

Hacker buys old Tesla parts on eBay, finds them full of user data



Enlarge / Inside a Tesla.

reader comments

41 with 32 posters participating

Share this story

Tesla infotainment systems are a marvel to behold. Among other things, they display Netflix or Youtube videos, run Spotify, connect to Wi-Fi, and of course store phone numbers of contacts. But those benefits require storing heaps of personal information that an amateur researcher found can reveal

owners' most sensitive data.

The researcher, who described himself as a “Tesla tinkerer that’s curious about how things work,” recently gained access to 13 Tesla MCUs—short for media control units—that were removed from electric vehicles during repairs and refurbishments. Each one of the devices stored a trove of sensitive information despite being retired. Examples included phonebooks from connected cell phones, call logs containing hundreds of entries, recent calendar entries, Spotify and W-Fi passwords stored in plaintext, locations for home, work, and all places navigated to, and session cookies that allowed access to Netflix and YouTube (and attached Gmail accounts).

All 13 of the devices showed that their last location was at a Tesla service center, an indication that they were removed by an authorized Tesla technician. Tesla service stations remove MCUs for several reasons. Most commonly, it’s to replace a faulty device or to upgrade to a newer, more advanced device model that improves the vehicle autopilot.

Your data on eBay

The researcher, who goes by the handle greentheonly, told me he obtained 12 of the units off of eBay from pages like this one. He got the other one from a friend. Based on conversations he’s had, he believes Tesla official procedure calls for removed MCUs to be sent intact back to Tesla and for damaged units to be hammered down to ensure that connectors are sufficiently damaged and then thrown into the trash.

“It looks like some service center employees sell intact units on the side instead of returning them (I imagine they just create a record of destruction/disposal internally),” the researcher said in an interview. “I know some people running salvage yards that say that’s one source of units they have for sale.”

Tesla representatives didn't return an email asking what the company's policy is for handling MCUs that are removed from vehicles.

greentheonly's discovery reveals a risk posed not just to Tesla owners but drivers of virtually any vehicle that has onboard devices that store personal data or provide remote tracking. A man who rented Ford vehicles from Enterprise Rent-a-Car reported having the ability to remotely start, stop, lock, unlock the vehicles long after he returned them not just once, but a second time four months after the first. As is the case with Tesla MCUs that make it back onto the market, the failure of rental companies to mandate that employees fully wipe infotainment systems of all previous customers' data represents a safety and privacy risk that could easily be avoided.

The moral of these stories is that it's up to individuals to perform factory resets when selling a car, returning a rental vehicle, or having an infotainment system serviced. Even then, there's no guarantee that previously stored data can't be recovered. The researcher said the Tesla MCUs keep information in a SQLite database that isn't deleted until the hard drive blocks that store it are overwritten by new data. While a factory reset may not be foolproof, it's likely to make the recovery process difficult and time consuming enough to provide a meaningful, if imperfect, defense. When possible, the truly security conscious should destroy the units.

<https://arstechnica.com/?p=1673633>