

United States Senate

WASHINGTON, DC 20510

April 30, 2024

The Honorable Lina M. Khan
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Chair Khan:

We write to request that the Federal Trade Commission (FTC) investigate several automobile manufacturers — Toyota, Nissan, Subaru, Volkswagen, BMW, Mazda, Mercedes-Benz, and Kia — for deceiving their customers by falsely claiming to require a warrant or court order before turning over customer location data to government agencies.

Over the past decade, the auto industry has added internet connectivity to many new cars. This internet connection is used by car companies to deliver software updates, to collect diagnostic data, and to track the movements of the vehicle. But depending on car companies' practices, these always-on data connections and the location data collected by cars and sent back to the automaker can seriously threaten Americans' privacy. Vehicle location data can be used to identify Americans who have traveled to seek an abortion in another state, attended protests, support groups for alcohol, drug, and other types of addiction, or identify those of particular faiths, as revealed through trips to places of worship.

In order to address the concerns voiced by legislators, advocates, and consumers, the auto industry adopted a voluntary set of privacy principles in 2014. The industry submitted these principles to the FTC and invited the agency to enforce them against the 19 companies that signed on. The principles were updated in 2018 and in 2022.

Since 2014, the industry pledged to require a warrant or court order before turning over vehicle location data to law enforcement agencies, except in emergencies or with customer consent. But recent investigations by our offices confirmed that only some of the car companies are honoring this commitment. Other companies revealed they turn over Americans' location data to the government with a mere subpoena, which does not require a judge's review and approval. A summary of the survey results are attached.

Our investigations found that five car companies put their customers' privacy first by requiring a warrant for location data, absent an emergency or customer consent: GM, Honda, Ford, Tesla and Stellantis. Ford's warrant policy is recent; the company adopted this higher standard after engaging with Senator Wyden's office. While less protective of customer privacy, Hyundai's policy of accepting a warrant or other court orders still meets the bar set by the industry in its voluntary privacy principles.

In contrast, Toyota, Nissan, Subaru, Volkswagen, BMW, Mazda, Mercedes-Benz, and Kia all confirmed that they will disclose location data to U.S. government agencies in response to subpoenas, which do not require a judge's approval. Volkswagen indicated that it will require a warrant for more than seven days of location data, but will disclose six days or less in response to a subpoena. These companies are not just less protective of their customers' privacy. Their policies directly contradict the public commitment the companies made and invited the FTC to enforce. As such, these companies may have engaged in deceptive conduct, which is prohibited by Section 5 of the FTC Act.

The significant differences in privacy protection by the different automakers are a result of the current state of federal privacy law. Congress has failed to act to protect Americans' privacy, and the Supreme Court has yet to issue clear guidance on whether the Fourth Amendment applies to all government surveillance of Americans' location data. While the Supreme Court's 2018 Carpenter decision confirmed that the Fourth Amendment applies to some location data, the Court declined to issue a clear, across-the-board warrant requirement, for example, when the government seeks data for a one-week period or less.

Government agencies must already obtain a warrant to demand the contents of Americans' emails, their private photos backed up to the cloud, and to search their phone. Location data is equally sensitive and deserving of the same strong protections. And warrant policies do not undermine public safety, because companies are permitted under longstanding federal law to turn over data immediately, in emergencies, without a court order.

The companies' practices related to data collection and retention also vary in ways that significantly impact user privacy. For example, Tesla indicated that currently it only receives location data when there is "a critical safety event (such as a collision, an airbag deployment, or automatic emergency braking event)." Likewise, Mercedes-Benz indicated that the company "does not engage in the systematic collection of historical location data from the vehicle" and only stores the most recent location where a vehicle was parked, which is deleted once that vehicle is parked at a new location. In contrast, Hyundai indicated that the company routinely collects and retains vehicle location data for up to 15 years, Toyota for up to 10 years, and Honda for up to 7 years. Not receiving or storing location data in the first place is by far the most important action that companies can take to protect their customers' privacy. Such practices not only ensure that automakers cannot be forced to violate their customers' privacy; they also reduce the potential harm when hackers or foreign spies steal a company's data.

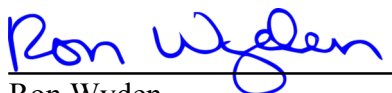
Finally, the auto manufacturers also differ significantly on the important issue of whether customers are ever told they were spied on. Of the auto manufacturers that responded to Senator Wyden's office, only Tesla currently has a policy of telling customers about legal demands, unless the company has received a judicial gag order. The other car companies do not tell their customers about government demands for their data, even if they are allowed to do so. Government surveillance notice policies are an important privacy best practice followed by many technology companies. While individuals who are prosecuted will typically be told by the

government how it obtained the evidence against them, individuals who are swept up in government dragnets and are never charged may never learn about such surveillance. Notice provided by tech companies has also played an important role in revealing government surveillance abuses, including investigations seeking to identify journalists' sources.

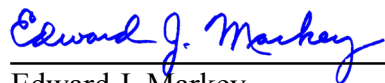
Our investigations into the privacy practices of the major auto manufacturers identified significant differences among automakers that can impact Americans' privacy, liberty, and safety. But consumers can only vote with their wallets when companies — or regulators — make such important product information available to the public. In this case, automakers have not only kept consumers in the dark regarding their actual practices, but multiple companies misled consumers for over a decade by failing to honor the industry's own voluntary privacy principles. Given the Federal Trade Commission's recent work to crack down on companies' misleading use of location data, we urge the FTC to investigate these auto manufacturers' deceptive claims as well as their harmful data retention practices. Moreover, given the brazenness of the automakers' deception, in addition to taking appropriate action against the companies, we also urge you to consider holding these companies' senior executives accountable for their actions.

Thank you for your attention to this important matter.

Sincerely,



Ron Wyden
United States Senator



Edward J. Markey
United States Senator

Automaker Policies Related to Government Demands for Customer Location Data

	Who requires a warrant?	Who tells their customers about demands for their data?
GM	YES	NO
Toyota	NO	NO
Ford	YES	NO
Hyundai	NO	NO
Stellantis	YES	NO
Honda	YES	NO
Nissan	NO	NO
Subaru	NO	NO
Volkswagen	NO	NO
Tesla	YES	YES
BMW	NO	NO
Mazda	NO	NO
Mercedes-Benz	NO	NO
Kia	NO	NO
Volvo	did not respond	did not respond