

No, cops aren't using SiriusXM to find criminals. Here's how they do it

reader comments

111 with 64 posters participating

Share this story

An Ars reader this week drew our attention to a news story out of Southern California. The case involved a man wanted on suspicion of attempted murder and other alleged crimes. He fled from one county to another, but according to the article, sheriff's deputies were able to locate him by "sending a 'ping' to his Sirius satellite radio," after which the suspect was found and arrested.

The mysterious "ping" grabbed the reader's attention, as well as several Ars staffers: what, exactly, did law enforcement do? How did it work? And what are the implications for everyone driving around with a SiriusXM satellite radio in their car?

The case

A representative for Sirius was unable to say if the company was involved in any specific way in this particular case or even if the case did indeed involve an actual Sirius product. Whatever happened, calling it a "Sirius radio ping" was probably a misnomer, the company told Ars, as Sirius satellite radio itself is a one-way operation. The actual radios have no

geolocating capacity and can't "ping" anything back to anyone.

That said, however, Sirius isn't just a radio company—it offers a variety of "connected car solutions." Among those solutions is SiriusXM Guardian, which is available on the Fiat Chrysler Uconnect infotainment system. Cars that have telematics equipment installed by the manufacturer—in this case, Fiat Chrysler—can send data over mobile networks using Sirius' connected services. Those cars, Sirius said, are a small subset of the total number of vehicles that have satellite radios installed.

Sirius additionally told Ars that it sporadically works with law enforcement bodies to comply with valid vehicle-location court orders. The company stressed that it does so by remotely activating the installed telematics hardware in a car, rather than by interacting in any way with the actual satellite radio.

The San Diego County Sheriff's Department, which apprehended the suspect in its jurisdiction, said the man was driving a Jeep Wrangler. Uconnect has indeed been available in Jeep vehicles for several model years. The Imperial County Sheriff's Office (where the suspect fled from) confirmed to Ars both that the suspect was one of the registered owners of the car and also that there was a Uconnect subscription registered to the vehicle.

The Uconnect privacy policy confirms that the service automatically collects user location data and that the company may share it, among other reasons, "to comply with applicable legal or regulatory obligations, including as part of a judicial proceeding, in response to a subpoena, warrant, court order, or other legal process, or as part of an investigation of or request by law enforcement or a government official." It seems that is what happened in this case.

The context

The majority of new model cars, from all automaker groups, now have some kind of onboard connectivity platform available to buyers. Those platforms—such as BMW’s iDrive, Volkswagen’s Car-Net, Ford’s Sync, and General Motors’ OnStar—have similar language disclosing the potential sharing of location data in their terms of service or privacy policies.

This kind of tracking, which is not particularly new, is sold as a benefit to subscribers, who can access the stolen vehicle assistance feature after filing a police report about the theft. Such cases pop up in local media from time to time, including a California story from 2016 and a Florida example from 2017.

The ability for your car to be precisely tracked, though, comes with exactly the kind of privacy concerns you would think. In 2017, Forbes delved into the world of “cartapping,” in which law enforcement agencies used telematics services such as Sirius or OnStar to locate or eavesdrop on individuals under investigation.

Attorneys for defendants arrested after such location data was gathered tried to have the evidence thrown out, Forbes found, but in multiple cases, judges declined. In one instance, a judge ruled that accessing the onboard OnStar device in a vehicle was not materially different from planting a GPS tracker on a suspect’s car. In another, a different judge determined that someone in the car turned on OnStar services and the police just happened find drugs in the car when showing up to have a look.

“Location information is highly sensitive and deserves protection under the Fourth Amendment,” American Civil Liberties Union staff attorney Nathan Freed Wessler told Ars. The technological ability for police to track almost any car in detail with essentially the push of a single button is new,

legally speaking, and needs to be done carefully. “If police are going to use onboard telematics data at all, they should have to go to a judge and get a warrant,” Wessler added.

It is unclear if Imperial County authorities had a court order for the vehicle location information in this case; the San Diego County authorities told Ars the suspect was allegedly suicidal during the 2:30am chase and that Imperial County law enforcement were concerned for his safety. In such exigent circumstances, Wessler said, where there is an “imminent threat” to someone’s life or safety, an exception to needing a court order is fine in principle—but it’s important that kind of exception not be abused.

<https://arstechnica.com/?p=1640011>