



**PRESS RELEASE | EMBARGOED UNTIL WEDNESDAY, SEPTEMBER 6  
@ 4AM CENTRAL EUROPEAN TIME**

**Press contacts:**

U.S. | Helena Dea Bala, [helena@pkpr.com](mailto:helena@pkpr.com)

Europe | Tracy Kariuki, [tracy@mozillafoundation.org](mailto:tracy@mozillafoundation.org)

---

**‘Privacy Nightmare on Wheels’:  
Every Car Brand Reviewed By Mozilla — Including Ford,  
Volkswagen and Toyota — Flunks Privacy Test**

*Mozilla’s latest edition of [\\*Privacy Not Included](#) reveals how 25 major car brands collect and share deeply personal data, including sexual activity, facial expressions, and genetic and health information*

**(WEDNESDAY, SEPTEMBER 6, 2023)** -- All 25 major car brands reviewed in [Mozilla’s latest edition of \\*Privacy Not Included](#) (\*PNI) received failing marks for consumer privacy, a first in the buyer's guide’s seven-year history.

According to Mozilla research, popular global brands — including **BMW, Ford, Toyota, Tesla, Kia, and Subaru** — can collect deeply personal data such as sexual activity, immigration status, race, facial expressions, weight, health and genetic information, and where you drive. Researchers found data is being gathered via sensors, microphones, cameras, and the phones and devices drivers connect to their cars, as well as through car apps, company websites, dealerships, and [vehicle telematics](#). Brands can then share or sell this data to third parties. Car brands can also take much of this data and use it to develop inferences about a driver’s intelligence, abilities, characteristics, preferences, and more.

In another first for Mozilla's \*Privacy Not Included research, none of the brands meet Mozilla's [Minimum Security Standards](#). Specifically, researchers couldn't confirm whether *any* of the brands encrypt all of the personal information they store on vehicles, and only one of the brands (**Mercedes**) even replied to Mozilla's questions about encryption.

The newest edition of \*PNI examines the privacy and security flaws of car brands spanning five countries: the U.S., Germany, Japan, France, and South Korea. Researchers spent 600 hours reading privacy policies, downloading apps, and corresponding with brands; the full methodology can be found [here](#).

The very worst offender is **Nissan**. The Japanese car manufacturer admits in their privacy policy to collecting a wide range of information, including sexual activity, health diagnosis data, and genetic data — but doesn't specify *how*. They say they can share and sell consumers' "preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" to data brokers, law enforcement, and other third parties.

Other top offenders include **Volkswagen**, which collects demographic data (like age and gender) and driving behaviors (like your seatbelt and braking habits) for targeted marketing purposes; **Toyota**, which features a near-incomprehensible galaxy of 12 privacy policy documents; **Kia**, whose privacy policy states they can collect information about your "sex life;" and **Mercedes-Benz**, which manufactures certain models with TikTok (which has its own privacy issues) pre-installed. Analysts [estimate](#) that by 2030, car data monetization could be an industry worth \$750 billion.

Not a single brand received Mozilla's Best Of designation, though researchers identified **Renault** as the least problematic. The European brand must comply with General Data Protection Regulation (GDPR), a stringent law governing the way in which personal data is used, processed, and stored.

**Says Jen Caltrider, \*PNI Program Director:** "Many people think of their car as a private space — somewhere to call your doctor, have a personal conversation with your kid on the way to school, cry your eyes out over a break-up, or drive places you might not want the world to know about. But that perception no longer matches reality. All new cars today are privacy nightmares on wheels that collect huge amounts of personal information."

**Says Misha Rykov, \*PNI Researcher:** "This isn't the first time Mozilla has uncovered an industry with terrible privacy practices. But cars are unique — their privacy flaws impact not just the driver, but also passengers and sometimes even nearby pedestrians. They can hear you, see you, and track you. Today, sitting in someone's car is a lot like handing your phone over to the auto manufacturer."

**Additional key findings include:**

- **Apps add a new level of complexity (and creepiness).** These days, few products come without an associated app — and autos are no exception. Today's cars have apps that can be handy, helping you find your ride in a crowded parking lot or start your car remotely. But these apps are also an avenue for collecting even more personal data. Further, the governance of these apps can be convoluted: **BMW** USA, for example, manages an app for **Toyota**.
- **Many car brands engage in "privacy washing."** Privacy washing is the act of pretending to protect consumers' privacy while not actually doing so — and many brands are guilty of this. For example, several have signed on to the automotive [Consumer Privacy Protection Principles](#). But these principles are nonbinding and *created by the automakers themselves*. Further, signatories don't even follow their own principles, like Data Minimization (i.e. collecting only the data that is needed).
- **Meaningful consent is nonexistent.** Often, "consent" to collect personal data is presumed by simply being a passenger in the car. For example, **Subaru** states that by being a passenger, you are considered a user — and by being a user, you have consented to their privacy policy. Several car brands also note that it is a driver's responsibility to tell passengers about the vehicle's privacy policies.
- **Autos' privacy policies and processes are especially bad.** Legible privacy policies are uncommon, but they're exceptionally rare in the automotive industry. Brands like **Audi** and **Tesla** feature policies that are confusing, lengthy, and vague. Some brands have more than five different privacy policy documents, an unreasonable number for consumers to engage with; **Toyota** has 12. Meanwhile, it's difficult to find a contact with whom to discuss privacy concerns. Indeed, 12 companies representing 20 car brands didn't even respond to emails from Mozilla researchers.

- **Car brands share personal information with law enforcement and governments.** **Hyundai's** privacy policy says, for example, that they can share data with law enforcement and governments based on "formal or informal" requests. **Kia's** policy says they may share data in many scenarios "if, in our good faith opinion, such is required or permitted by law." In other words: The threshold for sharing incredibly sensitive information is *very* low.
- **Data breaches are common.** Serious data leaks and breaches are ordinary in the industry, from **Tesla** employees gawking at videos captured by consumers' cars, to **Volkswagen** and **Toyota** leaking the personal information of millions of customers.
- **Consumers have very little control.** While consumers can choose to not use a car app or try not to use connected services, that might mean their car doesn't work properly — or at all. Consumers have almost zero control and options in regard to privacy, other than simply buying an older model. Regulators and policy makers are behind on this front.

***About \*Privacy Not Included***

*[\\*Privacy Not Included](#) is a buyers guide focused on privacy rather than price or performance. Launched in 2017, the guide has reviewed hundreds of products and apps. It arms shoppers with the information they need to protect the privacy of their friends and family, while also spurring the tech industry to do more to safeguard consumers.*

###