Congressional Research Service
Informing the legislative debate since 1914

# Vehicle Geolocation Data Collection: Issues for the 119th Congress

November 21, 2025

**Congressional Research Service**
https://crsreports.congress.gov
R48736

**CRS REPORT**
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48736

November 21, 2025

**Naseeb A. Souweidane**
Analyst in Transportation Policy

# Vehicle Geolocation Data Collection: Issues for the 119th Congress

Passenger and fleet vehicles collect several types of data, including geolocation data. Vehicle geolocation data support features such as navigation, emergency response services, vehicle tracking applications, personalized insurance rates, and fleet management tools. Automotive manufacturers, data brokers, insurance companies, and law enforcement are examples of entities that may access and use geolocation data for a variety of purposes.

Concerns about vehicle geolocation data collection include sensitive location tracking, data overcollection and retention, consumer awareness and consumer choice issues, data brokers' access, and data disclosure to law enforcement or other governmental entities. Vehicle geolocation data used to track a consumer's location may present risks that involve stalking, domestic violence, or threats from foreign adversaries. Consumers who choose to not share optional geolocation data may not realize that this choice may inhibit certain vehicle features. Consumers who share vehicle geolocation data may choose to do so on the basis of incomplete or misleading information in privacy policies and disclosures. Data brokers may facilitate the exchange of data to entities seeking to gain insights into marketing and analytics for commercial purposes or for activities such as monitoring traffic patterns and road conditions for public applications; these purposes could also make data accessible to bad actors. Law enforcement and other governmental entities might access geolocation data without a warrant, which may support them to identify a suspect's location while potentially presenting Fourth Amendment issues and exposing consumers to further tracking and risks.

Some stakeholders in the automotive industry voluntarily created a set of principles to regulate collection of consumer data. These principles require automotive manufacturers and suppliers to, for example, inform consumers about vehicle geolocation data being collected, obtain consent prior to data collection, and require a warrant or court order from law enforcement or other governmental entities when requesting such data. The automotive industry employs various measures to minimize risks associated with collecting geolocation data (e.g., de-identification), but data may be difficult to anonymize in some circumstances.

Several agencies share federal oversight and action related to vehicle geolocation data: the Federal Trade Commission (FTC), National Highway Traffic Safety Administration (NHTSA), Department of Commerce (DOC), Federal Communications Commission (FCC), and Department of Justice (DOJ). The FTC has several authorities related to vehicle geolocation data, including oversight of consumer disclosure practices and limiting of foreign adversaries' access to these data. NHTSA's most relevant responsibility related to vehicle geolocation data collection is its jurisdiction over motor vehicle safety. Relevant action from DOC includes a rule that bars the sale and import of certain connected vehicle technologies. The FCC has several authorities over dissemination of vehicle geolocation data and has proposed a rule that would disable connected vehicle services that may present risks for domestic-abuse survivors. The FCC also maintains a covered equipment list of technologies that pose certain security risks. DOJ has issued a rule that prevents the bulk exchange of personal data, including precise geolocation data, with foreign adversaries and other covered persons.

Congress may determine that current industry practices and self-regulation are sufficient to address privacy concerns related to vehicle geolocation data collection; in this case, Congress may take no action and defer to agencies and consider options for congressional oversight and investigation. Alternatively, Congress may seek to take action to address this issue. For example, Congress may consider comprehensive data privacy legislation (such as H.R. 8152, 117th Congress) that would limit risks associated with the collection and exchange of consumer data (e.g., by regulating data brokers or vehicles). A legislative avenue might include measures that would seek to apply data privacy laws to vehicles, limit insurance company access to geolocation data, protect survivors of domestic abuse, and limit warrantless access of geolocation data. Comprehensive data privacy legislation for vehicles (such as H.R. 10473/S. 5579, 118th Congress) could cover topics such as the access, sale, and exchange of vehicle data, including geolocation data. To limit insurance companies' access to vehicle geolocation data, Congress may choose to introduce legislation, launch investigations, hold hearings, or require research on the topic. To address risks associated with connected vehicle technologies, Congress could enact legislation (such as H.R. 2110, 119th Congress) that would allow domestic-abuse survivors to disable these technologies. Congress may evaluate options to limit warrantless access to geolocation data by law enforcement and governmental agencies either through legislation or by evaluating recent court decisions. In addition, as states have taken different approaches to regulating privacy related to vehicle geolocation data, Congress might include preemption provisions in legislation to reduce variation in approaches across states.

# Contents



## Figures



## Contacts

# Introduction

In-vehicle applications and services increasingly provide add-on functionalities and features, such as those enabling vehicle performance and health monitoring, vehicle remote access or control, navigation and traffic information, emergency response coordination, and vehicle tracking. Some applications and services may rely on data collected from the vehicle to support these add-ons. One type of data collected is vehicle geolocation data, which can be used to locate or identify the vehicle.

Vehicle geolocation data can present security and privacy risks. An example of such a risk is the exposure of a person's geolocation data to their abusive domestic partner or exposure of military personnel's data to a foreign adversary. In addition, data breaches and the sale of commercial or personal geolocation data may lead to adverse impacts for consumers, potentially leaving consumers unaware how their data are used, such as insurers raising rates.[1]

Congress has not passed comprehensive federal data privacy legislation, and no existing federal laws specifically regulate the collection, processing, and use of vehicle geolocation data. The absence of a comprehensive federal data privacy law has created a varied federal regulatory environment for consumer data, including vehicle geolocation data. Several agencies, such as the Federal Trade Commission (FTC), Department of Justice (DOJ), and Federal Communications Commission (FCC), have taken enforcement actions related to vehicle geolocation data collection. Likewise, some stakeholders within the automotive industry have voluntarily created self-regulated vehicle data privacy practices and industry standards.[2] Some Members of Congress have raised concerns about the industry's self-regulated practices of collecting, handling, and safeguarding vehicle geolocation data and have urged government agencies to assess the need for further federal regulatory action.[3]

This report provides a general overview of vehicle data collection with a focus on vehicle geolocation data. The report discusses the uses of geolocation data, concerns associated with the collection of geolocation data, practices within the automotive industry, and actions by federal agencies related to vehicle geolocation data collection. It also discusses options that Congress may consider if it chooses to address policy issues related to vehicle geolocation data.

# Vehicle Data Collection and Use

Advances in technology are transforming modern vehicles into sophisticated data hubs that can capture an extensive array of information to monitor vehicle performance and enhance driver experience and safety. Automotive manufacturers and third-party app or service providers may collect a variety of data from vehicles, including biometrics, fuel efficiency, personal

[1] Federal Trade Commission (FTC), "Cars & Consumer Data: On Unlawful Collection & Use," *Office of Technology Blog*, May 14, 2024, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use.

[2] Alliance for Automotive Innovation, *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*, November 12, 2014 (last reviewed March 2022), https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

[3] Letter from Sen. Edward J. Markey to the Hon. Lina M. Khan, FTC Chair, February 27, 2024, https://www.markey.senate.gov/imo/media/doc/senator_markey_letter_to_ftc_on_auto_privacy__022824pdf.pdf (hereinafter Sen. Markey letter to FTC Chair Khan, February 27, 2024).

communication, safety, vehicle identification, driver behavior, vehicle health, and geolocation.[4] Entities may collect vehicle data to evaluate consumer preferences, develop safety features, diagnose maintenance needs, improve communication, support market research, optimize navigation, and coordinate with emergency response.[5] For example, driver behavior data may reveal consumer preferences that can inform targeted advertisements, driver safety data aids the development of safety features, vehicle health data diagnoses maintenance needs, and geolocation data can support features such as navigation and emergency response. As vehicles become more technologically advanced and connected to other devices and the internet, the types and amounts of data collected may expand.

## Technologies That Enable Data Collection

Modern vehicles house information technologies that collect broad sets of data. These technologies include sensors, telematics control units (TCUs), electronic control units (ECUs), global positioning systems (GPS), vehicle communications networks, third-party monitoring devices (e.g., insurance plug-ins, event data recorders [EDRs], and on-board diagnostic ports [OBD-II]), dedicated short-range communications (DSRC) radio, and external imaging and scanning technologies (e.g., Light Detection and Ranging [LiDAR], radar, or cameras); (see **Figure 1**).[6] These technologies contribute to the increasingly connected nature of vehicles.

### Connected Vehicle Technologies[7]

Connected vehicle technologies, or "connectivity," enable communication between vehicles and their environment, which may include other vehicles, infrastructure, various networks, and other devices.[8] The communication enabled by connectivity requires a data exchange between the vehicle and its environment. The data exchange may enhance safety features, general performance, emergency response, entertainment, advanced driver-assistance systems, navigation, and traffic management.[9] Connectivity leads to an increased amount of data collected by vehicles.[10]

[4] U.S. Government Accountability Office (GAO), *Vehicle Data Privacy: Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role*, GAO-17-656, July 28, 2017, https://www.gao.gov/assets/gao-17-656.pdf.

[5] ITS America, *ITS America Connected Vehicle Privacy Brief: How Direct V2X Technologies Improve Safety and Efficiency While Protecting Privacy*, June 16, 2025, https://itsa.org/wp-content/uploads/2025/06/ITS-America-Connected-Vehicle-Privacy-Brief.pdf.

[6] Future of Privacy Forum (FPF), "Data and the Connected Vehicle Version 2.0" (infographic), September 16, 2024, https://fpf.org/wp-content/uploads/2024/09/FPF_connected_vehicl_v2_03_nosidebar-2.pdf (hereinafter FPF infographic, September 2024).

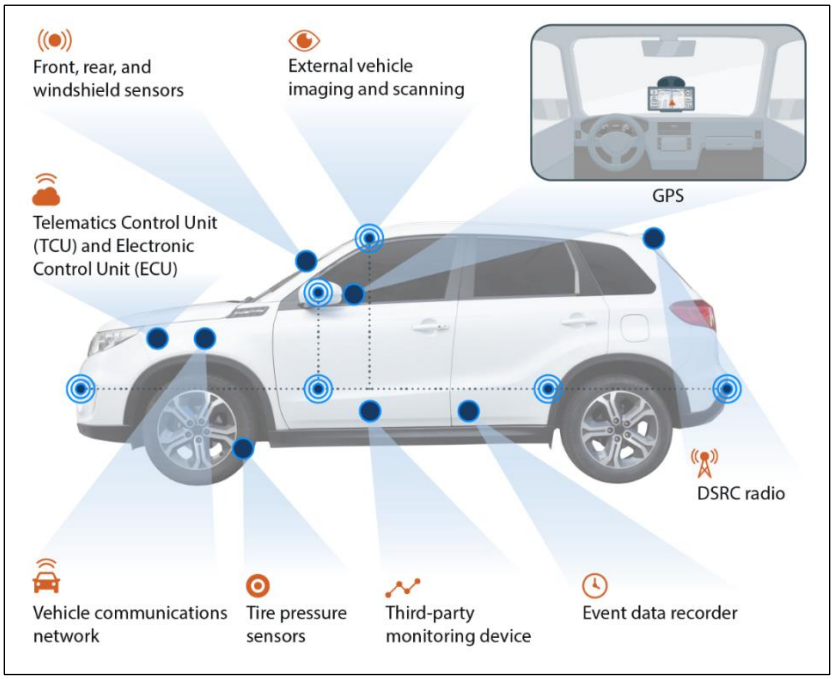
[7] The definitions of *connectivity* and *connected vehicle* vary among federal agencies but may refer to a vehicle that is connected to the internet, external servers, roadside units, or an automaker's cloud computing service.

[8] U.S. Department of Transportation (DOT), "How Connected Vehicles Work," February 27, 2020, https://www.transportation.gov/research-and-technology/how-connected-vehicles-work; and Marco De Vincenzi et al., "Security Risks and Designs in the Connected Vehicle Ecosystem: In-Vehicle and Edge Platforms," *IEEE Journal of Vehicular Technology*, vol. 6 (December 30, 2024), pp. 442-454, https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8782711.

[9] ITS America, *ITS America Connected Vehicle Privacy Brief: How Direct V2X Technologies Improve Safety and Efficiency While Protecting Privacy*.

[10] FTC, Bureau of Consumer Protection, *Connected Cars Workshop: Staff Perspective*, January 2018, https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf.

**Figure 1. Data Collection in Vehicles: Information Technologies**




**Source:** Adapted by CRS from Future of Privacy Forum, "Data and the Connected Vehicle Version 2.0" (infographic), September 16, 2024, https://fpf.org/wp-content/uploads/2024/09/FPF_connected_vehicl_v2_03_nosidebar-2.pdf.

**Notes:** DSRC = dedicated short-range communications. The presentation of technologies in this figure is illustrative.

## Geolocation Data

Geolocation data generally refers to data that enable the identification of the geographical position of a person, device, or vehicle. Such data may be mapped to further glean information about movements of a vehicle or individual. Vehicle features that rely on geolocation data include advanced driver-assistance systems (ADAS), navigation, infotainment systems, emergency response coordination services, vehicle tracking applications, personalized insurance programs, and fleet management tools.[11] These features are mainly supported by in-vehicle and smartphone applications (e.g., navigation applications, such as Waze and Google Maps, or music streaming services, such as Spotify and Apple Music), third-party monitoring devices, GPS, scanning technologies, in-vehicle TCUs, and connected vehicle technologies.[12] For example, vehicle navigation features are largely supported by GPS technologies that require the collection of

[11] AutoPi.io, "All You Need to Know About Vehicle Data (2025)," *The AutoPi Blog*, updated August 14, 2025, https://www.autopi.io/blog/the-meaning-of-vehicle-data/; Jorge Tavares et al., "Detection of Vehicle-Based Operations from Geolocation Data," *Transportation Research Procedia*, vol. 62 (March 11, 2022), pp. 341-349, https://doi.org/10.1016/j.trpro.2022.02.043; and Felix Sterk et al., "Unlocking the Value from Car Data: A Taxonomy and Archetypes," *Electronic Markets*, vol. 34 (February 13, 2024), pp. 12-24, https://link.springer.com/article/10.1007/s12525-024-00692-5 (hereinafter Sterk et al., "Unlocking the Value from Car Data").

[12] GAO, *Vehicle Data Privacy: Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role*; Jen Caltrider et al., "What Data Does My Car Collect About Me and Where Does It Go?," Mozilla Foundation, September 6, 2023, https://www.mozillafoundation.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/; and Melanie Reid, "Your Privacy on the Road: What Is Collected and How It Is Utilized," *Journal of Law and Technology at Texas*, vol. 5 (June 27, 2023), pp. 35-76, https://jolttx.com/2022/04/11/your-privacy-on-the-road-what-is-collected-and-how-it-is-utilized/ (hereinafter Reid, "Your Privacy on the Road").

geolocation data to determine the positioning of the device and the desired destination.[13] Emergency response coordination services rely on geolocation data to track vehicles and send their locations to emergency response teams.[14] OnStar, introduced in 1996,[15] is an example of a service that collects precise geolocation data to provide emergency response, roadside assistance, and navigation.[16]

Geolocation data support other use cases. In-vehicle and smartphone applications can use geolocation data to track a car's location, so a user can monitor where the vehicle is parked or where it is driven if the owner is not operating the vehicle. Geolocation data may offer consumers a customized experience by offering personalized directions based on trip history, speed, driving habits, delays in a given route, or risks associated with driving habits.[17] Third-party monitoring devices and applications installed on a user's phone may collect geolocation data to enable personalized car insurance rates by tracking location, vehicle usage, and driving habits.[18] Many of these programs are voluntary. Geolocation data are also used to improve performance of commercial fleets by optimizing routes as patterns emerge from datasets.[19] These features and use cases are becoming more commonplace, and they allow automotive manufacturers and other entities increasing access to vehicle geolocation data.

## Federal Definitions of Geolocation Data

Federal agencies have provided guidance on the meaning of terms related to geolocation data—such as geolocation information, sensitive location data, and precise location data—when regulating data collection practices. For example, the FTC defines *geolocation information* as data "sufficient to identify the street name and name of the city or town."[20] DOJ defines *precise geolocation data* as "data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters."[21] Because of its detailed nature, precise geolocation data can be considered personally identifiable information (PII) (similar to Social Security numbers or biometric data) and at points may expose sensitive locations.[22] When referencing sensitive locations, the FTC uses examples such as "medical and reproductive health clinics, places of religious worship and domestic abuse shelters."[23]

[13] GPS Technologies, "Top 5 Benefits of Using a GPS Tracker for Your Car," January 15, 2015, https://gpstechnologies.com/2025/01/top-5-benefits-of-using-a-gps-tracker-for-your-car/.

[14] OnStar, "OnStar Services and Consent," accessed September 21, 2025, https://www.onstar.com/legal/user-terms/onstar-services-consent.

[15] OnStar, "The Evolution of OnStar," accessed August 18, 2025, https://www.onstar.com/why-onstar/evolution-of-onstar-innovations.

[16] OnStar, "OnStar Services," accessed July 15, 2025, https://www.onstar.com/services.

[17] AutoPi.io, "All You Need to Know About Vehicle Data (2025)."

[18] Alison Tobin, "How Do Those Car Insurance Tracking Devices Work?," *U.S. News & World Report,* April 4, 2025, https://www.usnews.com/insurance/auto/how-do-those-car-insurance-tracking-devices-work.

[19] Sterk et al., "Unlocking the Value from Car Data."

[20] 16 C.F.R. §312.2, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.FTC.

[21] 28 C.F.R. §202.242, https://www.ecfr.gov/current/title-28/chapter-I/part-202/subpart-B/section-202.242.

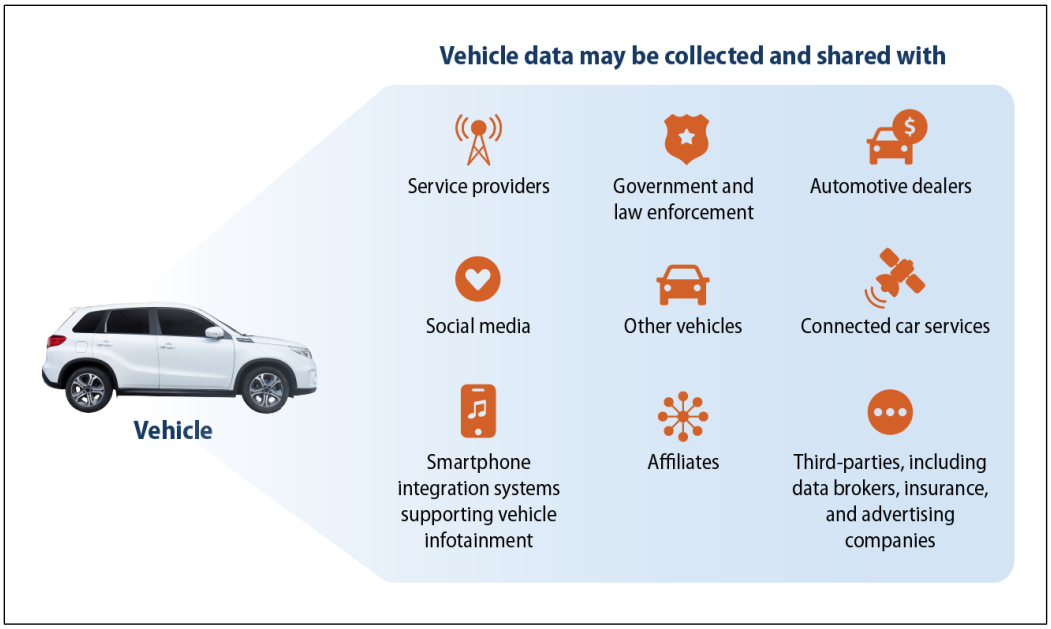
[22] The U.S. Department of Labor (DOL) defines *PII* as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." DOL, "Guidance on the Protection of Personally Identifiable Information (PII)," accessed June 25, 2025, https://www.dol.gov/general/ppii.

[23] FTC, "FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data," press release, June 8, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

## Entities That Access Vehicle Geolocation Data

The entities collecting vehicle geolocation data may do so for a variety of purposes. For example, an automotive manufacturer may collect the data to support in-vehicle technologies;[24] third-party service providers may use the data to provide vehicle support technologies;[25] data brokers may purchase the data to support market research efforts or evaluate consumer behavior;[26] insurance companies may use the data to offer personalized insurance rates for consumers;[27] and law enforcement may request access to the data to determine a suspect's precise geolocation information.[28] The aforementioned users of vehicle data and other potential users are reflected in **Figure 2**.

**Figure 2. Vehicle Data Access**




**Source:** Adapted by CRS from Jen Caltrider et al., "What Data Does My Car Collect About Me and Where Does It Go?," Mozilla Foundation, September 6, 2023, https://www.mozillafoundation.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/.

**Note:** Users included are a sample, not an exhaustive representation, of entities that collect vehicle data.

[24] FPF infographic, September 2024.

[25] Adonne Washington, *Vehicle Safety Systems: Privacy Risks and Recommendations*, FPF, March 2024, https://fpf.org/wp-content/uploads/2024/03/FPF-Vehicle-Safety-Systems_March2024.pdf.

[26] For more on data brokers, see CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Ling Zhu.

[27] Tobin, "How Do Those Car Insurance Tracking Devices Work?"; Kashmir Hill, "How Your Car Might Be Making Roads Safer," *New York Times*, December 20, 2024, https://www.nytimes.com/2024/12/20/technology/connected-cars-roads-data.html; and Kashmir Hill, "Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies," *New York Times*, March 13, 2024, https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.

[28] Letter from Sen. Ron Wyden and Sen. Edward J. Markey to the Hon. Lina M. Khan, FTC Chair, April 30, 2024, https://www.wyden.senate.gov/imo/media/doc/signed_wyden_markey_letter_to_ftc_with_attachmentpdf.pdf (hereinafter Sen. Wyden and Sen. Markey letter to FTC Chair Khan, April 30, 2024); and Reid, "Your Privacy on the Road."

# Issues Related to Vehicle Geolocation Data Collection

As discussed above, vehicle geolocation data collection often is required to enable various features, including those that improve safety and navigation. However, there are situations in which these data may present risks to consumers. This section discusses selected issues related to the vehicle geolocation data collection, including the tracking of sensitive locations, data broker access, data overcollection, consumer choice and awareness, and data disclosure to law enforcement.

## Tracking Sensitive Locations

Collection and sharing of vehicle geolocation data may create privacy and security risks for drivers, passengers, or other users of in-vehicle applications and services. For example, if geolocation data are shared, purchased, or exposed through a data breach, the affected user may be exposed to discrimination, harassment, emotional distress, or physical violence, as these data could unveil associated sensitive personal information.[29] The information could include religion, sexual orientation, health information, credit rating, or marital status.[30] Some Members of Congress and federal agencies have cited incidents in which an abuser might use sensitive location data to track a domestic-abuse survivor.[31] As another example, foreign adversaries might access sensitive location data of military and government personnel from vehicle technologies or data purchased from data brokers.[32]

### Access by Data Brokers

Data brokers collect and aggregate geolocation data from a variety of sources to gain insights into marketing and analytics for commercial purposes and public applications, such as monitoring traffic patterns and road conditions.[33] Data brokers may handle sensitive data, such as precise geolocation data, that present risks to consumers if insufficiently safeguarded. The data exchange between data brokers and other entities can create further risks for consumers depending on who

[29] FTC, "FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data." *Data breaches* are defined as "the loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data" (38 C.F.R. §75.112).

[30] Testimony of Justin Sherman in U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Who Is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy*, hearing, 118th Cong., 1st sess., April 19, 2023, H.Hrg. 118-26, https://www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Bio-ShermanJ-20230419.pdf (hereinafter Sherman, Testimony in H.Hrg. 118-26).

[31] Rep. Debbie Dingell, "Dingell, Crenshaw Introduce Bipartisan Safe Vehicle Access for Survivors Act," press release, March 17, 2025, https://debbiedingell.house.gov/news/documentsingle.aspx?DocumentID=5550; and Federal Communications Commission (FCC), "Supporting Survivors of Domestic and Sexual Violence," 89 *Federal Register* 30303, April 23, 2024, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence.

[32] Justin Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security*, Duke University, Sanford School of Public Policy, November 2023, https://techpolicy.sanford.duke.edu/wp-content/uploads/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf.

[33] Hill, "How Your Car Might Be Making Roads Safer"; and Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel*.

is able to access the data (e.g., foreign adversaries, domestic abusers, insurance companies, and other entities that could exploit the data without the knowledge or explicit consent of the targeted individual).[34]

## Overcollection and Retention of Vehicle Geolocation Data

Vehicle technologies may collect more data than necessary for them to function properly. Companies may opt to collect excess data or retain data for various reasons, such as to bolster internal marketing efforts or to sell these data to third parties as an additional means of revenue. These activities may create risks, such as exposure of sensitive data in data breaches. Some stakeholders suggest that geolocation data should be retained or exchanged only to the extent that they support the function for which the data were obtained and that measures should be taken to protect the data.[35]

## Consumer Choice and Awareness

### Consumer Choice

Consumers may have the choice to opt in or out of sharing their data (including geolocation data), but the functionality of some experience-enhancing features may depend on the extent of the data a consumer chooses to share. In some instances, a manufacturer will require the collection of geolocation data for an application to function and then use the data for secondary purposes, such as to optimize internal marketing efforts.[36] Companies can optimize marketing by personalizing advertisements to consumers based on their geolocation data.[37] If a consumer opts out of sharing geolocation data for secondary purposes, the vehicle feature may still function while minimizing the uses of their data but may be inhibited or not fully functional if a consumer opts out of allowing the vehicle to collect geolocation data altogether.[38] For example, navigation applications rely on geolocation data from a GPS device and may not be functional if a user opts out of such data collection.

### Consumer Awareness

Consumers face potential challenges when presented with privacy policies and disclosures on vehicle geolocation data collection, use, and sharing. For example, consumers might be unable to

[34] Sherman, Testimony in H.Hrg. 118-26.

[35] Trix Mulder and Nynke E. Vellinga, "Exploring Data Protection Challenges of Automated Driving," *Computer Law & Security Review*, vol. 40, no. 105530 (February 23, 2021), article 105530, https://doi.org/10.1016/j.clsr.2021.105530; and Patrick Rogers, " Leading the Charge: How Increased Adoption of Electric Vehicles Renews Calls for Data Privacy Protection in the United States," *William & Mary Environmental Law and Policy Review*, vol. 49, no. 1 (October 2024), pp. 277-297, https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1887&context=wmelpr.

[36] Anna Dowthwaite et al., "Privacy Preferences in Automotive Data Collection," *Transportation Research Interdisciplinary Perspectives*, February 13, 2024, article 101022; https://doi.org/10.1016/j.trip.2024.101022.

[37] Christian Wolgemuth, "Vehicle Location Data Creates Immense Value – Immense Implications for the Automotive and Tech Industries," *Corporate Counsel Business Journal*, August 13, 2021, https://ccbjournal.com/articles/vehicle-location-data-creates-immense-value-immense-implications-for-the-automotive-and-tech-industries/; and Merrimack College, "What Are the Benefits of Collecting Car Data?," July 12, 2019, https://online.merrimack.edu/what-are-the-benefits-of-collecting-car-data/.

[38] Alternatives to sharing data with a manufacturer's network may be available, such as by using edge computing, which allows data collection and processing in users' own devices. This option could lead to decreased performance and functionality from the technology. Mohd Fikri Azli Abdullah et al., "Edge Computing for Vehicle to Everything: A Short Review," *F1000Research* (November 10, 2023), https://f1000research.com/articles/10-1104/v4.

comprehend complex content presented in a privacy policy[39] or may not fully read a lengthy privacy policy document.[40] In addition, consumers reportedly have commented that they may not have been shown the disclosure of data practices.[41] The FTC may increase its scrutiny of automotive manufacturers if it determines their existing notice-and-consent data practices are insufficient.[42]

Another potential concern is consumers' unawareness of their geolocation data being shared with insurance companies. Geolocation data could reveal driving habits, the frequency of trips in high-crime neighborhoods, speeding, and braking patterns, depending on the granularity of the data. If consumers are unaware of these data sharing practices, they may unknowingly consent to sharing geolocation data, which could lead to insurers raising or lowering consumers' rates.

**Vehicle Geolocation Data Can Alter Insurance Rates**

The business practice of geolocation data sharing has come under FTC scrutiny. In 2024, the FTC investigated General Motors' (GM's) collection of vehicle geolocation data.[43] OnStar, a GM subsidiary, collected precise geolocation data for various vehicle services and sold the data to third parties and consumer reporting agencies.[44] Insurance companies accessed these data from consumer reporting agencies and used the data to determine insurance rates for certain consumers. Some Members of Congress urged the FTC to investigate such data sharing practices among automotive manufacturers, data brokers, and insurance companies.[45] At the conclusion of the investigation, the FTC decided that consumers were not properly informed of these data sharing practices when signing up for OnStar services.[46] In a consent order with the FTC, GM and OnStar agreed to not disclose geolocation data they collect to consumer reporting agencies for five years, in addition to other requirements.

## Disclosure of Data to Law Enforcement

Law enforcement and other governmental entities may access data provided by auto manufacturers, data brokers, and other entities through a variety of means, including warrants,

[39] Chiara Bodei et al., "Vehicle Data Collection: A Privacy Policy Analysis and Comparison," *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, vol. 1 (2023), pp. 626-633, http://dx.doi.org/10.5220/0011779500003405; and Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, November 15, 2019, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.

[40] Bodei et al., "Vehicle Data Collection: A Privacy Policy Analysis and Comparison."

[41] Kashmir Hill, "How G.M. Tricked Millions of Drivers into Being Spied On (Including Me)," *New York Times*, April 25, 2024, https://www.nytimes.com/2024/04/23/technology/general-motors-spying-driver-data-consent.html.

[42] 15 U.S.C. §45.

[43] FTC, *FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent*, January 16, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data.

[44] Hill, "How G.M. Tricked Millions of Drivers into Being Spied On (Including Me)."

[45] Letter from Sen. Edward J. Markey and Sen. Ron Wyden to the Hon. Lina S. Khan, FTC Chair, July 26, 2024, https://www.wyden.senate.gov/imo/media/doc/wyden-markey_auto_privacy_letter_to_ftc.pdf; and Sen. Markey letter to FTC Chair Khan, February 27, 2024.

[46] FTC, *In the Matter of General Motors LLC et al.*, decision and order, Docket no. 242-3052, January 16, 2025, https://www.ftc.gov/system/files/ftc_gov/pdf/242_3052_-_general_motors_decisionandorder.pdf.

subpoenas, or by purchase.[47] Such access may present Fourth Amendment issues.[48] In 2018, the U.S. Supreme Court held that, in general, governmental entities have to obtain a warrant to access certain historical geolocation data.[49] Various exceptions provided in the ruling allow law enforcement and governmental entities to purchase the information through data brokers or issue subpoenas to automotive manufacturers.[50] Geolocation data collection by law enforcement and other governmental entities may expose consumers to further tracking and risks enabled by these vehicle technologies.

# Industry Self-Regulation

Some stakeholders in the automotive industry have adopted voluntary data guidelines and practices. For example, the Alliance for Automotive Innovation, an automotive industry trade association, has published a set of principles for vehicle technologies and services to support consumer privacy protection.[51] Many members of the alliance—which includes over 40 automotive manufacturers, equipment suppliers, and technology companies—have agreed to adhere to these principles. The principles and sections relevant to geolocation data cover topics such as transparency and consumer choice; use and sharing of data in ways that are consistent with the purposes for which the data were collected, processed, and retained; data security; integrity and access; and accountability. For example, these principles generally require automotive manufacturers to provide consumers with clear information on the collection of geolocation data, obtain consent prior to collecting data in most circumstances, and require a warrant or court order from law enforcement or other governmental entities requesting this information.

## Data De-Identification Considerations

Some stakeholders in the automotive industry have adopted various measures to minimize the risks associated with geolocation data that are considered sensitive or PII. These measures include anonymizing or de-identifying the data.[52] Data anonymization or de-identification is a process to

[47] In a related context, law enforcement has sought access to geolocation data from companies such as Google and Apple through geofence warrants. For more on geofence warrants, see CRS Legal Sidebar LSB11274, *Geofence Warrants and the Fourth Amendment*, by Peter G. Berris and Clay Wild; Reid, "Your Privacy on the Road"; and Sen. Wyden and Sen. Markey letter to FTC Chair Khan, April 30, 2024 (describing inquiry from Sen. Wyden on automotive manufacturers providing detailed location information to law enforcement).

[48] For example, in a recent Fourth Amendment case, the Supreme Court examined constitutional limitations on law enforcement agencies' access of a certain subset of geolocation data (see Carpenter v. United States, 585 U.S. 296 (2018), https://www.supremecourt.gov/opinions/17pdf/585us1r62_mlho.pdf).

[49] The focus of the Supreme Court decision was on historical cell-site location information, Carpenter v. United States, 585 U.S. 296 (2018), https://www.supremecourt.gov/opinions/17pdf/585us1r62_mlho.pdf.

[50] Sen. Wyden and Sen. Markey letter to FTC Chair Khan, April 30, 2024; Noah Chauvin, "New Legislation Would Close a Fourth Amendment Loophole," Brennan Center for Justice, July 6, 2023, https://www.brennancenter.org/our-work/analysis-opinion/new-legislation-would-close-fourth-amendment-loophole; and Laura Hecht-Felella, "Federal Agencies Are Secretly Buying Consumer Data," Brennan Center for Justice, April 16, 2021, https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.

[51] Alliance for Automotive Innovation, *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*.

[52] Jim Waldo and Michael D. Smith, "Anonymity, De-Identification, and the Accuracy of Data," *Harvard Online* (blog), Harvard University, August 28, 2023, https://www.harvardonline.harvard.edu/blog/anonymity-de-identification-accuracy-data; and L. Hannah Ji-Otto et al., "Demystifying Data De-Identification for US Privacy Compliance," *Corporate Compliance Insights*, October 30, 2024, https://www.corporatecomplianceinsights.com/demystifying-data-de-identification-privacy-compliance/.

remove PII from a dataset.[53] Various mechanisms are used to de-identify geolocation data, such as replacing PII with unique numbers, aggregating geolocation data with other drivers' geolocation data, or removing all associated data.[54] Studies have found that personal information may still be identifiable from anonymized or de-identified datasets through certain measures.[55] For geolocation data specifically, an individual could be pinpointed by cross-referencing de-identified geolocation data with other data sources (e.g., timestamps of geolocation data, social media posts, IP address of the device, and known locations of nearby facilities or cell towers).[56]

# Federal Agency Authorities and Actions

Several federal agencies currently or in the future could have some regulatory authority over the use of vehicle geolocation data, including the FTC, the National Highway Traffic Safety Administration (NHTSA), the Department of Commerce (DOC), the FCC, and DOJ. Currently, the FTC can address related issues under its statutory authority to regulate unfair and deceptive interstate commercial practices.[57] The FCC has sought comment on the extent to which the Safe Connections Act (P.L. 117-223) could apply to connected car services and maintains a covered equipment list.[58] NHTSA has yet to take any regulatory action but may regulate vehicle geolocation data as they pertain to vehicle safety. DOC imposes import control regulations on connected vehicle technologies that collect sensitive data.[59] DOJ enforces regulations that prevent access to sensitive personal data by foreign adversaries.[60] The differing statutory authorities have enabled these agencies to take a variety of regulatory actions related to vehicle geolocation data collection.

[53] For example, in the context of health care, 45 C.F.R. §164.514(a) defines *de-identified information* as "health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information." Similarly, in 31 C.F.R. §800.202, the Department of Treasury defines *anonymized data* as "data from which all personal identifiers have been completely removed."

[54] GAO, *In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers*, GAO-14-81, January 6, 2014, https://www.gao.gov/products/gao-14-81. For more on data aggregation and personal identifiers, see CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Ling Zhu.

[55] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, January 2000, https://dataprivacylab.org/projects/identifiability/paper1.pdf; and Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[56] Sébastien Gambs et al., "De-Anonymization Attack on Geolocated Data," *Journal of Computer and System Sciences*, vol. 80, no. 8 (April 18, 2014), pp. 1597-1614, https://doi.org/10.1016/j.jcss.2014.04.024.

[57] 15 U.S.C. §45.

[58] P.L. 117-223.

[59] Department of Commerce (DOC), Bureau of Industry and Security (BIS), "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles," 90 *Federal Register* 5360, January 16, 2025, https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles.

[60] Department of Justice (DOJ), National Security Division, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," 90 *Federal Register* 1636, January 8, 2025, https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern.

## FTC

The FTC has several statutory authorities to regulate the collection of vehicle geolocation data, including the enforcement of consumer disclosures and the limiting of foreign adversaries' access to the data. Section 5 of the Federal Trade Commission Act (15 U.S.C. §45) provides the agency with the power to take actions against "unfair or deceptive acts or practices in or affecting [interstate] commerce." The law has empowered the agency to carry out enforcement actions against several entities, such as GM, Mobilewalla, and X-Mode, for their sale or sharing of sensitive or precise location data without consumer consent; the agency deemed such practices "unfair or deceptive" to consumers.[61] In the Protecting Americans' Data from Foreign Adversaries Act of 2024 (Division I of P.L. 118-50), Congress designated the FTC as the enforcing agency to prohibit data brokers from selling or transferring personally identifiable sensitive data of U.S. individuals, including precise geolocation data, to foreign adversaries or an entity controlled by a foreign adversary (which may include China, North Korea, Russia, and Iran). As of November 2025, the FTC has not taken action against any companies for violating Division I of P.L. 118-50.

## NHTSA

NHTSA is the federal agency responsible for motor vehicle safety, highway safety, behavioral safety programs, motor vehicle information, and automobile fuel economy programs.[62] NHTSA collects geolocation data for several programs, including the Crash Reporting Sampling System (CRSS) and the Fatality Analysis Reporting System (FARS).[63] The data are not reported directly from the vehicle but come from states and police reports that may not always provide a vehicle's representative location.[64] The ability to harness vehicle geolocation data for crash reporting could enhance CRSS and FARS, which are often used to identify and prioritize roadway safety projects, some of which receive federal funding. NHTSA's regulation and oversight of geolocation data is limited, but the agency has issued guidance documents, such as its 2022 nonbinding and voluntary guidance, "Cybersecurity Best Practices for the Safety of Modern Vehicles."[65]

## DOC

DOC has been involved in regulatory actions that impact the collection of geolocation data. In the first Trump Administration, Executive Order 13873 "imposed a prohibition on transactions

[61] FTC, "FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data"; FTC, "FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data," press release, December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data; and FTC, "FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent," press release, January 16, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data.

[62] Department of Transportation (DOT), National Highway Traffic Safety Administration (NHTSA), "Laws and Regulations," accessed July 17, 2025, https://www.nhtsa.gov/laws-regulations; 49 U.S.C. Chapters 301, 303, 321, 323, 325, 327, 329, and 331.

[63] DOT, NHTSA, "Crash Data Systems," accessed June 4, 2025, https://www.nhtsa.gov/data/crash-data-systems; and DOT, NHTSA, *Distracted Driving in 2023*, April 2025, https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813703.

[64] DOT, NHTSA, "Crash Report Sampling System (CRSS)," 2014, https://highways.dot.gov/safety/data-analysis-tools/rsdp/rsdp-tools/crash-report-sampling-system-crss; and DOT, NHTSA, "Fatality Analysis Reporting System," accessed September 22, 2025, https://www.nhtsa.gov/crash-data-systems/fatality-analysis-reporting-system.

[65] DOT, NHTSA, "Cybersecurity Best Practices for the Safety of Modern Vehicles," 57 *Federal Register* 55459, September 9, 2022.

determined by the Secretary [of Commerce], in consultation with relevant agency heads, to involve foreign adversary [information and communications technology and services] and to pose certain risks to U.S. national security, technology, or critical infrastructure," as described by DOC.[66] Under this authority, DOC's Bureau of Industry and Security (BIS) issued a final rule, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicle," on January 16, 2025.[67] The rule barred the sale and import of certain connected vehicle technologies that "present an undue and unacceptable risk to national security when designed, developed, manufactured, or supplied by persons with a sufficient nexus to the [People's Republic of China] or Russia."[68] The risks identified by the BIS include collection of sensitive information and geolocation data by such connected vehicle technologies.

## FCC

The FCC has considered its potential role in connected vehicle technologies and their associated equipment. Through the Safe Connection Act of 2022 (P.L. 117-223), Congress directed the FCC to carry out rulemaking that would allow a "survivor of domestic abuse to separate a mobile phone line from an account shared with an abuser." The FCC finalized its rule on December 5, 2023.[69] In April 2024, the FCC sought comment on additional actions it could take to protect survivors of domestic abuse who use connected cars.[70]

Additionally, per the Secure and Trusted Communications Networks Act of 2019 (P.L. 116-124), the FCC maintains a list of covered equipment that poses "an unacceptable risk to the national security of the United States or the security and safety of United States persons"[71] and prohibits the use of certain FCC funds for this equipment.[72] A consequence of equipment being placed on the FCC's covered list, per the Secure Equipment Act of 2021 (P.L. 117-55), is that the agency

[66] DOC, "Securing the Information and Communications Technology and Services Supply Chain," 89 *Federal Register* 96872, December 6, 2024, https://www.federalregister.gov/documents/2024/12/06/2024-28335/securing-the-information-and-communications-technology-and-services-supply-chain (discussing Executive Order 13873 of May 15, 2019, "Securing the Information and Communications Technology and Services Supply Chain," 84 *Federal Register* 22689, May 17, 2019). For more on the information and communications technology and services (ICTS) rule, see CRS In Focus IF11760, *The Information and Communications Technology and Services (ICTS) Rule and Review Process*, by Steve P. Mulligan.

[67] DOC, BIS, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles," 90 *Federal Register* 5360.

[68] DOC, BIS, "Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats," press release, January 14, 2025, https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats.

[69] FCC, "Supporting Survivors of Domestic and Sexual Violence; Lifeline and Link Up Reform Modernization," 88 *Federal Register* 84406, December 5, 2023, https://www.federalregister.gov/documents/2023/12/05/2023-25835/supporting-survivors-of-domestic-and-sexual-violence-lifeline-and-link-up-reform-modernization.

[70] FCC, "Supporting Survivors of Domestic and Sexual Violence," 89 *Federal Register* 30303, April 23, 2024, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence. (Prior to issuing the proposed rules and in response to media reports on risks to survivors from connected car technologies, the FCC Chair sent letters to wireless service providers and auto manufacturers in January 2024. In the letters, the FCC Chair sought input on existing connected car services, treatment of geolocation data, and ways to enhance protection for domestic violence survivors. For more information, see FCC, "Chairwoman on Safe Connected Cars for Domestic Violence Survivors," January 11, 2024, https://www.fcc.gov/document/chairwoman-safe-connected-cars-domestic-violence-survivors.)

[71] FCC, "List of Equipment and Services Covered by Section 2 of The Secure Networks Act," June 23, 2025, https://www.fcc.gov/supplychain/coveredlist.

[72] For more information on the FCC's covered list, see CRS Insight IN11663, *Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions*, by Jill C. Gallagher.

can no longer authorize the use of that equipment in the United States.[73] By law, determination of equipment safety and security is made by other agencies and equipment named by Congress in Section 889 of P.L. 115-232.[74] After the January 16, 2025, BIS final rule on certain connected vehicle technologies, the FCC's Public Safety and Homeland Security Bureau and Office of Engineering and Technology sought comment on whether the FCC's covered list should be updated to include the technologies listed in the BIS rule.[75]

### DOJ

DOJ has also engaged in rulemaking that seeks to regulate certain countries' or individuals' access of sensitive personal data as required by Executive Order 14117. On January 8, 2025, DOJ issued a final rule, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons."[76] The rule "prevent[s] U.S. persons from providing countries of concern or covered persons access to government-related data or Americans' bulk U.S. sensitive personal data through commercial data-brokerage transactions."[77] Precise geolocation data is included in the definition of *sensitive personal data*.

## State Action

Nineteen states have enacted varied comprehensive data privacy laws that regulate the use of geolocation data; this has led to differing regulatory environments across states.[78] For example, California enacted the California Consumer Privacy Act to address wide-ranging data privacy issues, including businesses' use of consumers' geolocation data.[79] The differing approaches among states could present a regulatory compliance challenge for entities that collect geolocation data and operate in multiple states. In response, some Members of Congress introduced bills in previous Congresses that would have contained preemption provisions aiming to reduce the variation in applicability of these state laws.[80] If a federal law or regulation were to preempt state laws, inconsistencies between state regulations might be mitigated.[81] However, the preemption

[73] CRS Legal Sidebar LSB10895, *New FCC Rules Ban Authorizations for Equipment Posing National Security Risks*, by Chris D. Linebaugh.

[74] See CRS Insight IN11663, *Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions*, by Jill C. Gallagher.

[75] FCC Public Notice DA 25-418, *The Public Safety and Homeland Security Bureau and the Office of Engineering and Technology Seek Public Input on Commerce Department Determination Regarding Certain Connected Vehicle Technologies*, May 23, 2025, https://docs.fcc.gov/public/attachments/DA-25-418A1.pdf.

[76] DOJ, National Security Division, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," 90 *Federal Register* 1636.

[77] DOJ, National Security Division, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," 90 *Federal Register* 1636.

[78] IAPP, "U.S. State Privacy Legislation Tracker 2025," updated September 23, 2025, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

[79] In the California Consumer Privacy Act of 2018, the term *geolocation data* is included in the definition of "sensitive personal information" subject to special protections; see Cal. Civ. Code §§1798.121, 140, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[80] H.R. 8152 (117th Congress); H.R. 8818 (118th Congress); H.R. 2110 (119th Congress); and S. 5579 (118th Congress). For more information on preemption, see the "'Related to'" section of CRS Report R45825, *Federal Preemption: A Legal Primer*, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes.

[81] Peter Swire, "U.S. Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws," IAPP, January 9, 2019, https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/ (hereinafter Swire, "U.S. Federal Privacy Preemption"); and Cameron Kerry et al., *Bridging the*

(continued...)

provision in some bills might inhibit a state's ability to enforce privacy laws that are stricter than federal privacy laws, leading to potential legal issues.[82]

# Policy Considerations

Congress may consider whether the regulatory framework under existing agency authorities or the current industry practices are sufficient to harness the benefits and mitigate the risks related to vehicle geolocation data collection. Congress may decide to not take legislative action and defer to agencies while engaging in oversight and investigation activities. Alternatively, Congress might decide that additional action is necessary from these agencies or encourage action in the private sector. If so, Congress would have a range of options to consider, depending on its policy priorities. Congress could request further rulemaking or studies from federal agencies on vehicle geolocation data. Congress might also clarify or specify federal agencies' authorities and responsibilities when regulating vehicle geolocation data or provide incentives for industry partners to engage in certain behavior or activities. Congress might consider agency capacity, specialization, or other factors when deciding to clarify, specify, or consolidate agencies' authorities. Congress could also choose to create a new agency to prioritize data privacy oversight. For example, the Data Protection Act of 2021 (H.R. 2134, 117th Congress) would have established an independent agency to regulate selected data practices.[83] Additionally, Congress may consider whether to preempt state laws to provide a unified federal regulatory framework through legislation.

Legislation that would broadly cover consumer data, such as a comprehensive federal data privacy law or law regulating data brokers, may accomplish some goals related to regulation of vehicle geolocation data. Congress might also opt for targeted legislation, which could cover vehicle data collection practices in general, limit data access by certain entities (e.g., insurance companies), provide specific measures to protect the data of domestic-abuse survivors, or clarify the process in which law enforcement may access geolocation data.

## Comprehensive Federal Data Privacy Legislation

In previous Congresses, some Members introduced legislation that would have broadly covered data privacy and certain aspects of vehicle geolocation data that fall under that scope (e.g., the American Data Privacy and Protection Act [H.R. 8152, 117th Congress] and the American Privacy Rights Act of 2024 [APRA; H.R. 8818, 118th Congress]). These bills attempted to establish federal requirements for how companies are to handle personal data. In these bills, vehicle geolocation data was covered in provisions on data minimization,[84] consumer awareness,[85]

*Gaps: A Path Forward to Federal Privacy Legislation*, Brookings, June 2020, https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf (hereinafter Kerry et al., *Bridging the Gaps*).

[82] Swire, "U.S. Federal Privacy Preemption"; and Hayley Tsukayama, "Federal Preemption of State Privacy Law Hurts Everyone," Electronic Frontier Foundation, July 28, 2022, https://www.eff.org/deeplinks/2022/07/federal-preemption-state-privacy-law-hurts-everyone.

[83] H.R. 2134 (117th Congress).

[84] See H.R. 8152, §101, and H.R. 8818, §102, for information on data minimization.

[85] See H.R. 8152, §201, for information on consumer awareness.

transparency,[86] data ownership,[87] the right to consent and object,[88] data brokers,[89] third parties,[90] and the potential overriding of state regulation.[91] Congress may opt against such broad legislation if it determines that current industry practices and self-regulation are sufficient to address privacy concerns or that comprehensive data privacy legislation would have potential adverse effects, such as reducing the industry's ability to introduce new technologies or creating a complex regulatory burden for the private sector.

## Legislation on Data Brokers

Congress may consider guiding the oversight of vehicle geolocation data sharing through legislation that would target data brokers. For instance, APRA would have regulated the exchange of vehicle geolocation data and related practices of data brokers.[92] Targeted legislation, such as the Data Broker Accountability and Transparency Act of 2019 (S. 2577, 116th Congress), would have established federal oversight of data brokers. Legislative options could include a requirement for data brokers to provide consumers with access to their personal information, to provide consumers an opportunity to correct inaccuracies, to register with the federal government, or to abide by other practices defined in legislation.

## Data Privacy Law for Vehicles

Legislation could target vehicle data collection specifically. Such legislation might address issues such as extent of the data collected, enforcement actions, limitations in the transfer and sale of the data, disclosure practices, consumer choice, and defining of regulatory authority. For example, the Auto Data Privacy and Autonomy Act (H.R. 10473/S. 5579, 118th Congress) would have prevented covered vehicle manufacturers from accessing or selling "certain covered vehicle data," including geolocation data, and designated the FTC as the agency to set the standards and enforce the act.[93] The collection of the covered data would have been permitted only with consumer consent or if the data were collected solely to improve vehicle performance or safety.[94] Exchange of the data would have been limited to certain circumstances, such as a warrant, court order, or emergency response facilitation, and the data would have been barred from foreign adversaries.[95] The proposed bill stated, "This Act supersedes any statute, rule, requirement, or

[86] See H.R. 8152, §202, and H.R. 8818, §104, for information on transparency.

[87] See H.R. 8152, §203, for information on data ownership.

[88] See H.R. 8152, §204, for information on the right to consent and object.

[89] See H.R. 8818, §112, for information on data brokers.

[90] See H.R. 8152, §302, and H.R. 8818, §111, for information on third parties.

[91] See H.R. 8152, §402; H.R. 8152, §404; and H.R. 8818, §116, for information on the potential to override state regulations. For more on these bills that would have preempted states laws, see CRS Legal Sidebar LSB10776, *Overview of the American Data Privacy and Protection Act, H.R. 8152*, by Jonathan M. Gaffney, Eric N. Holmes, and Chris D. Linebaugh; CRS Report R45631, *Data Protection Law: An Overview*, by Steve P. Mulligan and Chris D. Linebaugh; and CRS Legal Sidebar LSB11161, *The American Privacy Rights Act*, by Chris D. Linebaugh et al.

[92] See H.R. 8818, §112, for information on data brokers. For more on comprehensive data privacy legislation and data brokers, see CRS report CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Ling Zhu.

[93] See H.R. 10473, §§3(a)(1)-(2), and S. 5579, §§3(a)(1)-(2).

[94] See H.R. 10473, §§3(a)(1)(A)-(B), and S. 5579, §§3(a)(1)(A)-(B).

[95] See H.R. 10473, §§3(a)(2)-(3), and S. 5579, §§3(a)(2)-(3).

other legal obligation of a State or political subdivision thereof, or any Federal law or regulation, that relates to the requirements in this Act."[96]

## Insurance Companies' Access to Geolocation Data

A potential issue for Congress is insurance companies' access to vehicle geolocation data, as some of these companies may use the data to raise rates without consumers' awareness. The Senate Committee on Commerce, Science, and Transportation of the 116th Congress and the House Committee on Energy and Commerce of the 118th Congress both explored issues related to the exchange and sale of consumer data.[97] Options for congressional committees could include hearings on vehicle geolocation data accessed by insurance companies, requests to automotive manufacturers for information on their data collection practices, investigations of industry practices, requests for research by a specific agency, legislation that would limit the sale or transfer of geolocation data to insurance companies, or exploration of other avenues to limit such access.

## Protection of Domestic-Abuse Survivors

The risks that connected vehicles present to survivors of domestic abuse have been a congressional concern. For example, the Safe Vehicle Access for Survivors Act (H.R. 2110, 119th Congress) has been introduced and referred to the House Committee on Energy and Commerce. The act would "establish a process for survivors to request the termination or disabling of connected vehicle services that abusers misuse."[98] The act also would require the FCC to issue a notice of proposed rulemaking, in consultation with NHTSA, to prescribe how a motor vehicle manufacturer that provides a connected service is to address such connected vehicle service requests. Actions such as these may help protect the personal security of domestic-abuse survivors. For example, if a car is registered in an abuser's name who may then have access to vehicle tracking data, a domestic-abuse survivor could bolster personal security by requesting to disable connecting vehicle features that may expose the vehicle and survivor to tracking.

## Law Enforcement Access to Geolocation Data

Congress may consider whether to provide statutory guardrails for law enforcement and governmental entities that seek to access geolocation data. Several bills introduced in previous Congresses would have addressed the issue of warrantless access of geolocation data. For example, the Geolocation Privacy and Surveillance Act (S. 237, 114th Congress) would have specified the circumstances in which a person may acquire geolocation information.[99] The Closing the Warrantless Digital Car Search Loophole Act of 2021 (S. 3231, 117th Congress)

[96] See H.R. 10473, §7, and S. 5579, §7. For more on preemption clauses that use "that relates to," see the "'Related to'" section of CRS Report R45825, *Federal Preemption: A Legal Primer*, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes.

[97] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Examining Legislative Proposals to Protect Consumer Data Privacy*, hearing, 116th Cong., 1st sess., December 4, 2019, S.Hrg. 116-619, https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy; and U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Who Is Selling Your Data: A Critical Examination of the Role Data Brokers in the Digital Economy*, 118th Cong., 1st sess., April 19, 2023, H.Hrg. 118-26, https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-who-is-buying-and-selling-your-data-shining-a-light-on-data-brokers.

[98] H.R. 2110 (119th Congress).

[99] S. 237.

would have prohibited investigative and law enforcement officers from accessing vehicle geolocation data unless pursuant to a warrant.[100] The Auto Data Privacy and Autonomy Act (H.R. 10473/S. 5579, 118th Congress) would have barred the exchange of sensitive data, including geolocation data, without "a lawfully executed warrant" or "court order that provides the covered vehicle owner notice of the order and at least 48 hours to object and request a hearing."[101] Congress could decide that the Fourth Amendment as interpreted by the U.S. Supreme Court in *Carpenter v. United States*, which limits warrantless collection of historical geolocation data in certain circumstances, provides sufficient protection and that further legislation is not needed.[102]

## Author Information

Naseeb A. Souweidane
Analyst in Transportation Policy

## Disclaimer



[100] S. 3231.

[101] See H.R. 10473, §§3(a)(2)(A)(i)-(ii), and S. 5579, §§3(a)(2)(A)(i)-(ii), for information on warrants and court orders.

[102] Carpenter v. United States, 585 U.S. 296 (2018), https://www.supremecourt.gov/opinions/17pdf/585us1r62_mlho.pdf.