Connected Cars:
Privacy and Security for Survivors

Newer cars now run with computer systems, and may even be connected to the internet. Abusive individuals may misuse or manipulate these new functions, as well as older techniques to track or monitor a vehicle as a way to stalk someone. Connected car functionality can allow another person, other than the driver, to monitor the location of the car, or control features like volume, speed, alarms, or locks. This functionality can definitely be a risk for survivors.

This resource includes information about how to find out if your car is being monitored or controlled remotely, and what the options are to increase your privacy and safety.

What This Does and Doesn't Cover

This resource focuses on situations where an abuser or stalker has had physical access to your car and/or has access to a connected car account. In particular, it discusses ways that person might track your location. There are other privacy concerns associated with connected cars and the data that they may collect; however, this resource doesn't address those.

Connected cars use apps to allow the users to control or monitor the vehicle, even when they are not physically with the car. This resource will explain these apps, tips for increasing privacy and safety, and other tips for responding to abuse or stalking.

Misuse of *connected* car features is not the only way someone can track a car. Most of the material in this resource is focused on connected car features. However, these may or may not be how you are being tracked. Before moving onto them, we list a few other ways that you could be tracked in your car. These apply to both connected and unconnected cars. To skip straight to the content on

connected cars, click on the link that best applies to your situation:
If the Abuser Has or Had Access to the Car.
If the Abuser Has Not Had Access to the Car.

Here are some possible ways a car could be tracked that **aren't** related to the connectivity functionalities:

- Older cars might have a navigation system built-in or added later, such as OnStar or Garmin.
- Both older and newer cars may have on-board diagnostics (OBD) devices. These are meant to help fix problems with the car. An unauthorized OBD could be misused to track your activity.
- There are devices that can be installed that either track information to be downloaded later, or transmit data in real time. These are similar to devices used by insurers in their "safe driver" discount programs, or for parents to monitor teen drivers.
- Newer, more expensive cars offer people who sign up as owners very detailed information including location, speed, driving habits, and even the ability to control some things remotely like volume, speed, or locks.
- Abusive people and stalkers have also hidden other devices in or on cars. These include feature phones (not a smartphone), GPS trackers, and smaller Bluetooth trackers. Bluetooth trackers include:
    - AirTags.
    - Tiles.
    - SmartTags.
    - Trackers meant to be attached to pets' collars in case they get lost, to gather information including location. For more information on this, read more about Location Tracking.

- Your phone could also be used to track you without your knowledge. Read more about phone safety and privacy.
- Publicly-placed cameras, for example at tollbooths, borders, and other checkpoints, or private surveillance cameras connected to national data systems (e.g. Flock) could also make it possible for someone else to find out where your car has been.
- Electronic Toll Bills: If an abuser has access, toll statements may reveal a survivor's travel routes, dates, and times.
- Vehicle Service Bills: If accessible to an abuser, service transactions can disclose recent locations and service dates.
- Credit Card Statements: If an abuser has account access, credit card statements may expose nearby purchases, revealing locations and travel patterns.

Before We Start: Prioritize Safety

Using these options may increase your privacy and safety. They may be useful if you have shared a car with an abusive person in the past. However, these options may not protect you from all remote spying or monitoring. This is true whether the spying is through a car or some other form of tech.

There isn't one "right" way to respond to abuse and car safety concerns. There are only ways that do or don't fit your situation. What works for someone else may not work or be safe for you. Always prioritize safety and trust your instincts. They abusive person may know if you make changes to account settings or the car features. They might change their tactics or escalate their abusive behaviors. In some situations, making changes could also erase evidence. You may find these safety tips useful:

- Use a "safer" car or different type of transportation. This would be any vehicle the abusive person didn't have access to. Consider borrowing someone's car or using public transportation for certain trips you want to keep private.
- Get more information. Connected car features are one way an abusive person may monitor your location or harass you. Navigating violence, abuse, and stalking can be difficult and dangerous. Advocates and service providers can help you figure out options and local resources. They can also help you create a plan for your safety. You can contact a national helpline to be connected with local resources.
- To get more tips about tech abuse and increasing privacy and security, see Safety Net's Survivor Resources Toolkit.

If the Abuser Has or Had Access to the Car

What possibilities are there for misuse?
If the abuser has ever been a legitimate owner of the car, they may never have disconnected or unsynced their app account from the car. This could be true even if you are now the sole owner of the car, or have been awarded sole use of the car by a court. If this is the case, they may still have access to it through the app, which could let them know where the car is and allow them to control certain functions of the vehicle.

Some companies allow car owners to add authorized drivers. If you're the sole owner, consider if you ever added anyone else as an authorized driver or if the abusive person may have used your account to add themselves. If they were never removed as an authorized driver, they could still use the car's features.

There is also a system called Android Automotive OS (AAOS) that comes built into some cars. It can provide infotainment, navigation, messaging, and control of some functions of the car. It is not used on a phone. It is used from inside the car. It allows you to download some apps onto your car just as you could do with a phone or tablet. Wikipedia has a list of car models that have AAOS. Apple is currently working on an equivalent to AAOS.

AAOS is primarily a concern if an abuser or stalker might have physical access to your car. This is because AAOS stores its apps and data in the car itself. An abuser who can get inside the car may be able to open up your AAOS. This could allow them to see how you have used it, which could include messages you have sent through AAOS or where you have driven the car.

How can I regain control?
If you think the abuser knows your car account passwords, you can change them (if you feel safe doing so). You may have other options for adding security to these accounts, depending on the app.

We have a resource that discusses many options for increasing your password safety. It takes into account the reasons why people use weak passwords or reuse passwords. It also provides tips for having strong protection without running into these. In addition, you may also want to look at our Securing Devices & Accounts resource. It discusses tech security options more generally. The best option for you will depend on your situation. Both resources talk about how to figure out what works for you.

Sometimes you may be able to get help by speaking with the car company. Another option is having an advocate speak to the car company, either with you or alone. Companies generally have contact information on their websites. Customer service requests are usually first handled by people who have very little power within the company. This means that you may have to push to "escalate" the issue (send it to someone with higher rank). You may have to do this more than once.

If the Abuser Has Not Had Access to the Car

What possibilities are there for misuse?

In some cases, an abuser may know or be able to guess your car app account password. In this case, they may be able to access your account and from there, use its features for controlling the car. If your car usage data is stored in your account, they may be able to learn about your activities that way.

If you believe that your vehicle is being tracked, but the person has never had access to the account that you know of, consider the other ways that an abuser could monitor the car. In addition, consider talking to an advocate. Without access to either the vehicle itself or the account, it is less likely that the abuser is using the car's connectivity. The abuser could be using a tracker placed on the car, a phone hidden in the car, or some other means.

How can I regain control?

If the person has not had physical access to the car, but you believe they are still controlling or monitoring the car, the issue may be that the abuser knows an account password. From a device you know can't be monitored, change your

password. The How can I regain control? section above has more information about password safety and multi-factor authentication.

The company that provides wireless service for your car stores data about how you use their service. If the abuser knows your password for that company's account, they could view this information. They could also access it if they were on a family plan with you. The section Other related issues: Family plans and carrier apps explains how to regain control in this case.

How do I document misuse of my car?

If something that a person could see or hear is happening while you are in the car, you may be able to document it with a camera. Here are a few examples of this.

- The sound of the car doors locking when you didn't lock them.
- The sight of the car not responding when you attempt to regain control of it. For instance, this could be a video of you trying to unlock the car doors and they won't unlock.
- The sight of the abuser's car at your destination.

If you use a camera to document misuse of your car, it may be better to use a camera on a device that the abuser does not have access to. It may also be better to avoid connecting it to the car. Otherwise, the abuser may be able to access it.

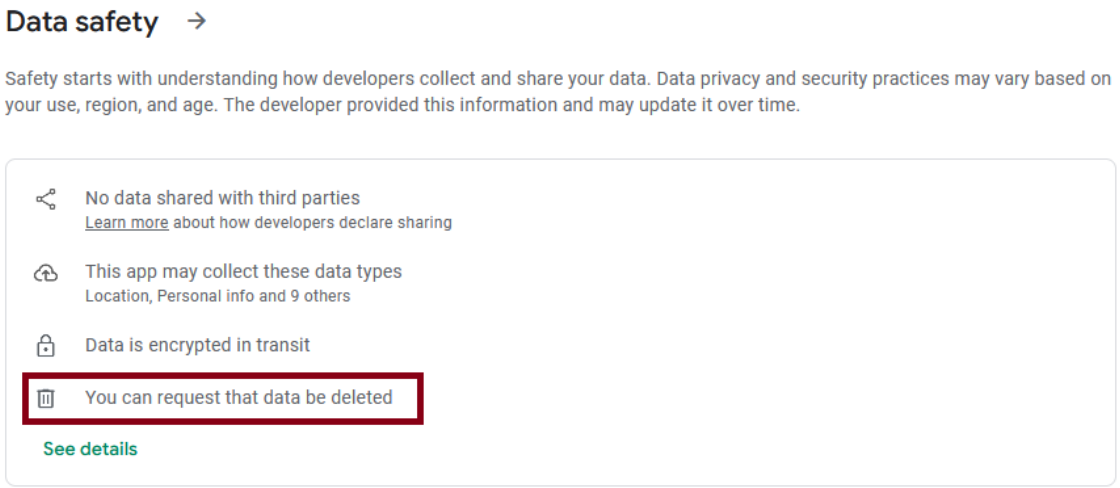
All of these services require some kind of account. There may be evidence of the abusive person's access or activity in the account data. For example, it could show that someone logged into your account from the city the abuser lives in.

You can learn more about documenting tech-facilitated abuse (not just involving cars) from these resources:

- Documentation Tips for Survivors (Safety Net).
- How to Gather Technology Abuse Evidence for Court (Safety Net and NCJFCJ).
- Evidence Issues in Cases Involving Technology (WomensLaw.org).
- Stalking Incident and Behavior Documentation Log (SPARC).

Data privacy concerns and tips

Some tech companies allow users to delete some or all of the data the company has stored about them. This may depend on where you live. To see what privacy rights you have by law, look for your state in the "green" portion of this chart. If it is in this part of the chart AND there is an 'X' under "Right to Delete," then companies *must* allow you to delete your data. Companies *can* still let you delete data if you live in another state (and some do). They are just not *required* to do so. For many apps, you can check whether they let all users delete data by going to their Google Play Store pages. Scroll down to the Data Safety section. If it says "You can request that data be deleted," then you can delete data regardless of which state you live in.



How to delete data will be different for each app or account. Try using Google or another search engine to search "delete data" and then the app or company name to find instructions specific to your app or car.

Other related issues: Family plans and carrier apps

In a connected car, a telecommunications company may provide the wireless connectivity. These companies are called "carriers." Verizon and AT&T are examples of carriers. They may also offer car-related apps to people who already use their phone services. This connectivity can be provided through features built into the vehicle and activated through a free trial or paid subscription. Or, it can be provided with a separate device. This device is plugged into the car's on-board diagnostics (OBD) port. Carrier apps may provide car-based Wi-Fi services to a vehicle, location tracking, crash detection services, and other features.

What possibilities are there for misuse?

Many people use family plans for cell service and data. If an abuser is on a family plan with you, they can log into the account and may be able to see how you have used the services. This could include your use of any car services or where you have traveled. This could also be an issue if an abuser knows or could guess the password to your account with a carrier.

How can I regain control?

The Safe Connections Act of 2022 makes it easier for survivors to leave family plans. Because of this law, you can leave a family plan even if you are not the primary owner of the plan. You can do so in a streamlined way without termination fees. Depending on your state, you may need to provide documentation. The different carriers each have their own processes (T-Mobile; Verizon; AT&T).

Like other accounts, your phone account may have a password. If you are the owner of your phone plan and you think an abuser knows your password, you can change it to help make sure that's not something they can access. You also might be able to add other security features to your account with your carrier as well. See How can I regain control? for links to our resources on password and account safety.

Supported by US DOJ-OVW Grant# 15JOVW-23-GK-05170-MUMU. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of the U.S. Department of Justice.