

It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy



By Jen Caltrider, Misha Rykov and Zoë MacDonald | Sept. 6, 2023

Ah, the wind in your hair, the open road ahead, and not a care in the world... except all the trackers, cameras, microphones, and sensors capturing your every move. *Ugh.* Modern cars are a **privacy nightmare**.

Car makers have been bragging about their cars being "computers on wheels" for **years** to promote their advanced features. However, the conversation about what driving a computer means for its occupants' privacy hasn't really caught up. While we worried that our doorbells and watches that connect to the internet might be spying on us, car brands quietly entered the data business by turning their vehicles into powerful data-gobbling machines. Machines that, because of all those brag-worthy bells and whistles, have an unmatched power to watch, listen, and collect information about what you do and where you go in your car.

All 25 car brands we researched earned our *Privacy Not Included warning label -- making cars the official worst category of products for privacy that we have ever reviewed.

[Read the reviews](#)

The car brands we researched are terrible at privacy and security

Why are cars we researched so bad at privacy? And how did they fall so far below our standards? Let us count the ways!

1. They collect too much personal data (all of them)

We reviewed 25 car brands in our research and we handed out 25 "dings" for how those companies collect and use data and personal information. That's right: **every car brand** we looked at collects more personal data than necessary and uses that information for a reason other than to operate your vehicle and manage their relationship with you. For context, 63% of the mental health apps (another product category that **stinks at privacy**) we reviewed this year received this "ding."

And car companies have so many more data-collecting opportunities than other products and apps we use -- more than even smart devices in our homes or the cell phones we take wherever we go. They can collect personal information from how you interact with **your car**, the **connected services** you use in your car, the car's **app** (which provides a gateway to information on **your phone**), and can gather even more information about you from **third party sources** like Sirius XM or Google Maps. It's a mess. The ways that car companies collect and share your data are so vast and complicated that we wrote an entire piece on **how that works**. The gist is: they can collect super intimate information about you -- from your medical information, your genetic information, to your "sex life" (seriously), to how fast you drive, where you drive, and what songs you play in your car -- in huge quantities. They then use it to invent more data about you through "inferences" about things like your intelligence, abilities, and interests.

2. Most (84%) share or sell your data

It's bad enough for the behemoth corporations that own the car brands to have all that personal information in their possession, to use for their own research, marketing, or the ultra-vague "business purposes." But then, most (84%) of the car brands we researched say they can **share** your personal data -- with service providers, data brokers, and other businesses **we know little or nothing about**. Worse, nineteen (76%) say they can **sell** your personal data.

A surprising number (56%) also say they can share your information with the **government or law enforcement** in response to a "request." Not a high bar court order, but something as easy as an "informal request." Yikes -- that's a very low bar! A 2023 rewrite of *Thelma & Louise* would have the ladies in custody before you've had a chance to make a dent in your popcorn. But seriously, car companies' willingness to share your data is beyond creepy. It has the potential to cause real harm and inspired our

worst cars-and-privacy nightmares.

And keep in mind that we only know what companies do with personal data because of the privacy laws that make it illegal not to disclose that information (go California Consumer Privacy Act!). So-called anonymized and aggregated data can (and probably is) shared too, with vehicle data hubs (the data brokers of the auto industry) and others. So while you are getting from A to B, you're also funding your car's thriving side-hustle in the data business in more ways than one.

3. Most (92%) give drivers little to no control over their personal data

All but two of the 25 car brands we reviewed earned our “ding” for data control, meaning only two car brands, Renault and Dacia (which are owned by the same parent company) say that all drivers have the right to have their personal data deleted. We would like to think this deviation is one car company taking a stand for drivers’ privacy. It’s probably no coincidence though that these cars are only available in Europe -- which is protected by the robust General Data Protection Regulation (GDPR) privacy law. In other words: car brands often do whatever they can legally get away with to your personal data.

4. We couldn’t confirm whether any of them meet our Minimum Security Standards

It’s so strange to us that dating apps and sex toys publish more detailed security information than cars. Even though the car brands we researched each had several long-winded privacy policies (Toyota wins with 12), we couldn’t find confirmation that **any** of the brands **meet** our Minimum Security Standards.

Our main concern is that we can’t tell whether any of the cars encrypt all of the personal information that sits on the car. And that’s the bare minimum! We don’t call them our state-of-the-art security standards, after all. We reached out (as we always do) by email to ask for clarity but most of the car companies completely ignored us. Those who at least responded (Mercedes-Benz, Honda, and technically Ford) still didn’t completely answer our basic security questions.

A failure to properly address cybersecurity might explain their frankly embarrassing security and privacy track records. We only looked at the last three years, but still found plenty to go on with 17 (68%) of the car brands earning the “bad track record” ding for leaks, hacks, and breaches that threatened their drivers’ privacy.

At a glance: How the car brands stack up

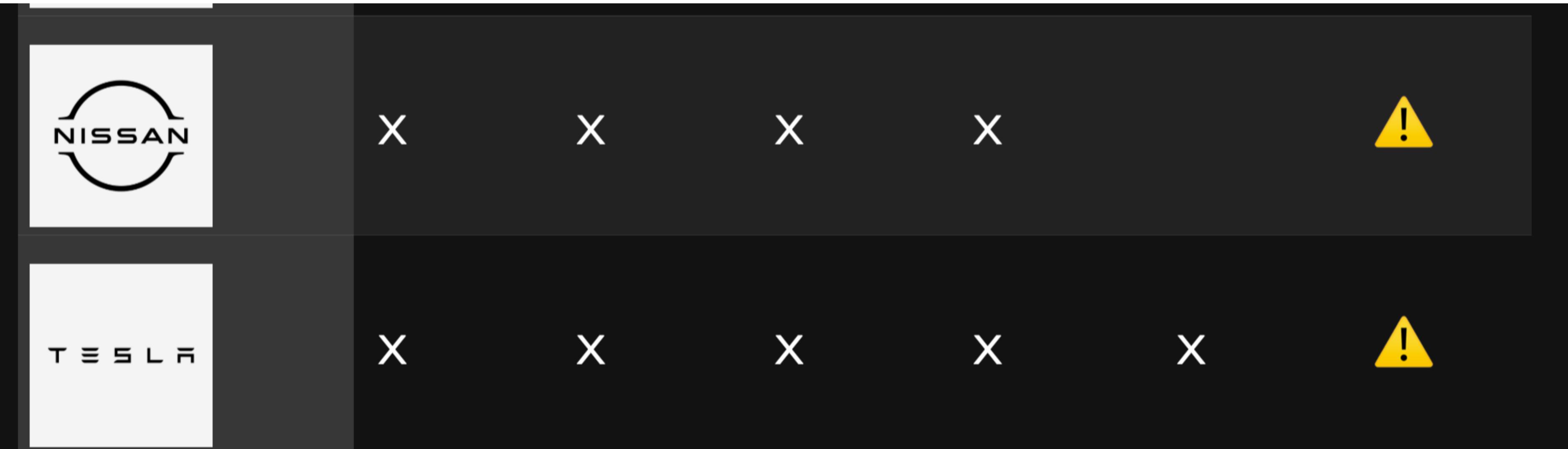
Here’s how the cars performed against our privacy and security criteria.

All the car brands we reviewed, ranked from bad to worst for your privacy

Car brand	Data use	Data control	Track record	Security	AI	Review
	X		X			!
	X		X			!
	X	X	X			!

	X	X	X	X	
	X	X	X	X	
Jeep	X	X	X	X	
	X	X	X	X	
	X	X	X	X	
	X	X	X	X	
	X	X	X	X	
	X	X	X	X	
	X	X	X	X	
	X	X	X	X	

	X	X	X	X	
 Mercedes-Benz	X	X	X	X	
 HONDA	X	X	X	X	
 ACURA	X	X	X	X	
 KIA	X	X	X	X	
 CHEVROLET	X	X	X	X	
 BUICK	X	X	X	X	
 GMC	X	X	X	X	
 CADILLAC	X	X	X	X	
 HYUNDAI	X	X	X	X	



Source: *Privacy Not Included

moz://a

Some not-so-fun facts about these rankings:

- Tesla is only the second product we have ever reviewed to receive all of our privacy “dings.” (The first was an AI chatbot we reviewed earlier this year.) What set them apart was earning the “**untrustworthy AI**” ding. The brand’s AI-powered autopilot was reportedly involved in 17 deaths and 736 crashes and is currently the subject of multiple government investigations.
- Nissan earned its second-to-last spot for collecting some of the **creepiest categories** of data we have ever seen. It’s worth reading the review in full, but you should know it includes your “**sexual activity**.” Not to be outdone, Kia also mentions they can collect information about your “**sex life**” in their privacy policy. Oh, and six car companies say they can collect your “**genetic information**” or “genetic characteristics.” Yes, reading car privacy policies is a scary endeavor.
- None of the car brands use language that meets Mozilla’s **privacy standard** about sharing information with the government or law enforcement, but **Hyundai** goes above and beyond. In their privacy policy, it says they will comply with “**lawful requests, whether formal or informal**.” That’s a serious red flag.
- All of the car brands on this list except for Tesla, Renault, and Dacia signed on to a list of **Consumer Protection Principles** from the US automotive industry group **ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.** The list includes great privacy-preserving principles such as “**data minimization**,” “**transparency**,” and “**choice**.” But the number of car brands that follow these principles? Zero. It’s interesting if only because it means the car companies do clearly **know what they should be doing to respect your privacy** even though they absolutely don’t do it.

What can you do about it? Well...

This is usually where we’d encourage you to **read our reviews**, and to choose the products you can trust when you can. But, cars aren’t really like that.

Sure, there are some steps you can take to protect more of your privacy, and we’ve listed them all in each of our **reviews** under “**Tips to protect yourself**.” They’re definitely worth doing. You can also avoid using your car’s app or limit its permissions on your phone. (Since many of the apps share a privacy policy with the vehicle, we can’t always tell which data is taken from your phone so it’s probably better to err on the side of caution by not using it.) But compared to all the data collection you can’t control, these steps feel like tiny drops in a massive bucket. Plus, you deserve to benefit from all the features you pay for without also having to give up your privacy.

The **lack of choice** has really been among the biggest bummers in reading up on cars and privacy. Consumers’ choices are limited in so many ways with cars, because:

They’re all bad

People don’t comparison-shop for cars based on privacy. And they shouldn’t be expected to. That’s because there are so many other limiting factors for car buyers. Like cost, fuel efficiency, availability, reliability, and the features you need. Even if you did have the funds and the resources to comparison shop for your car based on privacy, you wouldn’t find much of a difference. Because according to our research, they are all bad! On top of all that, researching cars and privacy was one of the hardest undertakings we as privacy researchers have ever had. Sorting through the large and confusing ecosystem of privacy policies for cars, car apps, car connected services, and more isn’t something most people have the time or experience to do.

Like we mentioned, ***all of the cars we researched earned our *Privacy Not Included warning label.*** All of the car brands we researched got our “data use” and “security” dings -- and most earned dings for poor data control and bad track records too! We can’t stress enough how bad and not normal this is for an entire product guide to earn warning labels.

It's so confusing

We spent over **600 hours** researching the car brands’ privacy practices. That’s three times as much time per product than we normally do. Even still, we were left with so many questions. None of the privacy policies promise a full picture of how your data is used and shared. If three privacy researchers can barely get to the bottom of what’s going on with cars, how does the average time-pressed person stand a chance?

But wait, there's more!

"Consent" is an illusion

Many people have lifestyles that require driving. So unlike a smart faucet or voice assistant, you don’t have the same freedom to opt out of the whole thing and not drive a car. We’ve talked before about the murky ways that companies can manipulate your consent. And car companies are no exception. Often, they ignore your consent. Sometimes, they assume it. Car companies do that by *assuming* that you have read and agreed to their policies before you step foot in their cars. Subaru’s privacy policy says that even passengers of a car that uses connected services have “consented” to allow them to use -- and maybe even sell -- their personal information just by being inside.

So when car companies say they have your “consent” or won’t do something “without your consent,” it often doesn’t mean what it should. Like when Tesla says, that sure! You can opt out of data collection, but it might break your car:

“ ”

However, **“if you no longer wish for us to collect vehicle data or any other data from your Tesla vehicle, please contact us to deactivate connectivity. Please note, certain advanced features such as over-the-air updates, remote services, and interactivity with mobile applications and in-car features such as location search, Internet radio, voice commands, and web browser functionality rely on such connectivity. If you choose to opt out of vehicle data collection (with the exception of in-car Data Sharing preferences), we will not be able to know or notify you of issues applicable to your vehicle in real time. This may result in your vehicle suffering from reduced functionality, serious damage, or inoperability.”**

TESLA'S CUSTOMER PRIVACY NOTICE

<https://www.tesla.com/legal/privacy>

A few of the car companies we researched take manipulating your consent one step further by making you complicit in getting “consent” from others, saying it’s *on you* to inform them of your car’s privacy policies. Like when Nissan makes you **“promise to educate and inform all users and occupants of your Vehicle about the Services and System features and limitations, the terms of the Agreement, including terms concerning data collection and use and privacy, and the Nissan Privacy Policy.”** OK, Nissan! We would love to meet the social butterfly who drafted this line.

Don't worry!! There is something you can do!

Hey woah don’t hang up your driving gloves just yet! We’re not saying the situation is hopeless. What we are saying is that it’s not fair for the burden to be on consumers to make “better choices” that in this case don’t exist. And we don’t want to take a page from car companies’ books by asking you to do things no reasonable person would ever do -- like reciting a 9,461-word privacy policy to everyone who opens your car’s doors.

You’re already helping us to spread the word just by reading our research. Our hope is that increasing awareness will encourage others to hold car companies accountable for their terrible privacy practices too. But that’s not all. **You can join our global movement for privacy rights for everyone, everywhere.**



Jen Caltrider

During a rather unplanned stint working on my Master’s degree in Artificial Intelligence, I quickly discovered I’m much better at telling stories than writing code. This discovery led to an interesting career as a journalist covering technology at CNN. My true passion in life has always

been to leave the world a little better than I found it. Which is why I created and lead Mozilla's *Privacy Not Included work to fight for better privacy for us all.



Misha Rykov

Kyiv-native and Berlin-based, Misha worked in big tech and security consulting, before joining Mozilla's privacy effort. Misha loves investigative storytelling and hates messy privacy policies. Misha is an advocate for stronger and smarter privacy regulations, as well as for safer Internet.



Zoë MacDonald

Zoë is a writer and digital strategist based in Toronto, Canada. Before her passion for digital rights led her to Mozilla and *Privacy Not Included, she wrote about cybersecurity and e-commerce. When she's not being a privacy nerd at work, she's side-eyeing smart devices at home.