José Donato
2016225043
donato@student.dei.uc.pt

CASE STUDY #2
Tracking Unmodified Smartphones Using Wi-Fi Monitors

SP
2020/08/20

1 The Problem

This paper [1] presents a strategy to track smartphones by deploying wi-fi monitoring equipment. By deploying seven 70 dollar access points in a certain area they were able to track people positions only using Wi-Fi without modifying their mobile phones configurations. In a small test, within 12-hour period, 23k unique devices were traced producing GPS-equivalent routes with mean error of 67 meters. This number can be further reduced by increasing the number of detections made of a given phone (of course, increasing the number of monitors - access points). The denser the monitors are positioned, the better the results will be.
This is an interesting approach to track user positions and routes but like so many other alternatives it constitutes a privacy problem. After each device detection in the monitor (access point), the data is forwarded to a central server second-by-second. The transmissions are identified by the unique MAC address from each phone. This can result in a problem because any person with background knowledge of someone's MAC address can easily get access to this person's positions by analysing the saved data (that contains all the MAC addresses and the corresponding set of positions).

2 Question A: Can a company using such approach be fined?

In the example presented, private information of each person in a certain area is saved to a central server without their clear consent. It is easy to imagine a situation where some company can benefit from such information: shopping center analysing the customers' common routes in their areas. Such approach without any type of consent would be easily considered privacy invasion. Of course, this would not be a problem if the customers would have been previously informed and agreed to such strategy. To sum up, at least in Europe, storing users private information (localization) without their consent would be punishable by fine because of General Data Protection Regulation (GDPR) [2]. Since this is exactly what happens in the paper [1], the company using such strategy would surely be fined.

3 Question B: How to anonymize a dataset of this nature?

Before answering this question we need to understand what the output's nature of this study would be. After tracking the positions of smartphones during one day, the resulting dataset would be, naturally, records containing unique identifiers (device's MAC address) and its corresponding set of detected positions by the monitors. With some background knowledge (knowing that some MAC address belongs to an individual) an attacker can easily identify the routes taken by that person. One obvious solution to anonymize such dataset would be differential privacy: by adding noise to each added record (the position of a smartphone at a given time), the privacy of each record's routes would be preserved without destroying the utility of the dataset. Of course this solution does not protect against record-linkage, i.e., if the attacker tries to identify whether one person is in the dataset or not. To solve this, other privacy algorithms need to be used - k-anonymity, for example.

References

[1] Musa, A. B. M., and Jakob Eriksson. "Tracking unmodified smartphones using wi-fi monitors." Proceedings of the 10th ACM conference on embedded network sensor systems. 2012.

[2] General Data Protection Regulation (GDPR) – Official Legal Text `https://gdpr-info.eu/`