We took the utmost care to make sure that this document accurately reflects the most up-to-date knowledge about technology and threat models. Still, in our field, technologies and security models continue to change rapidly. If you feel that something in this piece is out of date or have any further suggestions on how we could improve it, please drop us a line at gtp-jsf@internews.org

This document was last reviewed on 2022-05-24

Device location security

What we do and do not cover in this guide

This guide looks at how our mobile devices could leak data about our locations and what we could do to protect ourselves against it. It's designed for most Central European journalists' threat models and only looks at how our mobile devices could give up precise location data on us. It doesn't look at some of the other ways your location can be tracked, such as through payments, CCTV cameras, or images you post online, and doesn't cover coarse location data (for example, how your IP address might reveal which country or city you're in). If you have any questions about those, let us know and we're happy to direct you to the right resources!

Location, time, and threat models

Whenever we think about location data and how it affects our threat models, it's worth keeping three questions in mind:

- How precise is the location data that someone has on us?
- At what points in time does an adversary know about our location?
- How sensitive is your location data? Is it a problem if others know where your office or favorite coffee shop is located?

Location data could be pretty coarse, for example showing which city we are based in. It could also be quite precise, pointing towards our specific address.

Most journalists will spend a considerable amount of time in the city where their newsroom is located and will often hang out in the vicinity of their offices. This information is often public and not much of a

threat to them. Journalists might, however, also go on confidential business trips, meet sensitive sources, or do interviews in hostile environments. Some location data is more sensitive than others.

We might be at risk not just if our present location is leaked, but also if an adversary could get their hands on past locations. If you are currently at your office, but a transport app contains data about last night's trip from a restaurant to a courtyard where you met a source, this could potentially be considered sensitive data.

Finally, it's worth thinking about *who* specifically might have access to your location data, and whether you consider them to be part of your threat model. Your local coffee shop might quickly notice when you are and are not in the neighborhood by checking when you use your discount card but is not likely to use this information to harm you. Someone who has broken into your Uber account, on the other hand, might be a big threat, as they could figure out where exactly you live.

In the paragraphs below, we will summarize some ways in which our phones, apps, and telecoms obtain our location data, what risk this could potentially pose to journalists, and what we can do about it.

Individual apps and location data

The apps we use can collect a lot of location data about us. Some apps, for example taxi apps or turn-by-turn navigation apps, might require location access to function. Fitness apps, which track how far and fast you run, swim, or cycle can also collect very granular data on where your workouts take place. There are also many other apps for which location access can be useful but is not necessary for the app to function. WhatsApp, for example, only requires location access if you want to share your current location with other users. You can still message and call others without granting the app location access.

When thinking about apps accessing your location, it's worth keeping the following risks in mind:

1. **The app provider knows your present and past locations.** If you use an app like Uber, Glovo, or Google Maps, then its publisher will know about your present location, your searches, and possibly your past locations. They could potentially share such data with others, for example a government that has filled out a court order or police request.
2. **The app provider can sell your location data to others.** Some apps, especially those produced by smaller companies, could sell location data to other companies. This data is often used for things like advertising. Such data is almost always anonymized in such a way that it will be difficult to track you as an individual. In some past cases, location data has even been purchased by governments or security services, but even then, it was used to analyze the movements of groups, rather than individuals.
3. **Someone who accesses the app can see your past locations.** Apps such as taxi or map services often contain a search history. If, for example, your phone is searched by security services or border guards, then they could also see what places you searched or traveled to. Similarly, if your taxi app is linked an employer's or client's account or card, they might be able to access your trip data or–based on information about travel times and charges–infer quite a bit about your trips.

We can't fully stop the above from happening if we use location services on our phones, but there are a few steps we could take to mitigate those risks.

1. **Audit which apps access your location.** You can check in your phone settings to see what apps have been accessing your location (see here how to do so in iOS and here how to do it in Android). If you do not trust an app with your location, you can always prevent iOS or Android from giving it such data.[1]
2. **Consider changing your behaviors a little bit.** If you do not want your taxi app to have details on your home address, you can, if practicable, ask the app to drop you off on an alternative street a few blocks away and walk for the rest. If you have a trip or meeting and do not want it recorded in an app, it might be better to take a traditional taxi or public transport for that journey.
3. **Clear your location history.** Many apps, like Google Maps or Uber, will save some of your location, trip, or search history. In some cases, like Google Maps, you can clear such history in-app. Once you've cleared it, anyone who looks through your such apps will not be easily able to find your location or travel history. Not all apps allow you to selectively or fully clear your history, though. Bolt, in fact, recommends deleting your account and creating a new one on the same username in order to delete your history. Uber does not seem to have an easy way of erasing the history of individual trips, either. Alternatively, you can always delete the app from your device if you are in a place (such as a border crossing) when you are not using the service and fear your device might be searched. Don't forget that your email inbox might also contain records of your trips or deliveries. You might need to take a moment to delete email receipts of confidential or sensitive ones.
4. **Have a strong password and two-factor authentication for any services that need to remember your location.** If an adversary could log in to your fitness service, taxi service, or maps service, they could also gain access to some of your location and ride history. Make sure that you use long, unique passwords and–where possible–two factor authentication for such services.
5. **Look at the social sharing settings in your apps.** A fitness app called Strava would automatically suggest new exercise routes to its users. There was only one problem: those routes were based on existing users' exercise patterns, and therefore revealed sensitive locations such as military bases or individual homes. If you are using any location app with social settings, such as a fitness app, dig into its settings to figure out whom you are sharing data with. Remember that even something simple, like a summary of a morning run posted on Facebook, could let someone figure out your location.

---

[1] In modern smartphone operating systems, there's also the option of always giving the app permission to access your location (also known as background), or to only give it such permission when the app is in use (also known as foreground). If you give the app permission to always use your location, it will also capture your location even when it's in the background (so not on the main screen). This could be useful if you are for example reading an article on your phone and waiting for a notification on when to get off your train. If your app only captures the location when it's open, then it will only be able to read location data when it's displayed on the main screen.

Your mobile operating system

In addition to apps, mobile phone operating systems also collect quite a bit of location data. iOS, for example, will try to remember your home and work addresses and make navigation suggestions. Such data is usually stored pretty securely and anonymized – as a journalist, there's usually no need to worry about it unless your threat model specifically involves Apple or Google or an adversary who could compel them to share data they have on you (in which case, you will require very tailored security advice that might be different from the advice given to most other journalists).

Still, if you want to further reduce the data mobile operating systems collect on you, just follow those guides:

- iOS (look specifically at the data collected by system services)
- Android

Your telecom or mobile phone provider

As we wrote about above, in the past, whenever your mobile phone is switched on and connected to a network, your telecom will know where it is located. This is an unavoidable consequence of the way mobile phone networks have been designed – the telecom needs to know where the phone is in order to send signal to it. If you and your source are worried that a telecom or government wants to track you through your mobile phone locations, don't switch off your phones but leave them at a regular-seeming location (such as a home or office) before meeting them. That way, anyone who tracks you will assume that you are both at your offices, rather than being alerted to both your phones 'going dark'.

Don't forget that mobile phone towers only track devices, not individuals. If you buy a new anonymous SIM card and put it into a newly purchased phone, your telecom will see a new device but might not be able to tie it to you unless they see that the device has been hanging out at the same locations (home, office, business travel) you have been.

Conclusion (don't worry!)

There are many things that we can do to make our mobile device location more private. Those include the steps we described above and taking some basic precautions, for example asking a taxi app to drop us off a few blocks further than our home or only turning on our fitness trackers a few minutes after leaving home. This, along with basic security hygiene, should protect journalists from most of the location-based threats that they will face.

There are some situations–such as warzone reporting–where your threat model will differ markedly. This guide does not address such threat models, and we recommend seeking external advice and getting info on the most up-to-date technological and operational recommendations if you're planning a very dangerous reporting trip.

With thanks to Ashley Fowler, Jon Camfield, and Martijn Grooten for some incredible suggestions and revisions