) have inadvertently given away a possible private or work address.

4.1.1 Trollinger Marathon 2018

Overall 5,623 runners participated in the Trollinger Marathon 2018. Out of those 3.4% (189/5,623) tracked their activity during the race using Racemap.

Results are individually presented in the Table 1 in the appendix. Among runners that were signed into Racemap during the marathon 29 had tracked activity outside of the race track. It was possible to distinguish 21 private addresses (presumably residential addresses) and two possible work addresses. That is 12.2% of the users. Of special note: Recordings also showed two persons that were located in or nearby the local hospital. As these observations were made before the race, it may also be the workplace of the persons. Out of those 29 participants, 25 have signed in using their surname and first name and the rest only provided their first name.

4.1.2 Trollinger Marathon 2019

Overall 5,546 runners took part in the Trollinger Marathon 2019. Out of those 5.6% (312/5,546) used Racemap application for tracking. The individual results are presented in Table 2 in the appendix. Out of all participants that used Racemap, 48 have tracked some kind of off-track activity. Among these recorded activities, we could establish 28 private addresses (presumably residential addresses) and 8 possible work addresses. This is 11.5% of the Racemap users. 37 participants out of 48 used the surname and first name to sign into Racemap application. One participant used a pseudonym, that could not have been linked to a name. Another 10 participants used either their surname or their first name. Interestingly, one recording was shown in the hospital after the race.

4.1.3 Dresden Marathon 2019

There were 7,892 participants in the Dresden marathon 2019. Out of those 18.2% (1,439/7,892) have signed into Racemap. Because of the high number of Racemap users, it was not possible to manually follow every participant throughout the map. Therefore, we provide the individual results of ten sample participants in Table 3 in the appendix. The sample was chosen randomly out of those runners that have recorded activity outside the racetrack. In this sample, it was possible to establish six private addresses (possible living addresses) and one possible work address.

4.2 Other Personal Data Found

It was possible to establish the age group of each participant using the official websites of the events. Furthermore, information about an organization (e.g. Heilbronn University), club, or company a runner is associated with is accessible through this sources. Thus, the participants' workplace could be revealed easily.

Moreover, Internet resources that contain official photos of event participants are freely accessible. Photos of runners can be accessed through their race number; no further authentication was required.

A random sample of ten participants of events Trollinger Marathon 2018 and 2019, as well as Dresden Marathon 2019 was analyzed. We found photos of nine participants from the sample.

5 Discussion

5.1 Principal Findings

Our results show that, that it is possible to link an anonymous or pseudonymous – depending on the runners' individual input – GPS tracking data source with personal information, such as name, addresses and photos. If runners are not cautious and tracking is activated even outside the track, they might inadvertently give away their private and/or work addresses. Moreover, the photos of participants published by the marathon organizers pose a breach of privacy, as every photo is accessible through a unique race number. The race number itself is easily available via the organizer's website. Thus, everyone can retrieve a photo of any participant, even of children or prominent figures like politicians including their guards. Some platforms still display photos from events that took place in 2014 and 2012. Overall, it did not take much effort to analyze all provided data sources and link anonymous and pseudonymous data with personal information. Participants of running events give consent to every single service and platform and be well-informed about which data is published before, during, and after a marathon event. The authors would also like to point out that every service evaluated, operates in terms with the GDPR or similar legal frameworks. However, users, event organizers, and service providers seem to be not aware of the possibility of combining different data sources. Especially, users (runners) may be not aware about the possibility – and the little effort – on how personal data like private addresses, workplaces, or even hospital stays after an injury can be disclosed.

Based on our findings, we suggest the following measures for users, platform providers and organizers of marathons.

5.2 Suggestions for Users

1. Carefully read the privacy policy instead of just accepting the terms.
2. Provide pseudonymous data instead of personal information when registering to a tracking application. This could be a nickname or the race number to make cross-linking more difficult.
3. Manually turn off GPS services when not on track.
4. Delete the application and the corresponding account if it is no longer needed to avoid unwanted tracking.

5.3 Suggestions for Providers

Tracking providers can as well protect their users privacy. If providers implement a safety mechanism, e.g. a GPS corridor, even those users that are not being cautious, will have their private address protected. The corridor could filter all incoming location signals and display only those users that are on track or very close to the track. Even such thing as less detailed map display could make the exact address finding more complicated or impossible.

Furthermore, application providers could inform their users and warn them about shared data that will be made public. This could potentially raise more awareness and encourage users to be more considerate about their privacy.

5.4 Suggestions for Organizers

Raising awareness of participants about their data privacy is an important step that can be implemented by event organizers. Currently, organizers of e.g. Trollinger Marathon only encourage participants to use the tracking applications, but do not warn them about possible threats to privacy. The available information resources contain instructions on how to use the applications. No warning is given about when to turn GPS services on and start tracking or how to check if the application is still tracking one's location if a participant is no longer on track.

Furthermore, organizers could choose alternative solutions. There are providers that offer technologies that eliminate the possibility of tracking outside the track. Racemap, whose data sources were used in this analysis, offer such possibility. This technology is called Predictive Live Tracking: an algorithm calculates location and speed of every participant – based on prediction and "AI-based corrections" [Ra21b] – and visualizes these on the map [Tr19]. In comparison to technology used in the analyzed races, where every participant had a GPS tracker and was therefore followed in real time, this one only depicts users on the track of the event. Not a single user is tracked outside of it. An example of event using this technology is Generali München Marathon 2019 [Ra19b].

Another threat to participants' privacy are photos accessible online. These photos are accessible even almost 10 years after the event took place and are exposed to everyone. Organizers could mitigate this by assigning every participant a secret PIN code together with the race number. This PIN should then be used to access the photos in the marathon gallery. This would protect the participants, which is essential. Especially, for children and prominent personalities, whose photos are also being taken during the marathon, the question of privacy is important. It should be possible to opt out of photos. The photographers could get a list of race numbers of participants, that must not be photographed. Or at least these photos must not be published. Last but not least, the photographs should not be accessible after such a long period of time. The privacy policy of the Marathon-Photos service [Ma20] that still has images from the event of 2012, does not consider images personal information. Although their privacy policy states, that all personal data is deleted at the end of the calendar year, it only refers to name, Email address and gender. This should be changed and photos should be deleted according to the EU-GDPR regulations.

5.5 Limitations

Limitations of this publication include manual analysis process, which is quite time consuming and does not exclude the possibility of mistakes. An automatic evaluation of maps and other data sources could be beneficial in this context. Manual analysis was only possible for several hundred participants. A larger sample would allow better generalization of results.

Furthermore, this study only focused on one provider of live tracking, e.g., Racemap, which might be not generalizable for all other existing tracking applications. However, other providers use similar technology, namely GPS tracking and we strongly assume that the problem about involuntary tracking persists. The services evaluated in this study are not restricted to events organized in Germany, either.

We can only assume that the GPS-located off-track position of a person before and after a race represents their private / residential address. No cross-check of name of the persons and official records, e.g., telephone books, were conducted. However, we assume the probability that the residential address was disclosed is high. Especially if the address was observed before and after the race.

The study results and address look-up are based on the accuracy of the GPS-tracking. Some recordings indicate that there were some GPS-signal losses and/or mis-readings (see Table 1).

5.6 Comparison With Prior Work

In their demonstration study Jedrzejczyk [Je09] could re-identify $n = 3$ study subjects just by analyzing anonymous "location-based social networking application". Because of the small sample size in this study this should only be considered a feasibility study. However, using publicly available location data is similar to our study setting.

Emam et al [Em11b] conducted a systematic review about re-identification attacks on health data as well as other types of data, e.g., movie ratings or posts from social networks. Overall, they report that approximately one quarter (0.26) of these records could be re-identified. However, the confidence interval was quite large: $0.046 - 0.478$. This re-identification success rate is similar to our findings with 12.5% and 11.5% for the two Trollinger Marathons.

6 Conclusions

The results of our study show that self-tracking while running a marathon can inadvertently expose the runners' identity from public tracking data sets. By combining the tracking data with freely available data sources, further sensitive personal information, such as private addresses and pictures of the runners may be revealed. In future, the trend for self-tracking with technology will proliferate. Therefore, it is necessary to raise the awareness to privacy issues. The EU-GDPR aims to reach a high level of privacy but as shown this can only be achieved if all stakeholders apply proper measures. Our paper is a first step towards this.

References

[DT10] Day, S. M.; Thompson, P. D.: Cardiac Risks Associated With Marathon Running. Sports Health: A Multidisciplinary Approach 2/4, pp. 301–306, 2010.

[Em11a] Emam, K. E.; Jonker, E.; Arbuckle, L.; Malin, B.: A Systematic Review of Re-Identification Attacks on Health Data. PLoS ONE 6/12, e28071, 2011.

[Em11b] Emam, K. E.; Paton, D.; Dankar, F.; Koru, G.: De-identifying a public use microdata file from the Canadian national discharge abstract database. BMC Medical Informatics and Decision Making 11/1, 2011.

[Eu16] European Commission: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016, URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[He18] Hern, A.: Fitness tracking app Strava gives away location of secret US army bases. The Guardian/, 2018, URL: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases, visited on: 11/07/2023.

[HHB18] Hassan, W. U.; Hussain, S.; Bates, A.: Analysis of Privacy Protections in Fitness Tracking Social Networks-or-You can run, but can you hide? In: SEC'18: Proceedings of the 27th USENIX Conference on Security Symposium. USENIX Association, pp. 497–512, 2018.

[Ja17] Janssen, M.; Scheerder, J.; Thibaut, E.; Brombacher, A.; Vos, S.: Who uses running apps and sports watches? Determinants and consumer profiles of event runners' usage of running-related smartphone applications and sports watches. PLOS ONE 12/7, e0181167, 2017.

[Je09] Jedrzejczyk, L.; Price, B. A.; Bandara, A. K.; Nuseibeh, B.; Hall, W.; Keynes, M.: I know what you did last summer: risks of location data leakage in mobile and social computing. Department of Computing Faculty of Mathematics, Computing and Technology The Open University/, pp. 1744–1986, 2009.

[Je20] Jeon, S.; Seo, J.; Kim, S.; Lee, J.; Kim, J.-H.; Sohn, J. W.; Moon, J.; Joo, H. J.: Proposal and Assessment of a De-Identification Strategy to Enhance Anonymity of the Observational Medical Outcomes Partnership Common Data Model (OMOP-CDM) in a Public Cloud-Computing Environment: Anonymization of Medical Data Using Privacy Models. Journal of Medical Internet Research 22/11, e19597, 2020.

[LLV07] Li, N.; Li, T.; Venkatasubramanian, S.: t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In: 2007 IEEE 23rd International Conference on Data Enginering. IEEE, 2007.

[Ma07] Machanavajjhala, A.; Kifer, D.; Gehrke, J.; Venkitasubramaniam, M.: L-diversity: Privacy beyond k-anonymity. 1/1, 3–es, 2007.

[Ma20] Marathon-Photos: Marathon-Photos Privacy Policy, English, 2020, URL: https://static.marathon-photos.com/Marathon-Photos-Privacy-Policy.pdf, visited on: 11/07/2023.

[mi21a] mika:timing GmbH: 18. Heilbronner Trollinger Marathon, Deutsch, 2021, URL: https://trollinger.r.mikatiming.de/2018/?pid=start, visited on: 11/07/2023.

[mi21b] mika:timing GmbH: 19. Heilbronner Trollinger Marathon, Deutsch, 2021, URL: https://trollinger.r.mikatiming.de/2019/?pid=start, visited on: 11/07/2023.

[mi21c] mika:timing GmbH: Starterliste: Alle. Dresden Marathon 2019. Deutsch, 2021, URL: https://dresden.r.mikatiming.de/2019/?pid=startlist%5C_list, visited on: 11/07/2023.

[Ra18] Racemap GmbH: Racemap Trollinger Marathon 2018, English, 2018, URL: https://racemap.com/player/trollinger-marathon%5C_2018-05-06/, visited on: 07/21/2021.

[Ra19a] Racemap GmbH: Racemap Dresden Mararthon 2019, English, 2019, URL: https://racemap.com/player/dresden-marathon-2019%5C_2019-08-30/%5C#events=0, visited on: 07/21/2021.

[Ra19b] Racemap GmbH: Racemap Generali München Marathon 2019, English, 2019, URL: https://racemap.com/player/generali-muenchen-marathon-2019%5C_2019-10-07/, visited on: 07/21/2021.

[Ra19c] Racemap GmbH: Racemap Trollinger Marathon 2019, English, 2019, URL: https://racemap.com/player/trollinger-marathon-heilbronn%5C_2019-05-05/, visited on: 07/21/2021.

[Ra21a] Racemap GmbH: About Racemap, English, 2021, URL: https://racemap.com/about-us, visited on: 11/07/2023.

[Ra21b] Racemap GmbH: Racemap. Features: Predictive Tracking of all participants, English, 2021, URL: https://racemap.com/features#predictive-live-tracking.

[SBB15] Scheerder, J.; Breedveld, K.; Borgers, J.: Who Is Doing a Run with the Running Boom? In: Running across Europe. Pp. 1–27, 2015.

[Sw02] Sweeney, L.: K-Anonymity: A Model for Protecting Privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10/5, pp. 557–570, 2002.

[Tr19] Treppe, K.: Powerful Live Tracking at München Marathon, English, 2019, URL: https://racemap.com/blog/powerful-live-tracking-at-munchen-marathon, visited on: 11/07/2023.

[Wi18] Wiesner, M.; Zowalla, R.; Suleder, J.; Westers, M.; Pobiruchin, M.: Technology Adoption, Motivational Aspects, and Privacy Concerns of Wearables in the German Running Community: Field Study. JMIR Mhealth Uhealth 6/12, e201, 2018.

A Result Table for Trollinger Marathon 2018

	Before the race (A)						After the race (B)					Other (C)		
Observation	parking lot	private address	work address	driving	hospital	other location	private address	work address	driving	other location	back at track	disappeared	no movement	**Found Address**
1	•	•	–	–	–	–	–	–	•	–	–	–	–	√
2	•	–	–	–	•	–	–	–	•	–	–	•	–	
3	–	–	•	–	–	–	–	•	–	•	•	–	–	√
4	•	•	–	–	–	–	•	–	–	–	–	–	•	√
5	–	•	–	•	–	–	–	–	–	–	–	–	•	√
6	–	–	•	–	–	–	•	–	–	–	–	–	–	√√
7	–	–	–	–	–	–	•	–	–	–	–	–	–	√
8	–	•	–	–	–	–	–	–	–	–	–	–	–	√
9	–	–	–	–	•	–	–	–	–	–	–		–	
10	–	•	–	–	–	–	•	–	–	–	–	–	–	√
11	–	•	–	–	–	–	–	–	–	–	–	–	–	√
12	–	–	–	–	–	•	–	–	–	–	–	–	–	
13	–	–	–	•	–	–	–	–	–	–	–	–	–	
14	–	–	•	–	–	–	–	–	–	–	–	–	–	√
15	–	•	–	–	–	–	–	–	–	–	–	–	–	√
16	–	–	–	–	–	–	•	–	–	–	–	–	–	√
17	–	–	–	–	–	–	•	–	–	–	–	–	–	√
18	–	–	–	–	–	–	–	•	–	–	–	–	–	√
19	–	–	–	–	–	–	•	–	–	–	–	–	–	√
20	–	–	–	–	–	–	•	–	–	–	–	–	–	√
21	–	–	–	–	–	–	•	–	–	–	–	–	–	√
22	–	–	–	–	–	–	•	–	–	–	•	–	–	√
23	–	–	–	–	–	–	–	–	–	•	–	–	–	
24	–	–	–	–	–	–	•	–	–	–	–	–	–	√
25	–	–	–	–	–	–	–	–	•	–	–	–	–	
26	–	–	–	–	–	–	–	–	–	•	–	–	–	
27	–	•	–	–	–	–	–	–	–	–	–	–	–	√
28	–	•	–	–	–	–	–	–	–	–	–	–	–	√
29	–	•	–	–	–	–	–	–	–	–	–	–	–	√
∑	3	10	3	2	2	1	11	2	3	3	2	1	2	23

Tab. 1: Observed event categories (A, B, C) of Heilbronn Trollinger Marathon 2018 participants using Racemap. Entries ’private address’ and ’work address’ refer to addresses that were discovered during the analysis. Specific addresses were omitted in the table to respect the right to data privacy of the participants. Surnames and first names are therefore not provided in the table, either.

B Result Table for Trollinger Marathon 2019

	Before the race (A)						After the race (B)					Other (C)	
Observation	hospital	train station	private address	work address	driving	other location	private address	work address	driving	other location	hospital		**Found Address**
1	–	•	•	–	–	–	–	–	–	–	–	–	√
2	–	–	•	–	–	–	•	–	•	–	–	–	√
3	–	–	•	–	–	–	–	–	–	–	–	–	√
4	–	•	•	–	–	–	–	–	–	–	–	–	√
5	–	–	–	•	•	–	–	–	–	–	–	–	√
6	–	–	•	–	–	–	–	–	–	–	–	–	√
7	–	–	•	–	–	–	–	–	–	–	–	–	√
8	–	–	•	–	–	–	–	–	–	–	–	–	√
9	–	–	–	•	–	–	–	–	–	–	–	–	√
10	–	–	•	–	–	–	–	–	–	–	–	–	√
11	–	–	•	–	–	–	–	–	–	–	–	–	√
12	–	–	–	–	–	•	–	–	–	–	–	–	
13	–	•	–	–	–	•	–	–	–	–	–	–	
14	–	–	•	–	–	–	–	–	–	–	–	–	√
15	–	–	•	–	–	–	–	–	–	–	–	–	√
16	•	–	–	–	–	–	–	–	–	–	–	–	
17	–	–	•	–	–	–	–	–	–	–	–	–	√
18	–	–	–	•	–	–	–	–	–	–	–	–	√
19	–	–	•	–	–	–	–	–	–	–	–	–	√
20	–	–	–	–	–	–	•	–	–	–	–	–	√
21	–	–	–	–	–	–	–	–	•	–	–	–	
22	–	–	–	–	–	–	–	–	–	–	•	–	
23	–	–	•	–	–	–	–	–	–	–	–	–	√
24	–	–	–	–	–	–	•	–	–	–	–	–	√
25	–	–	–	–	–	–	–	–	•	–	–	–	
26	–	–	–	–	–	–	–	–	•	–	–	–	
27	–	–	–	–	–	–	–	–	•	–	–	–	
28	–	–	–	–	–	–	–	–	•	–	–	–	
29	–	–	–	–	–	–	•	–	–	–	–	–	√
30	–	–	–	–	–	–	•	–	–	–	–	–	√
31	–	–	–	–	–	–	•	–	–	•	–	–	√

32	–	–	–	–	–	–	–	•	•	–	–	–	√
33	–	–	–	–	–	–	–	•	–	–	–	–	√
34	–	–	–	–	–	–	–	•	–	–	–	–	√
35	–	–	–	–	–	–	–	•	–	–	–	–	√
36	–	–	–	–	–	–	•	–	–	–	–	–	√
37	–	–	•	–	–	–	–	–	–	–	–	–	√
38	–	–	–	–	–	•	–	–	–	–	–	–	
39	–	–	–	–	–	•	–	–	–	–	–	–	
40	–	–	–	–	–	–	•	–	–	–	–	–	√
41	–	–	•	–	–	–	–	–	–	–	–	–	√
42	–	–	–	–	–	–	–	–	•	–	–	–	
43	–	–	•	–	–	–	–	–	–	–	–	–	√
44	–	–	•	–	–	–	–	–	–	–	–	–	√
45	–	–	–	–	–	–	•	–	–	–	–	–	√
46	–	–	–	–	–	–	•	–	–	–	–	–	√
47	–	–	–	•	–	–	–	–	–	–	–	–	√
48	–	–	–	–	–	–	•	–	–	–	–	–	√
∑	1	3	18	4	1	4	11	4	8	1	1	0	36

Tab. 2: Observed event categories (A, B, C) of Heilbronn Trollinger Marathon 2019 participants using Racemap. No recordings in category C were observed.

C Result Table for Dresden Marathon 2019

	Before the race (A)	After the race (B)				Other (C)	
Observation	private address	private address	work address	driving	other location		**Found Address**
1	–	•	–	–	–	–	√
2	–	•	–	–	–	–	√
3	–	–	•	–	–	–	√
4	–	–	–	•	–	–	
5	–	–	–	•	–	–	
6	–	–	–	–	•	–	
7	•	–	–	–	–	–	√
8	•	–	–	–	–	–	√
9	•	–	–	–	–	–	√
10	•	–	–	–	–	–	√
∑	4	2	1	2	1	0	7

Tab. 3: Observed event categories (A, B, C) of Dresden 2019 Marathon - random sample of participants using the tracking service Racemap.