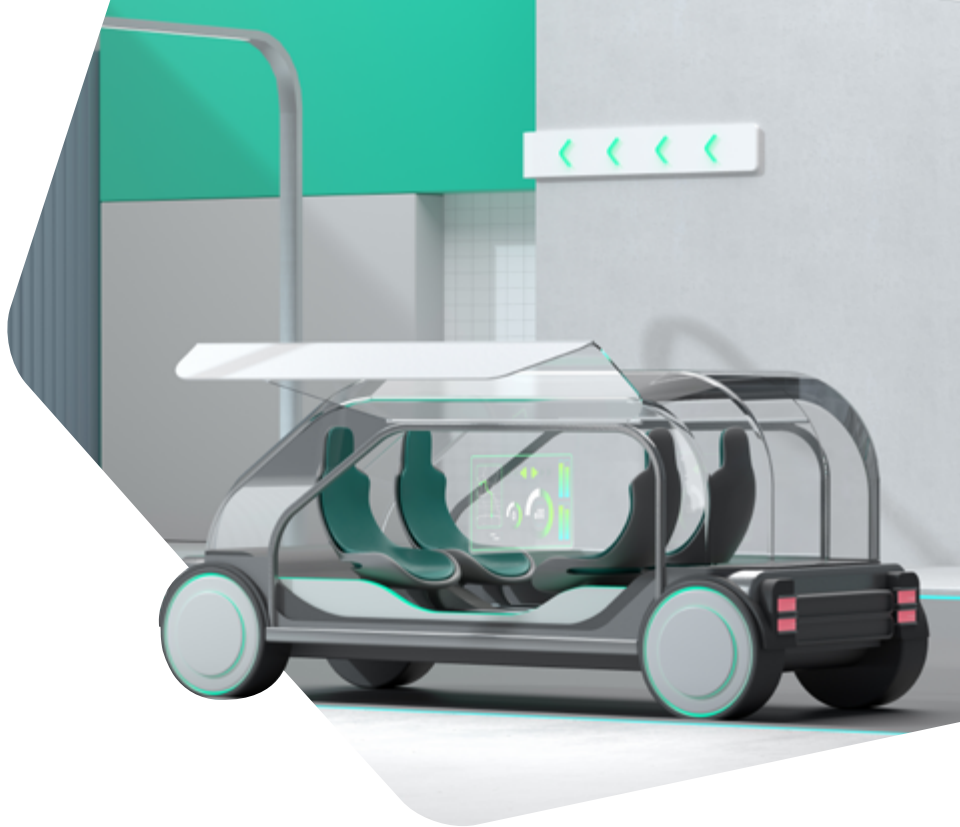


Is my car spying on me?



Modern cars come loaded with technology, including sensors, GPS, apps, infotainment systems, cameras and microphones. All of this can be used to remotely diagnose problems, call for help in an emergency, or enable or disable car functions through subscriptions. It can also produce valuable data to be sold to insurance companies and marketers. Cars often connect with drivers' smart phones, opening another avenue to personal data collection. This even can allow them to collect information such as where you go, how long you stay, who travels with you and whether or not you wear a seatbelt.

All of this naturally raises privacy concerns. A recent [Mozilla study](#) sounded an alarm, calling cars the “worst product category ever reviewed for privacy,” finding that many popular car brands collect “more personal data than necessary,” and that most of them say they have the right to share or sell it with other parties. The type of data they reserve the right to collect can range from your travel patterns to your media consumption habits to such intimate details as your sexual preferences and even your genetic information. The study also found that zero out of 25 researched car brands met the criteria for Mozilla's Minimum Security Standards.

Security is a concern on multiple levels. Successful attacks on vehicles have demonstrated that adversaries can use a wide arsenal of tools to penetrate vehicle systems, and that a successful attack may result in the theft of personal data, installation of malicious code, manipulations of functions or the theft of the vehicle.

Previous research has revealed potential shortcomings in terms of the way data is stored and secured by auto manufacturers. Kaspersky's [Automotive Threat Intelligence report](#) found that senior automotive executives have major concerns about the potential for cybercriminals to exploit vulnerabilities in software related to the production of connected cars. Sixty-four percent of C-Suite executives said they believe the automotive supply chain is currently vulnerable to cyberattack.

With all of this in mind, Kaspersky set out to find out what drivers think about the potential collection of their personal data by their car, a machine that lends, for many, a sense of personal sanctuary.

Methodology

In November, 2023, Kaspersky surveyed 2,000 American drivers about their knowledge and feelings about the potential collection of their personal data by their car manufacturer.

Key findings: drivers' thoughts on privacy

72% of drivers are **uncomfortable** with the idea of an **automaker sharing their data with third parties**, including 37% who said they are “very uncomfortable.” These figures were consistent across age groups. The reality appears to be that most automakers are indeed sharing data, with 84% of the car brands in Mozilla’s analysis reserving the right to share your personal data with third parties, such as service providers and data brokers, with 56% even saying they can share your information with the government or law enforcement upon request.

87% of survey participants said **automakers should be required to delete their data upon request**. Notably, this was one area where older drivers appeared more concerned about the issue, with 91% of respondents over the age of 55 answering “yes” to this question, compared to just 78% of respondents aged 18-24 and 81% of respondents aged 25-34 (ages 35-44: 85%; ages 45-54: 90%).

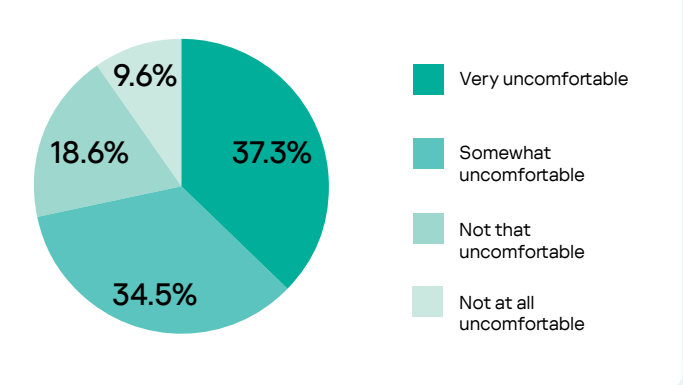
Getting data deleted is easier said than done in the U.S., where the right to be forgotten is not legally recognized, as it is in Europe, under the General Data Protection Regulation (GDPR). Drivers in five states – California, Colorado, Connecticut, Utah and Virginia – do at least have data privacy laws that afford some level of right to request to delete or opt out of the sale of personal information.

Only 28% say they have some idea what kind of data their automaker collects. This figure was, by far, the highest among younger drivers, at 49%. It dropped significantly as the age groups went higher, dropping to 16% of drivers over age 55 saying they think they know.

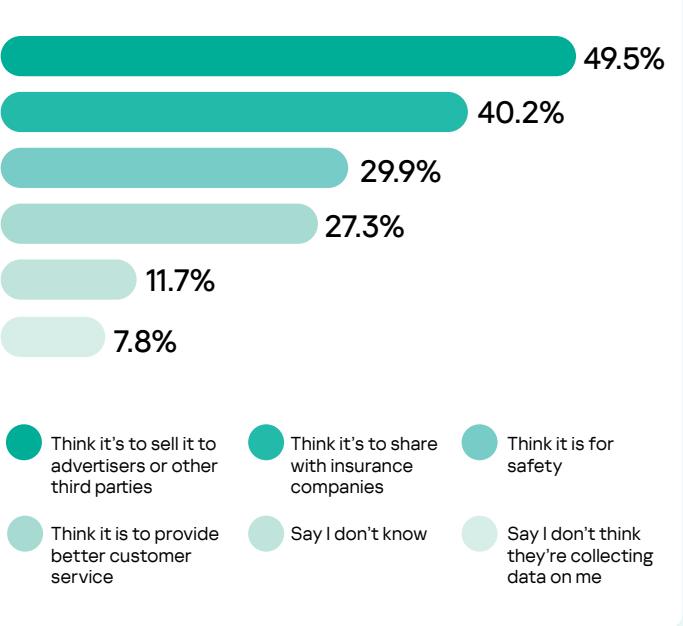
Given the amount of revealing personal information accessible via smartphones, which are very often wirelessly paired with cars, it’s difficult to know what information the car may be gaining access to. 72% of drivers who have it said they use either Apple CarPlay or Android Auto, which connect apps from a driver’s phone with their car’s onboard computer. Additionally, many cars now come with an app to install on your phone, which could theoretically then enable data collection even when you’re not in the car.

When asked why automakers might be collecting data about them (without being limited to a single answer) half (49.5%) said they think it’s to sell it to advertisers or other third parties, while 40% think it’s to share with insurance companies, 30% think it is for safety, and 27% think it is to provide better customer service. Twelve percent said they don’t know and 8% said “I don’t think they’re collecting data on me.”

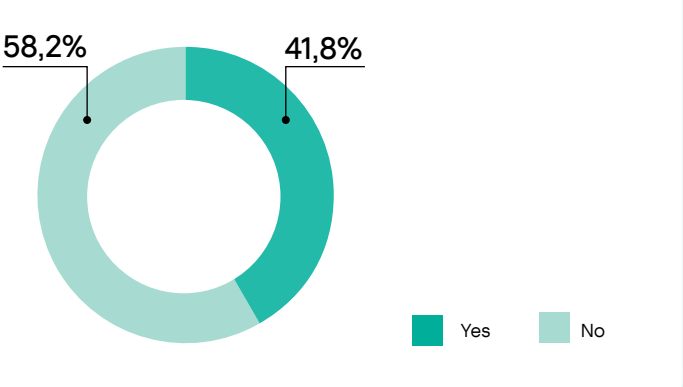
How uncomfortable are drivers with an automaker sharing their data with a 3rd party



Why drivers think their car company would collect their personal data



Are you worried about your car's tech collecting your data?

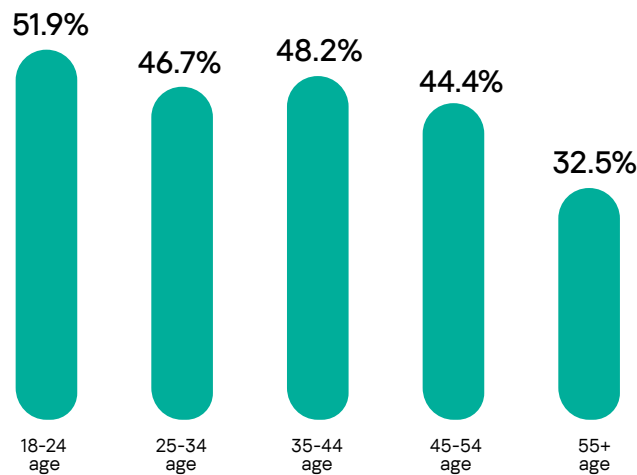


Perhaps somewhat surprisingly, most drivers said they are not concerned about their car's ability to collect data in the first place.

Only 42% of survey respondents said they are worried that their car's technology (sensors, infotainment system, cameras, microphones, and other apps and services you connect with your car), might be collecting their personal data.

However, taken together with some of the other data points revealing concern about that data being shared, this may simply reflect that drivers are realistic about their data exposure to technology in general – even willing to make some tradeoffs in exchange for convenience – while maintaining some level of expectation that their data should be treated responsibly. It's also worth noting that the levels of concern varied by age group, and were nearly 20% higher among younger drivers.

Percentage of drivers worried that car tech may be collecting their personal data, by age.

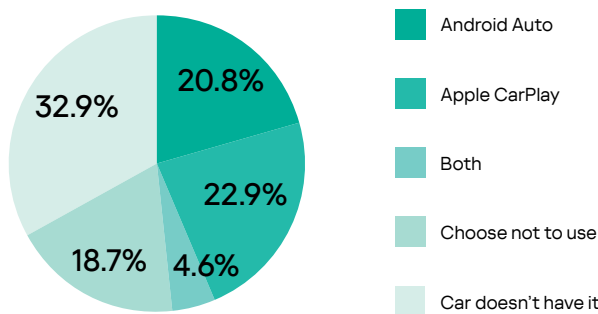


What drivers are doing

Most drivers appear to be wirelessly pairing their phone with their car. Only 20% of respondents said they don't pair their phone with their car via Bluetooth. Only 33% of respondents said their car doesn't have Android Auto or Apple CarPlay, while 19% said they car has the capability but they don't use it.

Perhaps somewhat predictably, use of Android Auto and Apple CarPlay was much higher among younger drivers, with 69% of drivers 18-24 saying they use one of those features, while that figure dropped to 46% among drivers ages 45-54 and to just 30% among respondents ages 55 and up.

What drivers use in their cars



Privacy experts have suggested limiting the information your phone shares with your car by disabling Apple's CarPlay and Android Auto pairing functions, as well as preventing it from sharing your address book when paired via Bluetooth. Sharing your address book may make it easier to quickly dial friends and family from behind the wheel, but it also turns over valuable, private information without any knowing what it might be used for. 42% of survey respondents who use Bluetooth said they avoid sharing their address book. Older drivers were much

less inclined to limit information shared with their car via Bluetooth, with only 20% aged 55+ saying they do so, compared to 49% of those aged 18-24, and figures ranging from 31% to 47% for the age groups in between.

71% of drivers said they would consider **buying an older car or one with less technology**, in order to protect their privacy and security. Those respondents broke down as follows: 32% said they would consider an older car, 22% said they would consider one with less technology, 18% said "both," while 29% said they wouldn't consider these options. Notably, younger drivers were the most likely to say they would consider boosting their privacy in this way, with 81% saying they would consider buying an older car or one with less technology (compared to 65% of respondents aged 55+ and 75% among both 35-44 and 45-54 age groups). Unfortunately for the privacy-minded, both of these options are likely to get less realistic as time goes on and connected cars make up a growing share of the available inventory.



Data Security

The referenced Mozilla study found that zero out of 25 car brands it researched met its minimum security criteria. When presented with this finding, 76% of respondents to the Kaspersky survey expressed concern, with 31% saying they are significantly concerned, and 45% saying they are somewhat concerned. A leak of customer data from a major auto manufacturer could result in large troves of sensitive data finding their way to the dark web, where it can be bought and sold by scammers looking to commit financial fraud and other attacks.

Security remains a significant concern for the automakers themselves. The Kaspersky study that captured C-Suite auto executives' supply chain security concerns identified "the integration of infotainment systems and connectivity technology from software providers" as the biggest supply chain risk, with 34% of respondents listing this as their top cybersecurity concern. The report notes that infotainment systems have become a main selling point, and generally include voice control, GPS, entertainment and other connected functionality. But they also introduce a range of new vulnerabilities, particularly given their involvement of an array of third-party tech vendors. Cybercriminals have increasingly demonstrated the effective strategy of targeting vulnerable suppliers, in order to ultimately gain access to their true target, which in this case could involve major car manufacturers and their customers.

Expert Insight



Kurt Baumgartner,
principal security
researcher,
Kaspersky

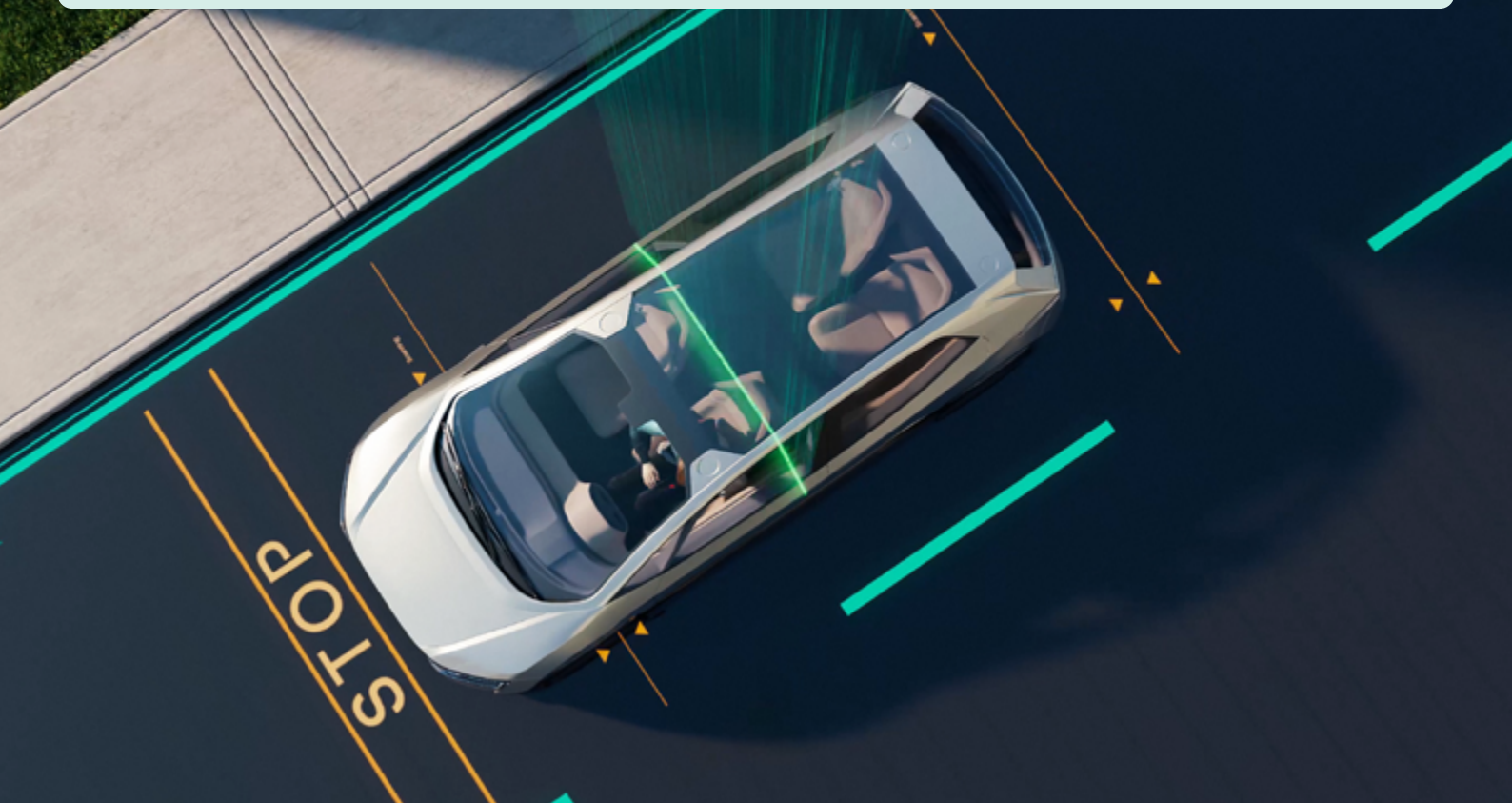
Cars are quickly becoming like so many other areas of consumer tech, where possessions that buyers thought were their property once they bought them, aren't completely under their ownership. Essentially, Americans pay thousands extra on these gadgets for surveillance technology to monitor themselves, and then have that personal data sold to arbitrary buyers. That personal data can include marital status, genetic characteristics or the speed you drive.

These survey results indicate that a lot of people wouldn't be

happy with the latitude automakers seem to be giving themselves with user data. Most people probably don't feel, for example, that their daily routines, their children's media consumption habits or information on their passengers need to be recorded by their car company and harvested as currency.

The collection of driver data creates yet another security risk for consumers, with data often being stored without sufficient protection and at risk of being leaked or stolen. The ever growing list of previous incidents, such as the Equifax, OPM and Deep Root Analytics breaches, demonstrate the risks.

Our data is highly valuable. As drivers, we need to advocate for privacy safeguards and common sense ownership agreements where we can enjoy the convenience of tech-enabled cars without giving it all up.



Conclusion

GM **recently did away** with CarPlay and Android Auto support, an apparent move to wrest back control of the user's digital experience on the road and, in turn, gain sole access to the data it produces. The company said it plans to grow its subscription business to \$25 billion within the next five years. Apple, meanwhile, is **reportedly planning** to take over just about everything on the dashboard with its next CarPlay system, from FM radio to climate control. With tech giants and automakers jockeying for a spot in the driver's seat, the consumer gets a sense of how lucrative these corporations believe driver data can be.

Given that most respondents said they don't know what kind of data their car company is collecting, and only half believe the company would sell it, drivers may not yet be widely aware of the issue. However, the survey results make fairly clear there is a limit to what consumers will put up with when it comes to their personal data, what companies might do with it, and how poorly it might be secured. In the absence of data protection regulations, they may want

to take steps to protect themselves, while checking their privacy policies and even demanding answers from the industry or action from their congressmen.

For their part, auto manufacturers are advised to carry out supply chain risk assessments and develop detailed cybersecurity plans that include real-time threat monitoring and incident response plans. More information is available in **this report**.

Drivers' habits, locations and preferences are likely becoming part of a growing, lucrative market. If legislation in this area were to respond to the kind of consumer attitudes expressed in this survey, it might wisely aim to follow the lead set by California and other states, and seek to return a level of control over personal data to the user. An automaker could also set itself apart from the competition by pledging not to collect or share personal data. In the meantime, there are some basic steps to follow to protect yourself.

Consumer tips

Don't install your car's mobile app on your phone.

Don't activate Apple's CarPlay or Android Auto pairing functions.

When you pair your phone via Bluetooth, don't allow the car to access your address book or other data.

Buy an older car or a car with a minimal set of "smart" sensors and/or no communication module.

Ask about the manufacturer's privacy policy when you purchase a new car.

Sign Mozilla's **collective petition to car manufacturers**



kaspersky.com

2023 AO Kaspersky Lab.
All rights reserved. Registered trademarks
and service marks are the property of their
respective owners.

kaspersky

Links:

Auto executives threat intelligence survey report:
<https://media.kasperskydaily.com/wp-content/uploads/sites/86/2023/09/12153626/Kaspersky-Automotive-Threat-Intelligence-FINAL.pdf>

Blog post: Mozilla reviews cars' privacy policies:
<https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>

Kaspersky blog post: How carmakers sell your data:
<https://usa.kaspersky.com/blog/spies-on-wheels-how-carmakers-sell-your-intimate-data/29089/>

For automotive industry software developers:
<https://os.kaspersky.com/solutions/kaspersky-automotive-secure-gateway/>