SURVEILLANCE SELF-DEFENSE

The Problem with Mobile Phones

Mobile phones have become ubiquitous and basic communications tools—now used not only for phone calls, but also for accessing the Internet, sending text messages, and documenting the world.

Unfortunately, mobile phones were not designed for privacy and security. Not only do they do a poor job of protecting your communications, they also expose you to new kinds of surveillance risks—especially location tracking. Most mobile phones give the user much less control than a personal desktop or laptop computer would; it's harder to replace the operating system (https://ssd.eff.org/en/glossary/operating-system), harder to investigate malware (https://ssd.eff.org/en/glossary/malware) attacks, harder to remove or replace undesirable bundled software, and harder to prevent parties like the mobile operator from monitoring how you use the device. What's more, the device maker may declare your device obsolete and stop providing you with software updates, including security fixes; if this happens, you may not have anywhere else to turn for these fixes.

Some of these problems can be addressed by using third-party privacy software—but some of them can't. Here, we'll describe some of the ways that phones can aid surveillance and undermine their users' privacy.

Location Tracking

The deepest privacy threat (https://ssd.eff.org/en/glossary/threat) from mobile phones—yet one that is often completely invisible—is the way that they announce your whereabouts all day (and all night) long through the signals they broadcast. There are at least four ways that an individual phone's location can be tracked by others.

1. Mobile Signal Tracking — Towers

In all modern mobile networks, the operator can calculate where a particular subscriber's phone is located whenever the phone is powered on and registered with the network. The ability to do this results from the way the mobile network is built, and is commonly called triangulation.

One way the operator can do this is to observe the signal strength that different towers observe from a particular subscriber's mobile phone, and then calculate where that phone must be located in order to account for these observations. The accuracy with which the operator can figure out a subscriber's location varies depending on many factors, including the technology the operator uses and how many cell towers they have in an area. Very often, it is accurate to about the level of a city block, but in some systems it can be more accurate.

There is no way to hide from this kind of tracking as long as your mobile phone is powered on and transmitting signals to an operator's network. Although normally only the mobile operator itself can perform this kind of tracking, a government could force the operator to turn over location data about a user (in real time or as a matter of historical record). In 2010, a German privacy advocate named Malte Spitz used privacy laws to get his mobile operator to turn over the records that it had about his records; he chose to publish them as an educational resource so that other people could understand how mobile operators can monitor users this way. (You can visit here (http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz) to see what the operator knew about him.) The possibility of government access to this sort of data is not theoretical: it is already being widely used by law enforcement agencies in countries like the United States.

Another related kind of government request is called a tower dump; in this case, a government asks a mobile operator for a list of *all of the mobile devices* that were present in a certain area at a certain time. This could be used to investigate a crime, or to find out who was present at a particular protest. (Reportedly, the Ukrainian government used a tower dump for this purpose in 2014, to make a list of all of the people whose mobile phones were present at an anti-government protest.)

Carriers also exchange data with one another about the location from which a device is currently connecting. This data is frequently somewhat less precise than tracking data that aggregates multiple towers' observations, but it can still be used as the basis for services that track an individual device—including commercial services that query these records to find where an individual phone is currently connecting to the mobile network, and make the results available to governmental or private customers. (The *Washington Post* reported (http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html) on how readily available this tracking information has become.) Unlike the previous tracking methods, this tracking does not involve forcing carriers to turn over user data; instead, this technique uses location data that has been made available on a commercial basis.

2. Mobile Signal Tracking — IMSI Catcher

A government or another technically sophisticated organization can also collect location data directly, such as with an IMSI catcher (a portable fake cell phone tower that pretends to be a real one, in order to “catch” particular users' mobile phones and detect their physical presence and/or spy on their communications). IMSI refers to the International Mobile Subscriber Identity number that identifies a particular subscriber's SIM card (https://ssd.eff.org/en/glossary/sim-card), though an IMSI catcher may target a device using other properties of the device as well.

The IMSI catcher needs to be taken to a particular location in order to find or monitor devices at that location. Currently there is no reliable defense against all IMSI catchers. (Some apps claim to detect their presence, but this detection is imperfect.) On devices that permit it, it could be helpful to disable 2G support (so that the device can connect only to 3G and 4G networks) and to disable roaming if you don't expect to be traveling outside of your home carrier's service area. These measures can protect against certain kinds of IMSI catchers.

3. Wi-Fi and Bluetooth Tracking

Modern smartphones have other radio transmitters in addition to the mobile network interface. They usually also have Wi-Fi and Bluetooth support. These signals are transmitted with less power than a mobile signal and can normally be received only within a short range (such as within the same room or the same building), although sometimes using a sophisticated antenna allows these signals to be detected from unexpectedly long distances; in a 2007 demonstration, an expert in Venezuela received a Wi-Fi signal at a distance of 382 km or 237 mi, under rural conditions with little radio interference. Both of these kinds of wireless signals include a unique serial number for the device, called a MAC address, which can be seen by anybody who can receive the signal. The device manufacturer chooses this address at the time the device is created and it cannot be changed using the software that comes with current smartphones.

Unfortunately, the MAC address can be observed in wireless signals even if a device is not actively connected to a particular wireless network, or even if it is not actively transmitting data. Whenever Wi-Fi is turned on on a typical smartphone, the smartphone will transmit occasional signals that include the MAC address and thus let others nearby recognize that that particular device is present. This has been used for commercial tracking applications, for example to let shopkeepers determine statistics about how often particular customers visit and how long they spend in the shop. As of 2014, smartphone manufacturers have started to recognize that this kind of tracking is problematic, but it may not be fixed in every device for years—if ever.

In comparison to GSM monitoring, these forms of tracking are not necessarily as useful for government surveillance. This is because they work best at short distances and require prior knowledge or observation to determine what MAC address is built into a particular person's device. However, these forms of tracking can be a highly accurate way to tell when a person enters and leaves a building. Turning off Wi-Fi and Bluetooth on a smartphone can prevent this type of tracking, although this can be inconvenient for users who want to use these technologies frequently.

Wi-Fi network operators can also see the MAC address of every device that joins their network, which means that they can recognize particular devices over time, and tell whether you are the same person who joined the network in the past (even if you don't type your name or e-mail address anywhere or sign in to any services).

On a few devices, it is physically possible to change the MAC address so that other people can't recognize your Wi-Fi device as easily over time; on these devices, with the right software and configuration, it would be possible to choose a new and different MAC address every day, for example. On smartphones, this commonly requires special software such as a MAC address-changing app. Currently, this option is not available for the majority of smartphone models.

4. Location Information Leaks From Apps and Web Browsing

Modern smartphones provide ways for the phone to determine its own location, often using GPS and sometimes using other services provided by location companies (which usually ask the company to guess the phone's location based on a list of cell phone towers and/or Wi-Fi networks that the phone can see from where it is). Apps can ask the phone for this location information and use it to provide services that are based on location, such as maps that show you your position on the map.

Some of these apps will then transmit your location over the network to a service provider, which, in turn, provides a way for other people to track you. (The app developers might not have been motivated by the desire to track users, but they might still end up with the ability to do that, and they might end up revealing location information about their users to governments or hackers.) Some smartphones will give you some kind of control over whether apps can find out your physical location; a good privacy practice is to try to restrict which apps can see this information, and at a minimum to make sure that your location is only shared with apps that you trust and that have a good reason to know where you are.

In each case, location tracking is not only about finding where someone is right now, like in an exciting movie chase scene where agents are pursuing someone through the streets. It can also be about answering questions about people's historical activities and also about their beliefs, participation in events, and personal relationships. For example, location tracking could be used to try to find out whether certain people are in a romantic relationship, to find out who attended a particular meeting or who was at a particular protest, or to try and identify a journalist's confidential source.

The *Washington Post* reported in December 2013 on NSA location-tracking tools that collect massive amounts of information “on the whereabouts of cellphones around the world,” mainly by tapping phone companies' infrastructure to observe which towers particular phones connect to when. A tool called CO-TRAVELER uses this data to find relationships between different people's movements (to figure out which people's devices seem to be traveling together, as well as whether one person appears to be following another).

Turning Phones off

There's a widespread concern that phones can be used to monitor people even when not actively being used to make a call. As a result, people having a sensitive conversation are sometimes told to turn their phones off entirely, or even to remove the batteries from their phones.

The recommendation to remove the battery seems to be focused mainly on the existence of malware (https://ssd.eff.org/en/glossary/malware) that makes the phone appear to turn off upon request (finally showing only a blank screen), while really remaining powered on and able to monitor conversations or invisibly place or receive a call. Thus, users could be tricked into thinking they had successfully turned off their phones when they actually hadn't. Such malware does exist, at least for some devices, though we have little information about how well it works or how widely it has been used.

Turning phones off has its own potential disadvantage: if many people at one location all do it at the same time, it's a sign to the mobile carriers that they all thought something merited turning their phones off. (That "something" might be the start of a film in a movie theater, or the departure of a plane at an airport, but it might also be a sensitive meeting or conversation.) An alternative that might give less information away is to leave everybody's phone in another room where the phones' microphones wouldn't be able to overhear the conversations.

Burner Phones

Phones that are used temporarily and then discarded are often referred to as burner phones or burners. People who are trying to avoid government surveillance sometimes try to change phones (and phone numbers) frequently to make it more difficult to recognize their communications. They will need to use prepaid phones (not associated with a personal credit card or bank account) and ensure that the phones and SIM cards were not registered with their identity; in some countries these steps are straightforward, while in others there may be legal or practical obstacles to obtaining anonymous mobile phone service.

There are a number of limitations to this technique.

> First, merely swapping SIM cards or moving a SIM card (https://ssd.eff.org/en/glossary/sim-card) from one device to another offers minimal protection, because the mobile network observes both the SIM card and device together. In other words, the network operator knows the history of which SIM cards have been used in which devices, and can track either individually or both together. Second, governments have been developing mobile location analysis techniques where location tracking can be used to generate leads or hypotheses about whether multiple devices actually belong to the same person.

There are many ways this can be done. For example, an analyst could check whether two devices tended to move together, or whether, even if they were in use at different times, they tended to be carried in the same physical locations.

A further problem for the successful anonymous use of telephone services is that people's calling patterns tend to be extremely distinctive. For example, you might habitually call your family members and your work colleagues. Even though each of these people receive calls from a wide range of people, you're likely the only person in the world who commonly calls both of them from the same number. So even if you suddenly changed your number, if you then resumed the same patterns in the calls you made or received, it would be straightforward to determine which new number was yours. Remember that this inference isn't made based only on the fact that you called one particular number, but rather on the uniqueness of the combination of all the numbers that you called. (Indeed, *The Intercept* reported (https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/) that a secret U.S. government system called PROTON does exactly this, using phone records to recognize people who placed phone calls in a “similar manner to a specific target” from new phone numbers.) An additional example can be found in the Hemisphere FOIA document (https://muckrock.s3.amazonaws.com/foia_files/7-3-14_MR6608_RES.pdf). The document describes the Hemisphere database (a massive database of historical call records) and how the people who run it have a feature that can link burner phones by following the similarity of their call patterns. The document refers to burner phones as "dropped phones" because their user will "drop" one and start using another one—but the database analytics algorithms can draw the connection between one phone and another when this happens, so long as both were used to make or receive calls to similar sets of phone numbers.

Together, these facts mean that effective use of burner phones to hide from government surveillance requires, at a minimum: not reusing either SIM cards or devices; not carrying different devices together; not creating a physical association between the places where different devices are used; and not calling or being called by the same people when using different devices. (This isn't necessarily a complete list; for example, we haven't considered the risk (https://ssd.eff.org/en/glossary/risk-analysis) of physical surveillance of the place where the phone was sold, or the places where it's used, or the possibility of software to recognize a particular person's voice as an automated method for determining who is speaking through a particular phone.)

A Note About GPS

The Global Positioning System (GPS) lets devices anywhere in the world figure out their own locations quickly and accurately. GPS works based on analyzing signals from satellites that are operated by the U.S. government as a public service for everyone. It's a common misconception that these satellites somehow watch GPS users or know where the GPS users are. In fact, the GPS satellites only transmit signals; the satellites don't receive or observe anything from your phone, and the satellites and GPS system operators do not know where any particular user or device is located, or even how many people are using the system.

This is possible because the individual GPS receivers (like those inside smartphones) calculate *their own positions* by determining how long it took the radio signals from different satellites to arrive.

So, why do we speak of “GPS tracking”? Usually, this tracking is done by apps running on a smartphone. They ask the phone's operating system (https://ssd.eff.org/en/glossary/operating-system) for its location (determined via GPS). Then the apps are able to transmit this information to someone else over the Internet. There are also tiny GPS-receiving devices that can be surreptitiously hidden in someone's possessions or attached to a vehicle; those receivers determine their own location and then actively retransmit it over a network, usually the mobile phone network.

Spying on Mobile Communications

Mobile phone networks were not originally designed to use technical means to protect subscribers' calls against eavesdropping. That meant that anybody with the right kind of radio receiver could listen in on the calls.

The situation is somewhat better today, but sometimes only slightly. Encryption (https://ssd.eff.org/en/glossary/encryption) technologies have been added to mobile communications standards to try to prevent eavesdropping. But many of these technologies have been poorly designed (https://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html) (sometimes deliberately, due to government pressure not to use strong encryption!). They have been unevenly deployed, so they might be available on one carrier but not another, or in one country but not another, and have sometimes been implemented incorrectly. For example, in some countries carriers do not enable encryption at all, or they use obsolete technical standards. This means it is often still possible for someone with the right kind of radio receiver to intercept calls and text messages as they're transmitted over the air.

Even when the best industry standards are being used—as they are in some countries and on some mobile carriers—there are still people who can listen in. At a minimum, the mobile operators themselves have the ability to intercept and record all of the data about who called or texted whom, when, and what they said. This information might be available to local or foreign governments through official or informal arrangements. In some cases, foreign governments have also hacked mobile operators' systems in order to get secret access to users' data. Also, IMSI catchers (described above) can be used by someone physically nearby you. These can trick your phone into using their fake “tower” instead of your mobile operator's legitimate infrastructure, in which case the person operating the IMSI catcher may be able to intercept your communications.

The safest practice is to assume that traditional calls and SMS text messages have not been secured against eavesdropping or recording. Even though the technical details vary significantly from place to place and system to system, the technical protections are often weak and can be bypassed in many situations. *See Communicating with Others (https://ssd.eff.org/en/module/communicating-others#overlay=en/node/43/) to learn how to text and talk more securely.*

The situation can be different when you are using secure communications apps to communicate (whether by voice or text), because these apps can apply encryption to protect your communications. This encryption can be stronger and can provide more meaningful protections. The level of protection that you get from using secure communications apps to communicate depends significantly on which apps you use and how they work. One important question is whether a communications app uses end-to-end encryption (https://ssd.eff.org/en/glossary/end-end-encryption) to protect your communications and whether there's any way for the app developer to undo or bypass the encryption.

Infecting Phones with Malware (https://ssd.eff.org/en/glossary/malware)

Phones can get viruses and other kinds of malware (malicious software (https://ssd.eff.org/en/glossary/malware)), either because the user was tricked into installing malicious software, or because someone was able to hack into the device using a security flaw in the existing device software. As with other kinds of computing device, the malicious software can then spy on the device's user.

For example, malicious software on a mobile phone could read private data on the device (like stored text messages or photos). It could also activate the device's sensors (such as microphone, camera, GPS) to find where the phone is or to monitor the environment, even turning the phone into a bug.

This technique has been used by some governments to spy on people through their own phones, and has created anxiety about having sensitive conversations when mobile phones are present in the room. Some people respond to this possibility by moving mobile phones into another room when having a sensitive conversation, or by powering them off. (Governments themselves often forbid people, even government employees, from bringing personal cell phones into certain sensitive facilities—mainly based on the concern that the phones could be infected with software to make them record conversations.)

A further concern is that malicious software could theoretically make a phone pretend to power off, while secretly remaining turned on (and showing a black screen, so that the user wrongly believes that the phone is turned off). This concern has led to some people physically removing the batteries from their devices when having very sensitive conversations.

As we discussed above, precautions based on powering off phones could be noticed by a mobile operator; for example, if ten people all travel to the same building and then all switch off their phones at the same time, the mobile operator, or somebody examining its records, might conclude that those people were all at the same meeting and that the participants regarded it as sensitive. This would be harder to detect if the participants had instead left their phones at home or at the office.

Forensic Analysis of Seized Phones

There is a well-developed specialty of forensic analysis of mobile devices. An expert analyst will connect a seized device to a special machine, which reads out data stored inside the device, including records of previous activity, phone calls, and text messages. The forensic analysis may be able to recover records that the user couldn't normally see or access, such as deleted text messages, which can be undeleted. Usually forensic analysis can bypass simple forms of screen locking.

There are many smartphone apps and software features that try to inhibit or prevent forensic analysis of certain data and records, or to encrypt data to make it unreadable to an analyst. In addition, there is remote wipe software, which allows the phone owner or someone designated by the owner to tell the phone to erase certain data on request.

This software can be useful to protect against data being obtained if your phone is taken by criminals. However, please note that intentional destruction of evidence or obstruction of an investigation can be charged as a separate crime, often with very serious consequences. In some cases, this can be easier for the government to prove and allow for more substantial punishments that the alleged crime originally being investigated.

Computer Analysis of Patterns of Phone use

Governments have also become interested in analyzing data about many users' phones by computer in order to find certain patterns automatically. These patterns could allow a government analyst to find cases in which people used their phones in an unusual way, such as taking particular privacy precautions.

A few examples of things that a government might try to figure out from data analysis: automatically figuring out whether people know each other; detecting when one person uses multiple phones, or switches phones; detecting when groups of people are traveling together or regularly meeting one another; detecting when groups of people use their phones in unusual or suspicious ways; identifying the confidential sources of a journalist.

Last updated: 2015-02-10