Court Documents Reveal How Feds Spied On Connected Cars For 15 Years

Wherever there is a connected device with a microphone, you can be 100 percent certain that some government agency is tapped into it and able to hear every word you speak. This means, connected cars, Smart Phones, Smart TV's, Alexa, Siri, etc. TN Editor

It's not always necessary to break into your computer or smartphone to spy on you. Today all are day-to-day devices are becoming more connected to networks than ever to add convenience and ease to daily activities.

But here's what we forget: These connected devices can be turned against us because we are giving companies, hackers, and law enforcement a large number of entry points to break into our network.

These connected devices can also be a great boon for law enforcement that can listen and track us everywhere.

Let's take the recent example of 2016 Arkansas murder case where

Amazon was asked to hand over audio recordings from a suspect's Echo.

However, that was not the first case where feds asked any company to hand over data from a suspect's connected device, as they have long retrieved such information from connected cars.
According to court documents obtained by Forbes, United States federal agencies have a 15-year history of "Cartapping" — where vehicle tech providers are ordered to hand over almost real-time audio and location data from a user.

How Police Have Spied On Connected-Cars For Years?

Example? In 2014, satellite radio and telematics provider SiriusXM provided location information of a Toyota 4-Runner following a warrant by New York police, which was recently unsealed.

The warrant asked SiriusXM "to activate and monitor as a tracking device the SIRIUS XM Satellite Radio installed on the Target Vehicle" for ten days, and the company admitted to Forbes that it complied with the order.

How did SiriusXM achieve this? The company simply turned on the stolen vehicle recovery feature of its Connected Vehicle Services technology on the target vehicle, Toyota 4-Runner. It's like Apple turning on the Find My iPhone feature to track a customer's location, the court documents [PDF] says.

SiriusXM said it worked with law enforcement periodically to provide such information on its customers with just a valid warrant. The company receives an estimated five valid court orders a year to monitor a suspect, though it declined to offer on-record comment.

SiriusXM is not alone. General Motors (GM) had repeatedly worked with federal agencies to provide not just location but also audio through its OnStar service, where people conversations are recorded when the in-car cellular connection is turned on.

According to Forbes, police asked GM to hand over OnStar data in

December 2009 from a Chevrolet Tahoe rented by suspected crack cocaine dealer Riley Dantzler.

OnStar's tracking is so accurate that even after the feds had no idea about Dantzler's car, it's able to "identify that vehicle among the many that were on Interstate 20 that evening," followed him from Houston, Texas, to Ouachita Parish, stopped Dantzler and found cocaine, ecstasy and a gun inside the car.

The defense lawyer argued that the court order compelling OnStar to hand over data was made in Louisiana, but since the tracking started in Texas, it went beyond the court jurisdiction.
In a separate case in 2007, OnStar was ordered to track and continuously reveal the physical location of GMC Envoy SUV of suspected heroin dealer Lamauro Coleman as he traveled around Michigan. When he was stopped, the feds found 43 grams of heroin.

Here's what Coleman's representation argued:

> *"The statute is silent as to the authority of the government to use a 3rd party product in [place] of physically installing a device of their own."*
>
> *"Allowing this type of intrusion is a leap the court shouldn't be willing to make. Authorizing OnStar agents to activate the system within a suspect's car renders statutory authority null. It effectively makes every single General Motors vehicle and every OnStar service representative an agent of the government."*

When talking about audio data, OnStar competitor ATX Technologies in 2001 was also ordered to provide "roving interceptions" data of a Mercedes Benz S430V. ATX complied with the order in November and spied on audible communications for 30 days, but declined when the FBI asked for an extension in December, the court documents [PDF] revealed.

In 2007, OnStar was ordered to provide audio data from a Chevrolet Tahoe belonging to Gareth Wilson in Ohio.

An emergency button in Wilson’s car was automatically pushed without his knowledge, which allowed an officer from the Office of the Fairfield County Sheriff to listen to the conversation about a possible drug deal, reads a 2008 opinion from the case.

Read full article here…