Are Self-Driving Cars a National Security Risk?

automoblog.net/self-driving-cars-security-risk/

Over the last decade-plus, autonomous vehicles (AVs) have been a major story in the automotive industry, capturing headlines and imaginations around the world. That narrative continues to take shape and move from story to reality, with the Insurance Institute for Highway Safety (IIHS) predicting 3.5 million self-driving cars on U.S. roads by 2025.

However, in addition to billions of dollars of investment and countless hours of engineering and research, self-driving cars have also brought new questions about safety and security to the industry. As more AVs start to hit the road for private and public use, these questions about personal and even national security become increasingly relevant – and increasingly urgent.

The FBI Says Self-Driving Cars Are a Security Risk

In January of 2023, FBI Director Christopher Wray spoke to the World Economic Forum Discussion on Technology and National Security in Davos, Switzerland about the potential threats posed by self-driving cars. He mentioned that AVs could be used as tools to harm people and a source of valuable and vulnerable personal data.

“When you talk about autonomous vehicles, it’s obviously something that we’re excited about, just like everybody,” said Wray. “But there are harms that we have to guard against that are more than just the obvious.”

Wray described self-driving cars as a potential new “attack” surface for terrorists to use to harm civilians. Referencing Russia’s current invasion of Ukraine, he discussed how online surveillance activity can be an early sign of a forthcoming attempt at cyber attacks. He also mentioned that the FBI and other agencies have noticed an uptick in digital surveillance activities within the U.S. from outside actors.

FBI Director Christopher Wray. Public domain photo by the Federal Bureau of Investigation, via Wikimedia Commons

“We’re increasingly concerned that the surveillance activity – the scanning, the research, all the preparatory activity – could be one thing, could be an indication of something more serious,” Wray said.

The FBI director also spoke about the potential for malicious use of personal data gathered by self-driving vehicles.

“A different kind of harm we’re concerned about is the enormous amount of data that autonomous vehicles, for example, aggregate,” said Wray. “And any time you aggregate lots and lots of sensitive data, it makes a very tempting target.”

Self-Driving Car Security Risks Have Already Been Demonstrated

Wray’s statements in Davos aren’t just theoretical. There are already real-world examples of how vulnerable self-driving cars can be. In his comments, Wray referenced a story about a simple way researchers were able to trick an automated Tesla.

“I’m thinking about a story I heard not that long ago about the researchers who were able to trick a self-driving car’s algorithm by essentially putting a piece of black tape over a stop sign,” he told the panel. “It caused the car to accelerate, about 50 miles an hour or

something."

The details of the story Wray referenced differ slightly from his anecdote, but the concerns it raised are the same.
In 2020, researchers at McAfee used a piece of tape to change a speed limit sign from 35 miles per hour to 85 miles per hour. The team reported that this resulted in the Tesla's cruise control automatically accelerating 50 miles per hour.

The researchers used a 2016 Tesla Model S and Model X in their test. Tesla said that later models didn't have the same vulnerability, which was attributed to a camera developed by Mobileye. Regardless, the team at McAfee's testing revealed just one of the ways in which AVs can be manipulated.

Cars Can Be Hacked and Controlled Remotely

Even if engineers at Tesla and other automakers producing AVs have rectified the specific vulnerability exposed by McAfee researchers, there are other potential threats. One of the major risks is cyber attacks from hackers.

In 2015, two cybersecurity professionals demonstrated how someone could hack into a vehicle and take control of it remotely. Chris Valasek and Charlie Miller, director of Vehicle Security Research at IOActive and a security researcher at Twitter at the time, respectively, were able to hack into a Jeep Cherokee and control its radio and other functions. Andy Greenberg, a reporter for Wired, drove the car as it was under Valasek and Miller's control and wrote about his experience.

"Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system," wrote Greenberg. "Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass."

After controlling some of the vehicle's electronic functions, Valasek and Miller moved onto a more serious exploit, cutting the Jeep's transmission while it was in motion.

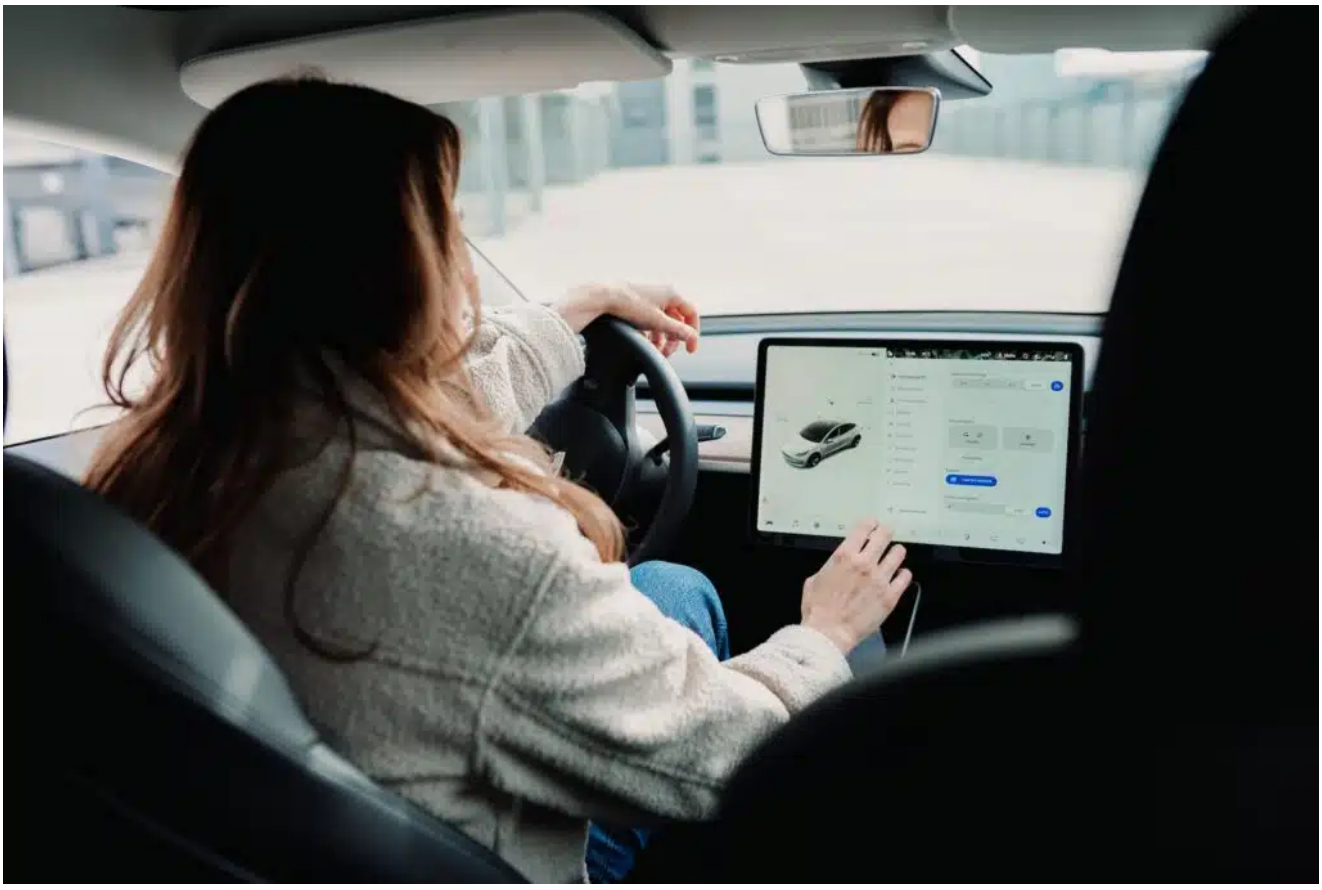
"Immediately my accelerator stopped working," Greenberg wrote. "As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an escape. The experiment had ceased to be fun."

While this demonstration happened in a controlled setting, it provided proof that increasingly-connected cars were hackable. It also offered a glimpse into how serious the consequences of such a hack could be.

All Modern Cars Can Be Hacked, But AVs Present Different Dangers

Notably, the Jeep Cherokee Valasek and Miller hacked was not a self-driving car. In an interview with Automoblog, security engineer and software developer Zac Morris said that an increasing reliance on electronically-controlled components opens up a risk to all vehicles, and not just autonomous ones.

“Non self-driving cars will be very likely attackable in all of the same ways as self-driving cars,” said Morris. “Nowadays, most cars are drive-by-wire. The wheel and pedals aren’t actually attached through hardware to the wheels, brakes, and throttle. Instead, they run through the electronic control unit, which modulates everything you input combined with functions calculated by the vehicle’s driver assist features. This includes things like steering assist and safety features like slide prevention and anti-lock brakes.”



Many automobile functions are increasingly controlled electronically. Photo by Jenny Ueberberg via Unsplash.

But while non-autonomous cars are also at risk for hacking, Morris suggested that the nature of driverless vehicles and technological developments around them could exacerbate the effects of a hack.

“For example, my car has basic AI in it for the lane assist feature,” he said. “But, my car also has a steering wheel. Even when it’s doing the lane assist thing I’m at the very least mostly paying attention to it. So, if the car tries to whip me into the median at 80 miles per hour, I’m more likely to catch it before it kills me. Tesla wants to take the steering wheels out of cars.”

Morris said that while AVs aren’t inherently more or less hackable than non-self-driving cars, drivers of AVs could be less able to counter a cyber attack on the road.

“There’s just not a lot you can do to stop it when every input you as the ‘driver’ have to control the car goes through the control unit that’s being tampered with,” he said. “The lack of any input consideration from the driver at all means accomplishing actual harm will be easier.”

The Security of Driver Data Is Also a Concern

In his address, the FBI director also mentioned a security concern over personal data. However, Wray isn’t the only government official to have brought up these concerns.

In September, 2021, the House of Representatives formed the Vehicle Data Access caucus, a bipartisan committee centered around driver data issues. At the time, Rep. Earl “Buddy” Carter (R-GA), who announced the caucus’ formation, spoke to the group’s purpose in a press release.

“We must ensure that users have access to the data being collected from [data collectors] and that the information is shielded from bad actors here and abroad,” said Carter. “Privacy, security, and innovation should go hand-in-hand.”

Telematics programs, which insurance companies use to monitor driver behavior and adjust premiums, are one of the committee’s main focal points. These programs track driving behaviors such as speed, braking, and even driver movements inside the vehicle and report them to private insurance companies. However, Morris said that the influx of technology in cars is also cause for concerns about data privacy.

“Modern cars have cameras and microphones all over the place, inside and out,” he said. “They also have a wealth of other data sources.”

Current-generation Tesla vehicles, for example, feature nine cameras in total – eight on the exterior and one on the interior. These cameras aid in the vehicles’ autopilot functions by constantly monitoring their surroundings and measuring distances between objects, speed, movement, and other variables. They can also record crashes and other traffic events to provide a record of the incident.

However, the cameras continue to run when the vehicles are off and unoccupied. This allows them to serve a surveillance function, ostensibly as an anti-theft and anti-vandalism feature.

Tesla vehicles have exterior cameras that can be activated even when the car is turned off. Photo by Taneli Lahtinen via Unsplash.

But in April, 2023, Reuters reported that Tesla employees had been sharing videos with each other and sometimes with people outside the organization. In its privacy notice, the company says that “camera recordings remain anonymous and are not linked to you or your vehicle.” However, videos also contain location data, allowing people with access to pinpoint where a vehicle was parked at the time of the recording – often at a person’s home.

Tesla said that it only received videos with owner consent and had stopped receiving videos from cars that were inactive. But Reuters reported comments from Tesla employees that said they were able to see private spaces such as the inside of a person’s garage in the videos they received, highlighting the potential for misuse.

Self-driving cars require features like cameras and light detection and ranging (LiDAR) to navigate their environments safely. But in doing so, they generate massive amounts of data about drivers inside the vehicle and the world around it. What bad actors could potentially do with that data is still a matter of speculation, but Morris said that the issue of automotive data collection is one many have yet to fully consider.

“We’re creating a massive number of surveillance drones on wheels that we pay money to own,” he said.

Concerns Remain, Yet AV Research and Development Presses Forward

Despite concerns about security risks and data privacy related to autonomous vehicles and automation features in other cars, researchers and engineers continue to push their development in the private and public sectors. A team of researchers at North Carolina A&T University's College of Engineering, for example, expects to launch an automated shuttle pilot program this fall. In June, it was reported that Google spinoff Waymo and other AV companies are seeking approval from San Francisco city officials to launch fleets of self-driving taxis.

It's clear that these concerns aren't slowing the progress of AV development. But Wray's comments at Davos suggest that the issues of security risks around self-driving cars and data privacy are on the government's radar. The FBI director expressed similar sentiments about the need to balance innovation with security as Rep. Carter voiced when he formed the Vehicle Data Access caucus.

"When you talk about autonomous vehicles, it's obviously something that we're excited about, just like everybody," Wray said. "But there are harms that we have to guard against that are more than just the obvious."

Whether government agencies concerned with security and privacy issues around self-driving cars will attempt to resolve those issues through regulation and other actions remains to be seen. Morris said that he believes they have yet to be adequately addressed in the private and public sectors. However, he said he still thinks self-driving cars still have the potential to be beneficial and make roads less dangerous.

"Self-driving car advocates are correct that if they can reach level four of self-driving development, it will make cars safer," said Morris. "When you think about it, it's kind of nuts that we let humans control 3500-pound machines that can go 140 miles per hour."