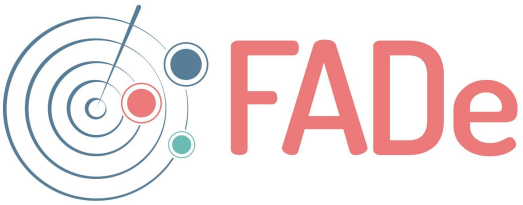

Protection of sensitive data during the execution of FADe project.

When the FADe project began, we knew that we wanted to publish as much information as possible to help other researchers use our data, both for work development and educational purposes. However, during the project's execution, we noticed that through various techniques, some of the low sophistication and others much more complicated, knowing in detail the data of the measurements made could lead to identifying those who operate these sensors. For this reason, during the FADe project's execution, 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 use of the sensors does not interact with the cellular network, behaving like cellular equipment without SIM cards that only eavesdrop on cellular towers in the same way as any turned on device, 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), these sensors' use represents any 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 criminalizing 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 safe communication channel.
    - 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 they 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 entry of various cellular devices by the customs of the country involved, especially in those countries where the entry of equipment can be susceptible to seizures by security forces.
- 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 project's analysis phase.

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 operators' identity (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 in being related to the FADe project openly.
- Avoid closely involving at events those organizations or partners that decided to remain anonymous.

AA/mar/2020