1.1 Tracking and Data Collection Techniques

1.1.1 Stingray (IMSI Catcher)

IMSI (International Mobile Subscriber Identity) catchers, so called stingrays, are fake cell phone towers which are tricking mobile phones into connecting with them. After the connection is established the stingray collects identifaction and location data and is even able to eavesdrop phone calls, text messaging and web browsing. It is believed that some kind of stingrays are even used against protests, like the BLM movement in the year 2020, so law enforcement can later identify participants which were present at those "gatherings". It is even possible for private companies or any private citizen to build these stingrays on their own [Vel20].

Because most stingrays are used by the government to exploit the rich source of data in order to aid their investigations they are setting up these stingrays because the standard procedure involves going to court and obtain phone records from a wireless carrier which can take a long time. Because these stingrays not only collect data from the targeted device but from any device in the area the simulation of cell towers have become a source of controversy over the time. In the US several states already have laws against the usage of IMSI catchers, but most often the use is kept a secret and therefore is hard to be prosecuted. The start of stingrays can be traced down to the CIA having problems to get local and national telecommunications companies to cooperate with US surveillance operations. Therefore the Harris Corporation sold the US military and intelligence agencies the cell site simulators. After these branches were saturated the Harris Corp. sold those stingrays to other federal agencies, until even the state and local law enforcements got a hand on IMSI catchers. [IMS].

1.1.2 Information Branching via Smart Meter

Smart Meters are electronic devices that records information such as consumption of electric energy, woltage levels, current, and power factor. These Smart Meters communicate with both the consumer and elictricity suppliers so each get information about the consumption behaviour. Because these are recording nearly real-time both ends can determine when a customer is home (-> high electricity consumption) or not (-> low energy consumption). Smart Meters can also devices that measure natural gas, water, or district heating consumption [WSM].

Because Smart Meters are connected to home Wi-Fi it can be easily hacked and therefore the information whether a homeowner is away or at the house can be conducted by a hacker in order to be able to rob the house. Furthermore those data which are shared with the energy supplier are use for analyzing and because the energy footprints are very precise even the television channel which a homeowner is watching can be revealed as well as other sensitive data. This data can then be either sold or shared with interested third parties which can then analyze the consumers behaviour further [Vel20].

1.1.3 Inaudible Sound Beacons (Cross-Device Tracking)

While watching a commercial on a Smart TV (or also hearing an advertisement on the radio), the device broadcasts inaudible sound beacons which are then collected by the smartphone of the watcher. With this cross-device tracking a company receiving this information can conclude whether a person watching/hearing this advertisement is looking for the product at a later point of the day and in the end buys it online or at a local shop [Vel20].

Furthermore there are many other ways for cross-device tracking to be used. In the early days of this "scheme" the companies who wanted to collect those kind of information had the user to sign in to their website in order to track the user's behaviour and their interaction between the computer and smartphone based on ads and the running history to which the company has direct access while the user is logged in. Then cookies were deployed, which provide users with an unique identifier with which it was not necessary anymore to have them logged in. The problem arose that with the increasing number of devices one user has it became harder to track one user across these. Even supercookies, which are not deleted when the user deletes the cookies saved on the computer, or web beacons were introduced but these technologies still couldn't help the problem that cross-device tracking was very hard to achieve. The first try to accomplish this task was to introduce browser-fingerprinting which are browser that are customizable to the user's taste and then produce a unique signal which can then be used to single out a certain user. At the present time due to the Internet of Things introduction in which many different types of devices, like smartphone, TV, cars and even entire homes can interconnect with each other, it is much easier to track which devices belong to which user and therefore the user's online behaviour can be concluded without much effort [WCD].

Bibliography

[IMS] *IMSI Catcher - Stingray*. `https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/`. – 25.06.2015

[Vel20] VELIZ, Carissa: Privacy is Power - Why and How you should take back control of your data. (2020)

[WCD] *Wikipedia - Cross-Device Tracking*. `https://en.wikipedia.org/wiki/Cross-device_tracking`. – Accessed: 28.09.2021

[WSM] *Wikipedia - Smart Meters*. `https://en.wikipedia.org/wiki/Smart_meter`. – Accessed: 28.09.2021