GAO Report: Your Car's GPS May Be Spying On You

January 8, 2014 - A new report from the Government Accountability Office reveals that GPS devices installed in automobiles are being used by auto manufacturers and GPS provider companies to accumulate vast amounts of location based data on users. The report covers a wide variety of risks to consumers in the event of a data breach by these companies. Those risks include stalking, privacy violations and identity theft.

For several years now, auto manufacturers have offered GPS as an option in many of their vehicles and more recently, it has become a standard feature in some luxury cars. As an alternative to installed GPS systems, virtually anyone with a smart phone can access GPS maps and directions from their mobile devices.

There is no real reason that GPS users need to identify themselves by name to use GPS services. But the companies providing the service may have access to that information anyway. Certainly if your GPS system was installed when your car was manufactured, and the service is run by the manufacturer, they know who you are. And since every single GPS device has a unique identifier associated with it, that means that someone out there knows where you are and could potentially provide that information to others whether you want them to or not. This also means that GPS data should now be considered personally identifiable information; just like your SSN or birth date.

The report points out that there are currently no regulatory standards for protection GPS data. Each of the ten companies reviewed by the GAO uses methods to de-identify GPS end users, but the methods each company uses vary widely. In some cases, re-identifying the end user would appear to be a fairly simple process.

All of the companies reviewed by the report also share some of their GPS data with third parties. They do this to provide additional services such as real-time traffic reports. And the shared data is all de-identified. But again, there is no industry or regulatory standard associated with their sharing of data. And there are no current regulations that would require consumer notification in the event of a data breach of GPS data. To the best of our knowledge, none of the state laws requiring consumer data breach notification actually identify GPS data as being "personally identifiable information."

There are some things that consumers can do to protect themselves. Here are a few suggestions:

- Use after-market GPS devices rather than those that are auto manufacturer installed.

- If possible, use a GPS service that doesn't require registration. If this is not an option, pick a user name that can't be associated with you if your GPS data is breached or if your device is lost or stolen.

- Most GPS devices allow users to permanently program their home address into your device. NEVER use your actual address. If this data is ever breached, it would allow a hacker to associate a name with your address, which could lead to fraud or ID theft.

The Washington Times has put together a short video on some of the report's findings. You can find that video below.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS