Protest Guide

por los Derechos Civiles

Asociación por los Derechos Civiles

November 2021

Written by: Alejo Kiguel
Design: Matías Chamorro
Cover design: El Maizal

Contents

Our *Protest Guide* is part of a campaign that seeks to raise awareness about the technologies that security forces could use to track and identify people at a protest.

ADC has regularly been monitoring the purchase and deployment of surveillance equipment in Argentina. In previous years, we carried out studies on the risks posed by law enforcement using drones,[1] expressed our views on cyber patrolling[2] and actively worked to stop the use of facial recognition in public spaces. Regarding the latter issue, we launched the website conmicarano.org.ar where we display a map of the provinces and towns of our country already using this type of technology. On the other hand, together with other civil society organizations in Latin America, we conducted joint research to disclose the names of the companies that develop and sell these solutions to the different governments in 2021.[3]

Although in Argentina the use of these types of surveillance in protests and demonstrations is still incipient, the growing purchase of equipment provided with them by authorities, such as security cameras, facial recognition, forensic data extraction tools and drones, together with the increase of cyber patrolling, show a clear advance in their employment, which poses a dangerous threat to human rights.

Through this guide, we intend to set forth how these technologies are being used around the world to monitor protests, how people can lessen the chance of falling victim to them and provide a series of recommendations to protect yourself should you attend a demonstration.

1. Electronic surveillance of your mobile devices

a) Images, contacts, documents, and other information on your phone

Where are my pictures, documents and contacts stored?

- **When using your phone, you generate data. For example, taking pictures or recording videos, creating, or editing notes and documents, and when adding new names or numbers to your address book.**

- **One thing you should understand is that when you create a file on your mobile, you are also producing associated information or ‘’metadata’’. For example, a picture taken creates metadata such as the time and place it was taken. This type of data can be just as important – or even more so - as the photo itself.**

- **All this information is stored in your phone’s internal memory, plus any external memory connected, such as a MicroSD card, or in the cloud, or both if you are using a cloud backup service.**

¿How can the police access the information on my phone?

- **There are a few ways in which security forces could access this data, depending on the where it is kept:**
-

- If the data is stored locally, it could be accessed by **mobile forensic data extraction tools,** which connect to your device and download the information saved in it. This method requires seizing your phone, since it cannot be done remotely.

- If your images, documents, and contacts are synchronized in a cloud service, such as iCloud, Dropbox, or Google Drive, they could be accessed by cloud data extraction tools, or a legal warrant could be issued to the cloud service provider.

Mobile forensic extraction tools

What do mobile forensic extraction tools do?

- **Mobile data extraction tools (MDET) are devices that allow you to extract information from cell phones, including:**
  - contacts;
  - call data, i.e., information on the caller or receiver, time, and duration;
  - text messages, including recipient and time;
  - stored files, such as photos, videos, audio files, documents, etc.;
  - application data, including the information stored in them;
  - location history;
  - search history in your browsers
  - connections to wi-fi networks, which may reveal the locations where you have connected, such as your workplace or a coffee shop.

.

How could cell phone extraction tools be used in a protest?

- To extract the stored data, the police need physical access to your phone.
- Within a protest or demonstration, they could stop or arrest you on signs of misconduct. In such cases, a judge must be informed immediately, and may order your detention and confiscation of your belongings, including your cell phone.
- Your phone may be taken even in certain situations when you are a witness or a victim of a crime
- In Argentina, most police forces have these mobile extraction and analysis tools. However, in order to use them, a court order should be issued to search it.

To bear in mind when going to a protest:

- As a user, you have some control over the data your phone generates and where it is kept. A good understanding of this means that you at least will know what data could be accessed should your device be seized.
- Keeping your operating system (Android or iOS) up to date is probably the best way to prevent it from being obtained through one of these tools.
- Although your phone should remain locked, some mobile extraction tools are especially designed to retrieve data

from locked phones. Nevertheless, an up-to-date operating system and a strong password should be your first step to protect it.

- Before going to a protest, you might consider backing up your data to your computer and then delete it from your device. However, some mobile data extraction tools can recover deleted information, and even access it in the cloud should you decide to store it there.

Cloud extraction tools

What are “cloud extraction tools” and how are they used?

- Cloud extraction technology allows to collect the information you store in a “cloud” through your cell phone or other devices.

- This type of extraction gets hold of your data stored online by applications such as Instagram, Telegram, Twitter, Facebook, and Uber, among others.ber.

How can cloud extraction tools be used in a protest?

- To extract your data from the cloud, law enforcement needs physical access to your mobile. Your device could be confiscated if you are detained during a protest for alleged misconduct, but also as a witness or even victim of a crime.

- **All the information obtained could be used to identify protesters and organizers and find out the meeting locations and actions.**

- **Your content in the cloud reveals not only information about you but about your friends, family, and anyone else who interacts with you online. For example, past contacts deleted from your phone may continue to be stored in the cloud.**

To bear in mind when going to a protest:

- **One possibility is to disable cloud backup on the phone apps you are using and log out of all cloud-based services. This will keep data from being put in the cloud and prevent access to it from your phone.**

- **Before attending a protest, beware that although your WhatsApp messages use end-to-end encrypted communications, the backups stored online could be accessed by the authorities using cloud extraction tools on your mobile.**

- **Some apps, such as Uber, Twitter, WhatsApp, and Facebook allow you to disable location data kept in the cloud. This can keep the police from tracking the places that you have been.**

- **As a user, you have some control over the data your phone generates in the first place, and where it is stored. A good understanding of this means that you at least will know what data could to be accessed should your device be seized.**

b) “Unique identifiers” on your phone

What are my “unique identifiers” and where are they stored?

- **Your phone and SIM card include unique identifiers, which the police can obtain to recognize you.**
- **The IMSI (International Mobile Subscriber Identity) is a unique number associated with your SIM card, whatever device you are using.**
- **In Argentina, all cell phone number owners must register in the provider company’s records. Therefore, if you have a subscription, the IMSI is probably associated with personal information, such as your name and address.**
- **The IMEI (International Mobile Equipment Identity) is a unique number that identifies your device. This means you get a new IMEI every time you change phones.**
- **The IMSI and IMEI cannot be altered any other way and can be linked to information about you (e.g., name, address) or your device (e.g., make, model).**
- **Other identifiers: certain components in your phone have unique identifiers as well, such as the MAC address of your wi-fi antenna, the BD_ADDR of your Bluetooth module or the advertising identifier.**

How can the police access my unique identifiers?

- **Apps and websites can obtain the advertising identifier on your phone. Although it is not linked to personal information, such as your name and address, it may be associated with other data like your location. Data brokers[4] can get hold of massive amounts of information from cell phones and sell them to law enforcement agencies, including advertising identifiers.**

- **Other unique identifiers, such as your MAC address, may be collected when you sign in to a wi-fi network, although they are not so easily linked to personal information that could lead to identify youe.**

- **In addition, the police could also learn the identifiers related to you through queries made to service providers.**

- **LThere could also be an attempt to seize your IMSI and IMEI with an IMSI Catcher, a device deployed to track all phones connected to a network in its proximity. Once the identifier is intercepted, it could be employed to seek for other personal information.**

What is an IMSI Catcher?

- **IMSI catchers, also known as Stingrays, are devices that locate and tracks all phones connected to a telephone network nearby, by "capturing" the unique IMSI numbers.**

- **IMSI is the subscriber's service key and consists of a unique number to your SIM card.**

- **This is done by acting like a false cell phone tower, tricking the phones within the area into connecting to it, thus intercepting their data without their users' knowledge.**

- **The most accessible information that can be obtained about you in this circumstance is your location. Cell phone towers inevitably do this through triangulation, which is how they provide their service in the first place. By placing itself between your mobile device and the cell tower, an IMSI receiver can determine your rough location.**

- **Although it is unlikely, more sophisticated attacks could occur, depending on the capabilities of the IMSI receiver and the network to which you are connecting. Some Stingray devices rely on known weaknesses in communication protocols and can force your phone to downgrade the ones it is using, lowering its level of security of and making it more easily accessible (e.g., by downgrading communications from 3G to 2G, since, as far as we know, content interception and real-time decryption can only be performed when the target is connected via 2G networks).**

- **IMSI receivers cannot read the content of encoded messages you exchange through platforms using end-to-end encryption, such as WhatsApp or Signal.**

How could IMSI receivers track my phone in a protest?

- **Police could use IMSI receivers to identify someone at a demonstration by catching the IMSI numbers of all phones**

nearby, which is an obvious infringement of the rights to freedom of expression, assembly and association, and privacy.

- **Some types of IMSI receivers can even block your calls and messages.**

To bear in mind when going to a protest:

- **Putting your phone in airplane mode or turning it off completely will stop an IMSI receiver from tracking you and your communications.**

- **If you want to prevent the content of your text messages from being intercepted by an IMSI catcher, you can stick to messaging services using end-to-end encryption, such as Signal and WhatsApp. A Stingray will know you are signing into these apps, but not be able to pick up the content.**

- **Using an ad blocker is another effective way to prevent companies from tracking you online and collecting personal information.**

c) Location through your cell phone

Where is my phone's location history stored?

Your phone can be located in two main ways: using GPS or mobile network location:

1. GPS

- **GPS (Global Positioning System) uses satellite navigation to locate your phone with relative accuracy, i.e., within range of a few meters, and relies on a GPS chip inside your phone.**

- **Depending on your device, GPS location history may be stored locally and/or in a cloud service such as Google Cloud or iCloud. It could also be collected by any app being used that has access to your GPS location.**

2. Mobile network location

- **Mobile network location (or Global System for Mobile Communications [GSM] location) depends on your cellphone service provider and can be determined only when you are logged in, i.e., when your phone is on and not in airplane mode but is much less accurate than GPS. Your rough location can be determined within a range of a few tens of meters in a city, or hundreds of meters in rural areas.**

- **This location data is stored by your cell phone provider.**

Other methods could also be used to determine your whereabouts indirectly, such as open wi-fi hotspots or Bluetooth beacons that ping your phone and collect location metadata embedded in your photos.

How can the police access my location history?

There are a number of ways that law enforcement agencies could access your phone's location:

1. GPS

- **Accessing GPS location history depends on where it is stored. It can be done via mobile extraction tools, which connect to your phone and download all the information stored on it, including details of the places visited. This method requires physical possession of your phone.**

- **Access to your GPS data may also be achieved through hacking your device, a sophisticated technique that could be done remotely.**

- **If your GPS location history is also collected in an online account, such as iCloud or Google Maps, it can be seized through cloud extraction technologies or a legal warrant to the service providers that keep such information.**

2. Mobile network location

- **Police can access your approximate location through your service provider. In Argentina, a court order is required to solicit this information.**

- **This implies that access to your phone is not necessary to determine your position in the proximity of a protest.**

- **Another way to get hold of such information is through an IMSI receiver (or Stingray), a device deployed to intercept and track all cell phones turned on and connected to a mobile network in a specific area. Placing itself as a fake cell tower, it allows to collect information from people at protests, meetings, or public events. información acerca de las personas que asisten.**

How to better control your location data

1. GPS

- **The best way to prevent authorities from knowing your location is to limit the generation of this type of data in the first place.**

- **In order to do this, you could deactivate your phone's GPS, often referred to as "location services". However, even turned off, your past location history may still be accessible.**

- **If you still need to use GPS, revise your app permissions to access your location.**

- **Removing these permissions for all apps can prevent the data from being uploaded to an online account.**

- **If one application does require access to your GPS data in order to function, inspect its settings so as to understand whether your location is stored online or just locally in the app. For example, when using Google Maps while logged into a Google account, you may choose to disable the location history from the settings so that it is not saved in the account.**

- **If you take photos with your location services enabled, the place where they are taken may be included in the metadata, known as EXIF data. You may want to turn off location services while taking photos, or else, clear this EXIF data afterwards through software or an app. Signal messenger application, for example, clears EXIF data when sending images.**

- **Similarly, switching off wi-fi or Bluetooth can prevent your phone from connecting to unwanted hotspots and providing indirect location data.**

2. Mobile network

- **When it comes to mobile network location, the only way to avoid being tracked is to disconnect from the network altogether.**

- **Having your phone switched off, in airplane mode or in a Faraday cage[5] will prevent connection to the mobile network and thus make GSM geolocation impossible. Using a Faraday cage or switching off the phone will prevent any communication through a telephone network, whereas airplane mode does allow certain types of connection, such as Bluetooth or GPS).**

d) Social media monitoring

What is social media monitoring?

- **The monitoring of social networks, or cyber patrolling, refers to the tracking, collection and analysis of information shared on social media platforms, such as Facebook, Twitter, Instagram.**

- **It can include scanning content posted on public or private groups or pages, or scraping, i.e., obtaining all the data from a social media platform, including the content you post and details of your behavior styles, such as things you like and share.(como lo que te gusta y compartís).**

- **Cyber patrolling allows the authorities to gather and examine a large amount of data, thus, create profiles and make predictions about users' behavior.**

- **In Argentina, legislation on social network monitoring is obscure. Although there have been attempts to regulate these practices through ministerial resolutions and protocols, ADC believes that as long as there is no legal support from the legislative branch, they cannot be considered constitutionals.**[6]

How could social media monitoring be used in protests?

- **Protesters often resort to social media to promote their action, communicate with one another and upload photos and videos of the meeting.**

- **This means that police could collect information from social media pages and groups to learn the identities and affiliations of its organizers, the location and timing of the planned action, and other particulars related.**

- **They could track social media posts related to past or future protests in order to identify protesters.**

- **In addition, they could use facial recognition software to screen images and videos uploaded to social media, thus detecting demonstrators' identities**

To bear in mind when going to a protest

- **If you upload your images of a protest to your social networks, they could be used to identify and locate people at the site.**

- **If location settings are enabled on your platforms or in your camera and photo apps while posting, the police could have access to such location data.**

- **SIf you want to post on social media during a protest, you should consider disabling location settings in the apps you use. If you share images, do not tag people participating without their consent, as this could create a trail which police could exploit to trace people at the event.**

- **If you upload photos of the meeting, consider removing EXIF data beforehand. EXIF is metadata linked to your images that can reveal information such as location, time and date, and the device employed.**

- **Beware that the place of an image can still be detected by observing reference points, such as a monument or a landmark. Consider this when you film your surroundings and try to avoid identifiable backgrounds.**

2. A guide to face and body surveillance

a) Face recognition

What is facial recognition technology?

- **Facial recognition technology (FRT) is a biometric system that makes it possible to pinpoint and identify people by their facial features.**

How does it work?

- Facial recognition works through software powered by an algorithm (i.e., a formula) that allows to track faces and map their features.

- Once facial contours are read, the application creates a template, or faceprint, with the geometrical representation of that individual face. The faceprint is the biometric data with which face recognition tech works.

- The faceprint can then be digitally analyzed and compared, in real time, to a large number of faces stored previously in a database, to find a match, thus identifying the person.

- Biometrics is a probability process, so once the software finds a potential match, it outputs a percentage that defines how likely it is to correspond to the same person.

- In Argentina, more and more places are implementing these systems without having conducted human rights impact assessments. In the microsite conmicarano.adc.org.ar we compiled the different face recognition initiatives currently deployed in Argentina.[7]

How could face recognition be used in a protest?

- Facial recognition could be applied to monitor, track and identify people's features in public spaces, including protests. This can be done overtly or secretly, without people's knowledge or consent

- Cameras with FRT can take photos or shoot videos and identify people in real or at a later time. It can also capture and analyze existing images, for example, photos and video footage uploaded to social media.

- As biometric data is gathered from protesters, it can be added to one or more databases stored previously, where it is compared with profiles collected from other sources to find a match.

- The data could also be stored to create a new database of people attending protest marches for future comparison and identification purposes.

To bear in mind when going to a protest:

- FRT works by capturing the image of a person's facial features, so if you intend to maintain anonymity, you might consider covering your face, for example, with a scarf.

- Other options include wearing makeup and clothing with designs intended to disrupt accurate facial recognition. However, this technology is constantly adjusting and gaining accuracy, so cosmetics and clothes design may become less effective in the future.

- **Face recognition can also be used in social media. Remember this before posting any images of a protest in which the faces of other participants appears.**

- **Another option is to apply face blurring software before putting up photos or videos online.**

b) How body cameras can be used in a protest

What do body-worn video cameras do?

- **Body cameras are video cams that attach to an agent's clothing - often at chest, shoulder, or head level - and can record events, including sound, from the wearer's perspective.**

- **Body cameras can normally have seen them on the police officer's chest, and while they are recording, an intermittent flashing light should appear on the device.**

- **In Argentina, they are used by most security forces.**[8]

How could body-worn video cameras be used at a protest?

- **Body-worn cameras can be used to monitor the deeds and possible misbehavior of protesters.**

- **Outside demonstrations, body cameras normally switch on only at detecting an incident. But during a protest meeting, they may run all through.**

- **Most cameras require footage to be manually uploaded to a server, but some of the latest video surveillance technology allows live streaming directly to police headquarters.**

- **Although there is no information about such usage in Argentina, the footage could be further processed by facial recognition software, among other media**

To bear in mind when going to a protest:

- **Despite the fact law enforcement agencies claim body cameras function as "independent witnesses" and could even deter police abuse, the truth is that they can be switched on and off at any time, or they can decide where to direct them, for which police are always in control of what situations are recorded or not**

- **See our separate guide on facial recognition technology, regarding the processing of body camera recordings by facial recognition software.**

c) How police drones can be used at a protest

What are police drones?

- **Drones are remotely controlled unmanned aerial vehicles (UAVs) of many sizes.**

- **They are usually equipped with cameras, and eventually with other more sophisticated tools, such as facial recognition technology, license plate readers, or GPS geo-location finders, among others.**[9]

- **Drones may also be provided with loudspeakers, surveillance equipment, radar, and communications interception tools, such as IMSI receivers.**

How could drones be used during protests?

- **Camera drones can be used to remotely trace people's movements in public spaces, including during protests, without their consent or knowledge.**

- **Similarly, when furnished with communications interception software, drones can also be used to catch and monitor protesters' calls and messages within the area of the protest or its surroundings.**

To bear in mind when going to a protest:

- **The use of drones and the impact on your anonymity depends on the technologies they are equipped Consult our guides on facial recognition technology and IMSI receivers, as these are tools that a drone could use to spy on protesters' actions.**

* * *

3. Notas

1 https://adc.org.ar/wp-content/uploads/2019/06/033-alto-en-el-cielo-12-2017.pdf

2 https://adc.org.ar/2020/04/22/sobre-la-necesidad-de-una-ley-para-regular-lainvestigacion-en-fuentes-abiertas-y-redes-sociales/

3 The full report is available at https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/

4 Data brokers are companies that buy and sell the information you create while using the internet. More information at https://www.amnesty.org/es/latest/research/2017/02/muslim-registries-big-data-and-human-rights/

5 A Faraday cage or bag is a socket used to block electromagnetic waves and block all communications from your phone or computer equipment. A homemade way to create a Faraday shield is to wrap up your device with large amounts of aluminum foil, which will keep it off the grid.

6 To learn more about cyber patrolling in Argentina, please visit our web site
https://adc.org.ar/2020/04/22/sobre-la-necesidad-de-una-ley-para-regular-la-investigacionen-fuentes-abiertas-y-redes-sociales/

7 Con Mi Cara No, https://conmicarano.adc.org.ar/, a microsite launched by ADC especially dedicated to inform on facial recognition and alert the population about its dangers.

8 https://www.argentina.gob.ar/noticias/frederic-entrego-400-camaras-de-video-demontaje-corporal-para-las-fuerzas-federales

9 More information on the use of drones in Argentina available at https://adc.org.ar/wp-content/uploads/2019/06/033-alto-en-el-cielo-12-2017.pdf


APC
por los Derechos Civiles