



WV Executive Branch Privacy Tip

This week's tip is brought to you by the Identity Theft Resource Center (<https://www.idtheftcenter.org/>). Reprinted with permission.



Rental Car Risks: What it means for Your Identity

If you are traveling and plan to rent a car, there is a very specific privacy pitfall threatening you. Rental car companies have begun offering premium features in their fleets of vehicles, including things like Bluetooth sound systems, on-board GPS navigation and infotainment devices for everything from playing music to showing movies. The upgraded technologies can pose a threat to your identity.

Most rental car companies have no policy concerning deleting your Bluetooth-enabled activities from the vehicles once you return them. Some privacy organizations have even rented cars with the intention of seeing what past users are still stored in the device. It was a surprise to discover that many big-name rental car companies do not delete old user information, and that previous renters' info was still easily visible.

Now, this might seem like a small concern in comparison other identity threats – like having your Social Security number stolen – but rental car risks exposing information like downloads, navigation and your phone's identity. Your personal data should not be accessible to anyone else, especially the random individual who rents a car after you.

It is unfortunate that rental car companies are not concerned as they should be about your personal information. Sadly, this is a trend we see across many industries as misuse of personal data and data breaches are on the rise. Even if companies are not as worried about someone finding out your information via rental car technology, there are still steps consumers can take to minimize car rental risk.

Do not connect

The very first solution is to not connect your phone to the vehicle. This might not be ideal for integrated use, but it is the safest of precautions a consumer can take.

Delete the history

If you choose to connect, delete your own history from the Bluetooth system and the GPS navigator. If you do not know how, ask the service department when you return the car.

Block your name

Some Bluetooth-enabled devices will use a nickname for the device when connecting, such as “Lisa’s iPhone.” If your nickname is in your device and is picked up by the car’s system, it is possible that the next patron could piece together your nickname, your whereabouts (from the GPS) and your social media profiles in order to follow you. This could lead to other malicious activity.

Avoid having the GPS take you home

You already know where you live, so if you are using the GPS in a rental car, do not have it take you all the way to your house. It is enough to take you to your city or town, then shut it off and find your own way for the rest of the trip. This prevents others from finding your home location to plan a robbery or other malicious activity.

Do not skip the inspection

Do not skip the inspection when you return a vehicle. It is a good time to ask for help if you cannot delete your Bluetooth activity, and prevents any disputes later about damage to the vehicle. Some car rental places have started letting you place the keys in the car and leave without seeing an attendant, but avoid this and you will be happy in the long run.

Of course, the [Identity Theft Resource Center](#) is here to help. Speak to an identity theft advisor for toll-free, no-cost assistance at (888) 400-5530. For on-the-go assistance, check out the free ID Theft Help App from ITRC.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.