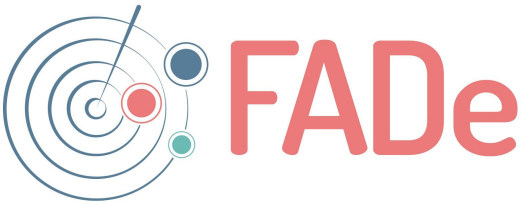

Protection of sensitive data during the execution of FADe project.

When starting FADe project, we knew that we wanted to publish as much information as possible to help other researchers to use our data, both for work development and for educational purposes, however, during the execution of the project we noticed that through various techniques, some of low sophistication and others much more complex, knowing in detail the data of the measurements made could lead to identifying those who operate these sensors. For this reason, during the execution of the FADe project, some measures were explored and established that seek to protect as much as possible that information that could put at risk the operators and / or local teams involved.

It is worth noting that as a fundamental principle of the project at a technical level, the sensors used do not interact in any way with the cellular network, behaving like cellular equipment without SIM cards that only eavesdrop to cellular towers in the same way as any device on, except by the fact that the sensor records this activity for later analysis. Due to this, in none of the jurisdictions where the monitoring was carried out (and in no other that we have investigated) the use of these sensors represents any type of illegal activity, however, given the nature and context of several countries in the region, We decided to handle the project in the safest possible way, given the possibility of criminalization of this study by security forces or other actors who may be inconvenienced by carrying out this sort of investigation.

Therefore, the following measures were taken for each stage of the project:

1. **Preparing the measurement.**

- Do not announce the intention of the project until its publication.
    - This includes cities and / or local allies prior to authorization.

    - A google account was created for each smartphone, so if a sensor is compromised, it would not filter information about the others. This account would not have any numbering or indicative of how many sensors there would be in each city or how many cities were under monitoring.
- Definition of a save communication channels.
    - Signal.
    - Email encrypted with PGP (Pretty Good Privacy).
- Protection of the database where the information would be stored.
    - Access only from preset IP addresses.
    - Access only using TLS certificates. (Transport Layer Security).

2. During measurement

- Avoid using cell phone mobile lines, or in case of using them, make sure that do not bear the names of people associated with the LCO (Local Coordinating Organization). In some cases, these telephone mobile lines were acquired on behalf of the regional coordinating team.
- Buy local smartphones. Depending on the case, smartphones were acquired in each receiving city, to minimize the suspicious entry of various cellular devices by the customs of the country involved, especially in those countries where the entry of equipment can be criminalized or susceptible to illegal seizures by security forces.
- Enter devices by parts. At the time of entering devices to each country involved, an attempt was made to distribute them in smaller amounts, preventing a single person from entering all the device at the same time, especially since these equipment can be particularly suspicious, since they are made up of old cell phones, and a specially built cable (USB serial) to handle data with these devices.
- Develop discreet sensor management strategies:
    - Inside cars, motorcycles, bicycles, etc.
    - In bags, drawers, bookcases, etc.
- To take into consideration:
    - In case of operational risks of any collaborating member of the project or other related activities, it was suggested to stop the measurement.
    - It is suggested that each of the LCO's are not aware of which other cities are monitored until after the analysis phase of the project.

3. During the analysis

- Coordinate normalization, that is:
    - Use approximate locations, set a margin of error of about 300-400 meters.

    - Hide sweep frequency data, that is, the result does not reveal the number of readings on the same geographic point.
    - Applying the above described, greater computational efficiency can be achieved, analysis is faster, and also the servers used can be less powerful.
- Avoid specifying measurement times, except in those cases in which this information does not reveal the identity of the operators (e.g., in a low traffic area at a specific time, only the sensor and the collaborative team cell phones have been reported in the area).

4. During publication

- Only publish those allies (LCO's) interested to be related to the FADe project openly.
- Avoid closely involving at events those organizations or allies that decided to remain anonymous.

South
LIGHTHOUSE

AA/mar/2020