Tesla cars keep more data than you think and spy on everything

- Crashed Tesla vehicles, sold at junk yards and auctions, contain deeply personal and unencrypted data including info from drivers' paired mobile devices, and video showing what happened just before the accident.
- Security researcher GreenTheOnly extracted unencrypted video, phonebooks, calendar items and other data from Model S, Model X and Model 3 vehicles purchased for testing and research at salvage.
- Hackers who test or modify the systems in their own Tesla vehicles are flagged internally, ensuring that they are not among the first to receive over-the-air software updates first.

Kate Fazzini | Lora Kolodny
CNBC.com

Robyn Beck | Pool | Getty Images
Elon Musk, CEO of Tesla, speaks at an unveiling event for the Boring Company's test tunnel in Hawthorne, Calif., on Dec. 18, 2018.

If you crash your Tesla, when it goes to the junk yard, it could carry a bunch of your history with it.

That's because the computers on Tesla vehicles keep everything that drivers have voluntarily stored on their cars, plus tons of other information generated by the vehicles including video, location and navigational data showing exactly what happened leading up to a crash, according to two security researchers.

One researcher, who calls himself GreenTheOnly, describes himself as a "white hat hacker" and a Tesla enthusiast who drives a Model X. He has extracted this kind of data from the computers in a salvaged Tesla Model S, Model X and two Model 3 vehicles, while also making tens of thousands of dollars cashing in on Tesla bug bounties in recent years. He agreed to speak and share data and video with CNBC on the condition of pseudonymity, citing privacy concerns.

Many other cars download and store data from users, particularly information from paired cellphones, such as contact information. The practice is widespread enough that the US Federal Trade Commission has issued advisories to drivers warning them about pairing devices to rental cars, and urging them to learn how to wipe their cars' systems clean before returning a rental or selling a car they owned.

But the researchers' findings highlight how Tesla is full of contradictions on privacy and cybersecurity. On one hand, Tesla holds car-generated data closely, and has fought customers in court to refrain from giving up vehicle data. Owners must purchase $995 cables and download a software kit from Tesla to get limited information out of their cars via "event data recorders" there, should they need this for legal, insurance or other reasons.

At the same time, crashed Teslas that are sent to salvage can yield unencrypted and personally revealing data to anyone who takes possession of the car's computer and knows how to extract it.

The contrast raises questions about whether Tesla has clearly defined goals for data security, and who its existing rules are meant to protect.

A Tesla spokesperson said:

> "Tesla already offers options that customers can use to protect personal data stored on their car, including a factory reset option for deleting personal data and restoring customized settings to factory defaults, and a Valet Mode for hiding personal data (among other functions) when giving their keys to a valet. That said, we are always committed to finding and improving upon the right balance between technical vehicle needs and the privacy of our customers."

What your Tesla knows

Data stored on a Tesla Model S, Model X or Model 3 vehicle is not automatically erased when the car is hauled away from an accident site or sold at auction. This means personal details remain on the car, and can be learned by people who come into possession of the car or certain of its components, according to GreenTheOnly's research.

Tesla sometimes uses an automotive auction company called Manheim to inspect, recondition and sell used cars. A former Manheim employee, who asked to remain anonymous, confirmed that employees do not wipe the cars' computers with a factory reset. Manheim declined to comment.

GreenTheOnly and fellow white-hat hacker Theo, a Tesla proponent who has repaired hundreds of wrecked Teslas, bought a totaled white Model 3 for research purposes late last year. They found the vehicle was owned by a construction company in the greater Boston area, and used by people who worked there. The construction company did not respond to multiple requests for an interview.

Theo
Security researchers bought this wrecked Model 3 to evaluate the data that remains in the car's computers after a crash.

The researchers shared records with CNBC that showed the car's computers had stored data from at least 17 different devices. The data was not encrypted.

Mobile phones or tablets had paired to the car around 170 times. The Model 3 held 11 phonebooks' worth of contact information from drivers or passengers who had paired their devices, and calendar entries with descriptions of planned appointments, and e-mail addresses of those invited. **(**CNBC called and e-mailed several of the people who had paired their phones to the vehicle to verify their information was authentic.)

The data also showed the drivers' last 73 navigation locations including residential addresses, the Wequassett Resort and Golf Club, and local Chik-Fil-A and Home Depot locations.

Then, there was the crash.

This video extracted from the wrecked Model 3 shows the car speeding out of the right lane into the trees off the left side of a dark two-lane route.

GPS and other vehicle data reveals that the accident happened in Orleans, Massachusetts, on Namequoit Road, at 11:15 pm on Aug 11, and was severe enough that airbags deployed.

Call logs show that an iPhone present in the car at the time of the crash belonged to a relative of the founder and chairman of the company that owned the Model 3. Moments before the vehicle crashed, researchers found, incoming call logs indicate that a family member had called the driver of the Model 3.

Another video stored on the car showed an earlier accident where the Model 3 side-swiped a guard rail.

Rolling computers

In general, cars have become rolling computers that slurp up personal data from users' mobile devices to enable "infotainment" features or services. Additional data generated by the car enables and trains advanced driver-assistance systems. Major auto-makers that compete with Tesla's Autopilot include GM's Cadillac Super Cruise, Nissan Infiniti's ProPilot Assist and Volvo's Pilot Assist system.

But GreenTheOnly and Theo noted that in Teslas, dashboard cameras and selfie cameras can record while the car is parked, even in your garage, and there is no way for an owner to know when they may be doing so. The cameras enable desirable features like "sentry mode." They also enable wipers to "see" raindrops and switch on automatically, for example.

GreenTheOnly explained, "Tesla is not super transparent about what and when they are recording, and storing on internal systems. You can opt out of all data collection. But then you lose [over-the-air software updates] and a bunch of other functionality. So, understandably, nobody does that, and I also begrudgingly accepted it."

Theo and GreenTheOnly also said Model 3, Model S and Model X vehicles try to upload autopilot and other data to Tesla in the event of a crash. The cars have the capability to upload other data, but the researchers don't know if and under what circumstances they attempt to do so.

Tesla has a reputation as technologically cutting-edge and friendly to white-hat hackers.

For example, Tesla was the first auto maker to offer "over the air" updates to its cars. CEO Elon Musk shows up at cybersecurity gatherings like DefCon, to the delight of the "makers and breakers" of code who attend them.

> tweet 1

The company is one of a handful of large corporations to openly court cybersecurity professionals to its networks, urging those who find flaws in Tesla systems to report them in an orderly process — one that gives the company time to fix the problem before it is disclosed. Tesla routinely pays out five-figure sums to individuals who find and successfully report these flaws.

Even in his PayPal days, CEO Elon Musk was an early proponent of this kind of crowdsourced security research, notes David Baker Chief Security Officer at BugCrowd, the platform Tesla uses to manage its own "bug bounty" program.

However, according to two former Tesla service employees who requested anonymity, when owners try to analyze or modify their own vehicles' systems,

the company may flag them as hackers, alerting Telsa of their skills. Tesla then ensures that these flagged people are not among the first to get new software updates.

Baker is sympathetic. He said: "Tesla does have to safeguard against those who would try to reverse-engineer their software, or engage in malicious hacking. And they can't just wipe the car necessarily. These are computers. There could be a forensic need to contain and retain the data. But I would think that what they will want to work on is a way to have all that stored data encrypted, as it would be on your cell phone."

WATCH: This Tesla owner got so frustrated waiting for repairs, he took matters into his own hands.

Tesla owner frustrated so repairs his own Model S and says it's easy as 'Legos' 1:58 PM ET Tue, 28 Aug 2018 | 05:16

Kate FazziniTechnology Reporter