International Working Group
on Data Protection
in Telecommunications

675.57.15

Working Document on Wide Area Location Tracking[1]

64th meeting, 29-30 November 2018 (Queenstown)

Scope

1. The Working Group has previously identified risks related to location tracking, adopting common position documents on privacy and location information in mobile communications services[2].

2. New applications have emerged in recent years, with the potential for wide adoption, that are capable of posing specific new risks to the privacy of individuals. Take, for example, the broadcasting of location data from devices installed in our cars, or from the vehicles themselves. These data can be used to improve road use efficiency, thereby reducing CO_2 emissions, or to improve the safety of drivers and pedestrians. Similarly, within the broad category of "smart city" services, a frequent exchange of data between citizens' devices and a plurality of service providers is envisaged in order to create public benefits, like making public services more effective and cost efficient. Many of these applications rely on being constantly connected, thus enabling individuals' movements to be tracked.

3. This Working Paper examines the data protection and privacy risks associated with large scale collection of location data in the public interest, giving recommendations for their lawful implementation and on possible technical and organizational arrangements in order to mitigate these risks.

Background

4. Physical location tracking, namely the ability of modern technology to follow individuals' movements and keep a record of them, is an area where people's real and virtual lives meet. Being connected to a service provider from a specific georeferenced place (given, for

[1] The Office of the Privacy Commissioner of Canada abstains from the adoption of this Working Paper.

[2] Common Position on Privacy and location information in mobile communication services (updated Berlin, 18./19.11.2004), and Working Paper on Location Tracking from Communications of Mobile Devices (Berlin, 13./14. October 2015)

instance, by the spatial coordinates used by the GPS embedded in the application), we attach a real, physical dimension (the place where we are) to our virtual sphere (the action we are performing while connected).

5. These streams of location data, being shared at least with the service provider to which we are connected and possibly to other third parties, reveal our mobility pattern and offer new opportunities for predicting our next move, either in the physical or virtual sphere. If our locations are known, then not only our past behavior is revealed, we can also be directed towards specific locations, based on our previous service usage (e.g., to stop at the nearby shop where a given item we are searching for online can be found), or on our previous route (e.g., to stop at the nearby gasoline station because we are low on fuel).

6. The trend toward including predictive capacity is likely to continue, and the number of tracking applications is set to increase, due to the many devices that we carry and wear, and to the increasing number of objects capable of registering our location history. In the past walking, driving, riding a bicycle or jogging were activities with very limited risks of being tracked. However, they are now becoming increasingly connected activities, and being tracked is becoming the norm.

7. The International Working Group on Data Protection in Telecommunications recognizes that there might be a genuine public interest in discovering some patterns from mobility flows which can be of broad and collective interest, but this must be balanced with safeguards for the rights and freedoms of the involved individuals.

8. If no safeguard is in place, the main risk will be the creation of a strong bias: that our being guided (or forced) into doing certain things and going certain places, based on a service provider's assumptions about our needs is the best way to meet them. This approach is questionable, at best, reducing or eliminating the opportunities for individuals to make free discoveries.

9. This concern is exacerbated by the consideration that location tracking in many circumstances is an undetectable activity. Although we can still, to a limited extent, control the devices that we carry and wear, it is not possible for individuals to control who eventually has access to that data and what their use will be beyond providing connectivity and communication functionalities. There is an inherent lack of people's capability to control the increasingly sensors equipped active space surrounding them that is very difficult to mitigate. Traditional data protection safeguards like notice and consent do not easily apply in these circumstances.

10. New concepts are emerging in the data protection legal framework, in addition to the consolidated principles of data protection, which might prove much more effective in this context. These include accountability, or the commitment taken by the data controller to ensure and demonstrate to external stakeholders (data subjects, data protection authorities) full compliance with data protection principles in practice and to respect individuals' personal sphere.

11. Privacy by design is another relevant tool to engineer the processing operations in such a way that safeguards for individuals are integrated in the processing itself from the earliest stages of the design of a product, application or service.

Personal data

12. The identifiability of location data is well known[3]: just a few points in a path are enough to single out an individual in a population with a high degree of precision, taking into account the mostly regular patterns of people's mobility. The availability of other metadata, like timestamps, or of other technical parameters and configuration settings of software and applications increases the identifiability of location data. So does the presence of further contextual elements, like the sparsity of the area, the daytime or a peculiar sequence of events. Finally, the availability of location data from other sources, may allow for the combination of supposedly anonymous location data sets in a way that renders them identifiable.

13. Location data may, under certain circumstances, also reveal very sensitive individuals' attributes, like religious beliefs (if one end of a location path is a worship place), or pathologies (if one end of the path is a hospital), especially if recurrent mobility patters can be identified in one's history of movements.

Privacy risks

14. Location tracking can be a silent operation, and lack of transparency on the identity of the data controller or on the purpose of the processing is a major source of privacy risks for individuals. The device owner may not be aware that the data emitted from his devices, which is being provided for the purpose of being connected, or for getting a service from a provider, can also be collected over time to record his or her movements. Individual awareness is not sufficient to mitigate such risks, simply because in many cases the only way to avoid tracking is to disconnect, or refrain from using a service.

15. The reuse of data for purposes beyond the original scope, is another privacy risk, threatening full respect of the purpose limitation principle..

16. Location data, combined with data from other sources, may extend the tracking beyond line of sight, over large scales and for prolonged times, and can allow predicting the physical location of individuals. This entails risks for individuals not only in their digital sphere, but in

[3] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

their real lives, generating an uncomfortable sense of surveillance or chilling effects, deterring individuals from participation in some activities or use of some products and potentially providing elements for stalking, blackmailing, thefts.

17. Analysis of location data may create negative externalities also for other individuals. Inference on the context where location data were generated, or on the way groups or networks of individuals are created may potentially put at risk also other individuals[4], or allowing revealing sensitive areas[5].

18. Lack of trust is another privacy risk inherent to tracking individuals' movements. If controllers are not trustworthy, data can be processed in a non-neutral way inducing individuals to accomplish specific actions (in their real life sphere or in their digital sphere) which are more in the interest of the observer than the in the interest of the individual him/herself.

19. Forced adoption is another risk for individuals' freedoms. Triggering adoption of location tracking for purposes of public interest does not equal imposing adoption. Potential benefits per se should incentivize citizens, for instance, to adhere freely to smart city applications or similar services.

20. There is a risk that organizations insufficiently anonymize location data after they finish legitimate processing in order to preserve their utility. This may lead to processing of that data for incompatible reasons although the data or a portion thereof might still be identifiable.

Recommendations

Recommendations to Organizations

21. Organizations contemplating the processing or location for purposes of public interest data should ensure that they have an appropriate legal basis, in their respective jurisdiction, for any such processing. In this respect, transparency on the purpose and on the way data are processed are a necessary prerequisite for the implementation of any valid legal basis.

[4] In a very famous research experiment New York taxi drivers details were extracted from the allegedly anonymised datset of taxi routes, made available by the municipality. With some post-processing on other metadata (locations and timestamps) and cross check with other available data sources (e.g. the occurrence of public events in a certain venue) it was also possible to reveal the identity of the passengers in the taxies, https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn

[5] U.S. soldiers are revealing sensitive and dangerous information by jogging, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.9aa09730e4ba

22. Organizations implementing any combination of location data with other sources of information (e.g., internet browsing data, transaction history, loyalty cards) on an identified or identifiable person, or any combination of multiple device identifiers that can be associated to a single individual to further increase the effectiveness of tracking (e.g., multiple smart phones, tablets and fitness bands linked to the same individual) should be based on the individual's informed consent.

23. Organisations should not share location data with third parties without the valid informed and specific consent of the individual concerned or as compelled under law.

24. Organizations should conduct a Data Protection Impact Assessment to identify any specific privacy risks related to the large scale processing of location data. They should also implement appropriate measures to address and mitigate such risks.

25. Organisations are encouraged to adopt privacy by design mechanisms made available by industry, ex ante and during the processing operations, in order to ensure effective safeguards to individuals and mitigate any privacy risk.

26. Assessments of the need to notify authorities and individuals of security incidents affecting location data should be paid due regard taking into account the inherent high risk of the data

27. Once the purpose has been accomplished, organizations should promptly delete, also via automated procedures, or anonymize location data. The anonymization method applied should be proven to be reliable and regularly reviewed. If large sets of location data are anonymized, then re-identification should not be possible with reasonable effort for all people concerned, even those with unusual movement patterns. If location data is aggregated in order to anonymize it, then the usual measures of anonymity apply (k-anonymity, l-diversity, t-closeness).

Recommendations to Industry

28. Device manufacturers and software developers should develop appropriate mechanisms to proactively notify individuals about location tracking;

29. Device manufacturers and software developers should provide individuals with periodic reminders (just-in-time notices) that location tracking is taking place;

30. Device manufacturers and software developers should engineer and make available privacy by design options (such as noise injection, other methods to ensure differential privacy, the introduction of air gaps) in order to reduce the identifiability of location data.

31. Device manufacturers and software developers should engineer and make available privacy by design options like the use of temporary pseudonyms (device IDs, PKI certificates), with

an adequate refresh frequency, in order to avoid long range tracking, beyond what is necessary for any scope of public utility (like road accidents detection, transport optimization etc.).

32. Device manufacturers and software developers for location tracking applications should promote codes of conduct, endorsed by industry associations and appropriate to the intended use and application.

33. Device manufacturers and software developers should provide mechanisms whereby individuals can select the tracking options (timing, frequency, locations and so on) that best fit their preferences.

34. By default, location services should be switched off. Users should be given the opportunity, through easily accessible and prominently displayed dashboards, to delete all or part of the previously collected data.

Recommendations to regulators

35. Regulators should promote the enactment of trust in the organizations implementing location tracking mandating transparency on the processing operations and the adoption of best practices, and through careful and periodic checks on their operations by means of requirements to be audited.

36. Regulators should promote the enactment of trust in the use of devices and application through the scrutiny of certification schemes and codes of conduct. On the other hand, they should warn consumers against the use of privacy unfriendly services.