# High tech in vehicles puts drivers' privacy up for grabs

By Karl Henkel
The Detroit News
February 21, 2014


Every time a motorist slides in behind the wheel, odds are that car or truck is gathering information: How aggressively the driver accelerated, whether the speed limit was observed, how hard the brake pedal was applied. And beyond driving habits, where and when the car was driven, what route was taken and whether the seat belt was buckled.

Few laws or regulations address ownership of data collected by infotainment and navigation systems in dashboards and by electronic black boxes under hoods. Auto data privacy is the industry equivalent of the Wild West, according to automotive industry and law experts.

Should drivers expect information collected by their cars to be private? Can police or other government agencies get their hands on recorded data after a crash to review drivers' whereabouts if they're suspected of a crime? What if automakers decided to sell details about driving habits to marketers who want to broadcast targeted ads as motorists run errands?

These questions come at a time when many Americans are fearful of their privacy in the wake of National Security Agency leaks and the answers are largely unclear.

One thing is sure: Automakers collect data and they share it, several recently told a Government Accountability Office investigation. And according to the terms of use for many voice-activated and navigation systems, automakers have the right to share that information with marketers or anyone else they might want to.

Those facts — and the secrecy surrounding what automakers might do with personal information — have alarmed consumer advocates and raised questions within the industry about the future of data collection.

"The automotive industry needs to think hard about the type of information they want to collect and who they want to pass it on to," said Thilo Koslowski, a vice president at technology research firm Gartner Inc. "Anything that focuses more on the driver than the vehicle, that's where consumers won't find a whole lot of value."

Few laws restrict what information can be collected, how long it can be saved and who it can be shared with — whether with private companies or the government.

The Driver Privacy Act, pending in Washington, pertains only to so-called event data recorders, or "black boxes." Like the black boxes on commercial aircraft, they save key information — in this instance speed, brake application and seat belt use. The moments leading up to an accident, for example, would be recorded. The recorders cannot, however, transmit data in real time.

Fourteen states have laws restricting who can access black-box data and how it can be shared, according to the National Conference of State Legislatures. California, for instance, says owners of the vehicle can retrieve black box information, but so can law enforcement authorities depending on court jurisdiction. Michigan has no such prohibitions. And no states prohibit police from accessing information after a crash.

President Barack Obama in 2012 introduced a White House Consumer Privacy Bill of Rights that outlines a set of common privacy practices for multiple industries, including automotive. But on the eve of its second birthday, the blueprint hasn't gained traction with lawmakers.

Sen. Al Franken, D-Minn., who chairs the Judiciary subcommittee on Privacy, Technology and the Law, recently queried Ford Motor Co. after the automaker's marketing chief, Jim Farley, said the company knew the whereabouts of millions of customers. Ford admitted to collecting data but not sharing it, although its customer agreement for its SYNC voice-activated system says it can do so.

Franken said he plans to reintroduce a location privacy bill in the coming weeks.

Mark Aiello, a partner and automotive industry team leader with the Detroit office of international law firm Foley & Lardner LLP, said that “there’s just not a lot of law on this subject as it pertains to vehicles.”

“It’s a new, developing area, as most of the case law today has dealt with cellphones that track or locate a person,” he said.

Ford Motor Co. chief executive Alan Mulally has called on the federal government to provide guidance on consumer privacy. “It’s really important that we have boundaries and guidelines,” he said at the Detroit auto show last month.

Ford recently received a patent for targeted in-car advertisements: Cars would collect data, including location, to decide which ads to broadcast to each driver. Other automakers are looking at similar features.

Some studies suggest a majority of consumers would accept microtargeted ads, but Koslowski said motorists might consider such targeted advertising more invasive than helpful. “If the marketing angle was that interesting, Google would have been there 10 years ago,” he said.

High Court's stance unclear

The U.S. Supreme Court has indicated it isn’t sure how it would rule in some cases involving automotive privacy.

In the 2012 case United States v. Jones, the court found that long-term attachment of a GPS by the government to a private citizen’s vehicle constitutes a search under the Fourth Amendment. Justice Samuel Alito wrote that “even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.”

Data collection for infotainment, voice-activated or navigation systems is outlined in written terms agreed to by consumers before they use a voice-activated, navigation or infotainment system. Those agreements are often filled with dense legal jargon. Most motorists click “yes” without reading.

Some public interest groups such as the Washington-based Electronic Privacy Information Center are calling for federal legislation to make those contracts consumer friendly; drivers would decide exactly what data could be shared.

“None of this data collection should be turned on as default, especially when they are collecting so much information,” said Khaliah Barnes, administrative law counsel at the center.

Until the rules become clearer, motorists could unknowingly share personal information or have their own data used against them in court.

“These are still corporations and this information is still going to be worth a lot of money to various people,” said attorney Steven Gursten, owner at Michigan Auto Law and president of the Motor Vehicle Trial Lawyers Association. “We are depending on the good citizenship of nameless people in giant corporations to keep our info private.”

Driver-less complications

Automakers are working on driverless-car technology that could help prevent accidents. Comprehensive communication between cars, traffic signals and buildings are at the foundation of these plans, and that requires constant updating of information like location and speed.

At first glance, collection of that information would seem harmless.

It could, for example, be used to help police solve a crime. Though the Supreme Court said the government cannot place a GPS device on a car for long-term tracking without a driver's knowledge, it said nothing about information obtained from a device that a driver knows is there.

Let's say a gas station was robbed and law enforcement wanted to secretly tap into information about a car that it suspects might have been used in the getaway. Aiello, a lawyer, said it's unlikely the government could legally access locator information transmitted from that car without a warrant. But if it requested information about all cars that might have been within 1,000 feet of the gas station at the time of the crime, it's less likely a warrant would be necessary.

"That's going to be the next big case," Aiello said. "It's going to be a vehicle that a driver purchased with GPS ... and knows that an automaker is tracking that GPS."

There are also legal ramifications if a federal agency — specifically, the National Highway Transportation Safety Administration — mandates technology that would track a vehicle's location. NHTSA this month said it will require for all new vehicles to eventually communicate with one another to help reduce accidents. That could pose not only privacy, but also safety threats, as sophisticated hackers could take over wireless signals exchanged between cars.

Federally mandated GPS tracking devices would not be subject to Fourth Amendment protections under current law, the Supreme Court said in its ruling.