BMW Group

December 21, 2023

Re: Your Letter Dated November 30, 2023

Dear Senator Markey,

In response to your letter dated November 30, 2023, we thank you for the opportunity to share our approach to car data. Also included in this letter is our press release dated September 14, 2023, regarding Mozilla Foundation's "Privacy Not Included" publication. In this press release, we address and correct several points.

Across BMW vehicles, the customer controls *if* their data is used and *how* their data is used. Generally, BMW only collects data from its vehicles if the customer voluntarily selects options within the Data Privacy menu. Further, BMW empowers the customer to make specific, detailed, and informed selections and entire categories relating to how their vehicle data is collected and used.

The focus of data collection in a BMW is on providing the highest level of customer experience using transparent privacy notices and privacy choices. In order to receive the full functionality of the BMW telematics system to offer services and entertainment features, the customer must first link their vehicle to their online secured BMW ConnectedDrive account. The online account provides BMW customers with a comprehensive privacy policy. Customers may then opt in to specific or category-based privacy choices relating to how they would choose to have their data collected or used. BMW does not sell customer data collected from its vehicles. Furthermore, BMW takes comprehensive security measures designed to protect customer data that relate to the collection, transfer, and use of customer information from the vehicles to BMW's systems, including the encryption of this information. BMW also takes privacy measures, such as deidentification, designed to ensure that internal data use further protects customer privacy.

Company
BMW of North America, LLC

BMW Group Company

Mailing address
PO Box 1227
Westwood, NJ
07675-1227

Office address
300 Chestnut Ridge Road
Woodcliff Lake, NJ
07677-7731

Telephone
(201) 307-4000

Website
bmwusa.com

BMW customers control how vehicle data is collected and sent outside of their vehicle. The option to decline sharing data with BMW is clear and the customer must affirmatively consent to data being shared. Customers must consent to connect the vehicle with their online account or app. This activates features which may send vehicle data to BMW's backend systems. Once completed, customers may enter the Data Privacy menu using their in-vehicle dashboard and select or de-select individual functions and features. If customers do not consent to the collection and use of vehicle data, BMW generally limits its connected services to life saving services such as Emergency Call and Automatic Crash Notification. However, BMW customers may even choose to completely disable all data collection and transfer from their vehicles. In this case, the vehicle's SIM will not connect to the Mobile Network and no vehicle data is sent to the backend. In those cases, even the Emergency Call and Automatic Crash Notification services will not function.

Data stored locally in the vehicle can be deleted via "Reset to Factory Settings" in the vehicle itself. Personal data within the vehicle (i.e., recent destinations, saved stations, etc.) is stored in each driver profile. If the vehicle is used with the "Guest" profile, personal data is not stored or retained after the next life cycle, which entails a 15 minute duration between the vehicle being turned off and back on again. Customers can have their data deleted by emailing this request to our Customer Care Organization, linked on our Privacy Policy.

When received through proper Service of Process and bound by law, we have provided personal information collected by the vehicle to Law Enforcement. We provide this information only in response to a subpoena, warrant, court order, or other valid legal process. If we are instructed by law enforcement to notify the vehicle owner when we comply with a request, we will do so.

Thank you again for your interest in our approach to car data. We look forward to continuing the dialogue with you.

Sincerely,

Thomas Ruemenapp
Vice President of Engineering, US

PRESS RELEASE

BMW of North America Responds to Mozilla Foundation's "Privacy Not Included" Survey. Woodcliff Lake, NJ – September 14, 2023

BMW of North America takes data privacy and the data security of our customers very seriously. We provide our customers with comprehensive data privacy notices regarding the collection of their personal information and allows vehicle drivers to make granular choices regarding the collection and processing of their personal information. Further, we allow our customers to delete their data whether on their apps, vehicles or online. BMW NA does not sell our customer's in-vehicle personal information and provides our customers the opportunity to opt out of BMW targeted behavioral advertising on the Internet. With that, we would also like to clarify a few of the allegations made by Mozilla Foundation in their recent "Privacy Not Included" survey. While the story published on September 6, 2023, includes several inaccuracies, we wanted to address and correct five important points.

1. All BMW vehicle interfaces permit consumers to opt in or out of various types of data collection and processing that may happen on their vehicles. If they choose, BMW customers may opt out of ALL optional data collection relating to their vehicles at any time by visiting the BMW iDrive screen in their vehicle. In addition, BMW drivers may, at any time, completely disable the transfer of any data from BMW vehicles to BMW services by disabling their embedded SIM on their vehicles via contacting BMW and completing a form. However, many customers voluntarily enable this feature, given that eCall and SoS calls would not be possible after the cellular connection to the vehicle is disabled.

2. BMW's collection of data relates to BMW's own marketing efforts, legal compliance obligations, law enforcement issues and related items. Using commonly available web browser controls, BMW NA customers may opt out of data collection used to make inferences about drivers' preferences and habits and to opt out of receiving marketing communications at any time.

3. The report expresses concerns over BMW sharing customer data within our "family of companies" and "with third party dealers, service providers, and business partners." BMW centralizes data collection and processing activities to create

efficiencies and to better secure its systems. Additionally, BMW NA shares personal information with authorized dealers to better service our customers, and BMW NA customers choose which dealers they interact with. Much like any other company in the world, BMW NA uses service providers to accomplish certain tasks. For example, we may use an email service provider to send emails or use advertising companies to advertise. These providers are contractually obligated to keep confidential any information BMW provides to them. They are also not permitted to use that information for their own purposes. Finally, we only share personal information with business partners when our customers request that we do so. Regarding Mozilla's comment that states: "we can't quite tell if they share (or sell) all that data with other third parties for their advertising purposes as well," – we would like to confirm that BMW NA's privacy policy explicitly states that BMW NA does not sell its customers personal information, such as their names, addresses, driving habits, Vehicle Identification Numbers, or other information that is tied to the customers or their vehicles. Additionally, BMW NA engages in online behavioral advertising solely for its own products or services (that is, to sell its vehicles to consumers). We do not sell this online information for use by other third-party companies for their own marketing purposes.

4. Contrary to Mozilla's report, BMW NA provides multiple avenues for every customer to completely delete their data. First, customers' may exercise their privacy rights using an online portal (whether for access, correction, or deletion). Second, BMW NA customers may delete their data from their vehicles using available features on iDrive. Third, BMW NA customers may delete the information relating to their My BMW app using the delete functionality near the privacy and terms portion of the app. Furthermore, BMW NA voluntarily complies with every individual's privacy requests in the US regardless of the customer residing in a state where consumer privacy laws allow for such rights (whether relating to access, correction, deletion, or opting out of sale with respect to online behavioral advertising) exist.

5. With regard to Mozilla's warning to drivers that "you might not want your insurance company to know about your lead foot.... except, there's a pretty high likelihood they already do," BMW NA operates a permission and consent based CarData program that is available to each customer on their My Garage feature within BMWusa.com. Each BMW customer can specifically select any business partner with whom they would like to share data from their vehicles, and can revoke these permissions at any time. BMW NA does not share customer's personal information with insurance companies without consent. Insurance carriers have been operating telematics-based insurance programs for over a decade. If BMW customers wish to share their telematics information with their insurance carriers, then that is solely based on their choice. BMW merely ensures that any such sharing of data is done in an informed, controlled, consented, and secure manner. Furthermore, BMW customers may choose to share data relating to their driving behavior with their insurance carriers (without using any BMW vehicle system or the BMW back end) simply by using their insurance carrier's mobile app or OBD2 hardware connected insurance programs.

# # #

VIA ELECTRONIC TRANSMISSION

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building,
Washington, DC 20510

December 21, 2023

Dear Senator Markey:

Thank you for your recent letter inquiring into Ford's privacy practices related to personal information generated by connected vehicles ("connected vehicle data"). We welcome the opportunity to share details of Ford's privacy practices. Ford is committed to being a trusted steward of the personal information our customers choose to share with us. For example, Ford helped lead the development of the automotive industry's *Consumer Privacy Protection Principles* and has committed to adhering to them since their original adoption in 2014.

Customer Benefits of Connected Vehicle Data. While details about vehicle connectivity vary by model, model year, and trim level, Ford and Lincoln vehicles in North America generally have been equipped with cellular connectivity technology since the end of 2019. Connected vehicle data may include vehicle data (e.g., odometer, oil level, diagnostic trouble codes), driving behavior data (e.g., speed, braking), location data (e.g., precise GPS data), microphone, LiDAR, and internal and external cameras.

We use connected vehicle data to make our vehicles more enjoyable to drive and own, including by providing and improving services that are requested by our customers. For example, connected vehicle data is used to provide navigation services, vehicle health alerts and reports, connected radio, and connected weather. In electric vehicles (EVs), connected vehicle data may also power EV smart charging features and services, such as finding locations of nearby Blue Oval electric-vehicle charging stations, paying for charging, and EV charge programming.

We also use connected vehicle data to improve vehicle quality, make our vehicles safer, and minimize environmental impact. For example, we use connected vehicle data to develop and improve vehicle features such as autonomous vehicle technology, and to more quickly identify and remedy potential vehicle performance issues. Connected vehicle data may also be used in recall-related investigations. As the National Highway Traffic Safety Administration recently concluded in a June 2023 letter to automakers, connected vehicle data can be "an important

801 Pennsylvania Avenue NW
Suite 400
Washington, DC 20004

source of information for safety oversight and field performance monitoring by the authorities and vehicle manufacturers."[1]

Customer Notice. We provide notice to our customers about our connected vehicle privacy practices in our Ford Connected Vehicle Privacy Notice, which supplements the Ford U.S. Privacy Notice, and specifically governs personal information originating from Ford or Lincoln vehicles that are purchased or leased by individual consumers for personal use in the United States.[2] Some customers may also choose to download the FordPass and LincolnWay apps and associate their vehicle with their FordPass or LincolnWay accounts so that, for example, they can use the app to "Find My Vehicle" or enable other connected services. These customers can learn more about Ford's relevant privacy practices by reviewing The FordPass Terms and Privacy Policy[3] and The Lincoln Way Terms and Privacy Policy.[4]

Consent and Consumer Rights. Ford provides our customers with a choice as to whether or not they wish to share connected vehicle data with us. Using in-vehicle settings, customers may turn vehicle connectivity off entirely (resulting in a disconnection from the cellular network) and may exercise granular settings that control sharing vehicle data, driving data, and/or location data with Ford. Customers can continue to enjoy connected features or services that do not rely on the data that they choose not to share. For example, customers cannot utilize a "Find my Vehicle" feature if they choose not to enable location data sharing, but they can still receive vehicle health alerts or any of the other services that do not require location to function. Notably, if a customer turns off data sharing with Ford and later turns it back on, none of the relevant connected vehicle data from when the data sharing was turned off will be offboarded from the vehicle if or when data sharing is resumed. Thus, for example, if location data sharing is turned off on a Monday, location data from Tuesday through Thursday will not be offboarded from the vehicle if location data sharing is turned back on that Friday.

Ford complies with all applicable state privacy laws regarding consumer rights, including processing requests by authorized agents in accord with applicable state laws. Earlier this year, Ford also began processing any request we received from individual customers *across the United States* to access and/or delete their connected vehicle data. We anticipate publicly announcing this nationwide initiative in an upcoming privacy policy update.

---

[1] *See* article describing NHTSA letter by David Shepardson, *US tells automakers not to comply with Massachusetts vehicle data law* REUTERS (June 13, 2023), *available at* https://www.reuters.com/business/autos-transportation/us-tells-automakers-not-comply-with-massachusetts-vehicle-data-law-2023-06-13/. See Ford's Connected Vehicle Privacy Notice for more information on how Ford collects, uses and shares connected vehicle data.

[2] *Available at*: https://www.ford.com/help/privacy/#connectedvehicleprivacynotice. The Connected Vehicle Privacy Notice supplements Ford's general U.S. Privacy Notice, which governs Ford's collection, use and disclosure of all personal information that Ford collects through its products, services and features, including websites, mobile applications, online services, and vehicles. *See* https://www.ford.com/help/privacy/#USprivacypolicy.

[3] *Available at*: https://www.ford.com/support/how-tos/fordpass/manage-my-fordpass-account/fordpass-privacy-policy/.

[4] *Available at*: https://www.lincoln.com/lincolnway/en_us/termsprivacy.html#two. Consumers may also review The Ford California Consumer Privacy Act Policy and Notice at Collection, which supplements the Ford U.S. Privacy Notice and the Connected Vehicle Privacy Notice for California residents and addresses the CCPA's statutory requirements.

Cybersecurity Safeguards. While no organization can eliminate cybersecurity risk entirely, we devote significant resources to a multi-layered cybersecurity program that is reasonably designed to protect against, and mitigate the effects of, among other things, cybersecurity incidents where unauthorized parties attempt to access connected vehicle data.

Ford's cybersecurity program leverages both internal and external techniques and expertise. Internally, among other things, we perform penetration tests, internal tests/code reviews, and simulations using ethical hackers (commonly referred to as a "Red Team") to assess vulnerabilities in our information systems and evaluate our cyber defense capabilities. We also perform phishing and social engineering simulations with, and provide cybersecurity training for, personnel with access to connected vehicle data (and other Ford assets). On a monthly basis, we disseminate security awareness newsletters to employees to highlight emerging or urgent cybersecurity threats and best practices.

Externally, we invest in enhancing our cybersecurity capabilities and strengthening our partnerships with appropriate business partners, service partners, and government and law enforcement agencies to understand the range of cybersecurity risks in the operating environment, enhance defenses, and improve resiliency against cybersecurity threats. For example, we monitor notifications from the U.S. Computer Emergency Readiness Team ("CERT") and various Information Sharing and Analysis Centers (each an "ISAC"); review customer, media, and third-party cybersecurity reports; and offer bounties to responsible third parties who notify us of vulnerabilities they are able to detect in our cyber defenses (commonly referred to as a "Bug Bounty").

Our capabilities, processes, and other security measures include:

- Security Information and Event Management ("SIEM") software, which provides a threat detection, compliance, and security incident management system;
- Endpoint Detection and Response ("EDR") software, which monitors for malicious activities on external-facing endpoints (e.g., Windows workstations, servers, MAC clients, and Linux endpoints);
- Cloud monitoring, running on primary public and private cloud environments; and
- Disaster recovery and incident response plans.

Ford has not suffered a data breach involving connected vehicle data.

De-identification and Data Minimization. In addition to the safeguards described above, we also implement strict controls on who may access connected vehicle data, and only retain it for as long as it is necessary for legitimate business purposes. Importantly, Ford seeks to *optimize*, not maximize, connected vehicle data for the benefit of our customers. We seek ways in which we may be able to protect customer privacy through the use of privacy-enhancing technologies such as deidentification. We also continue to look for ways to further minimize the data we collect and retain because we know that sometimes the best way to protect connected vehicle data is to never collect it in the first place. Below are two examples of how we employ privacy-enhancing technologies and data-minimization practices.

Phone data. When a consumer in an equipped Ford or Lincoln vehicle chooses to connect their phone to the vehicle, Ford does not collect any data from the phone other than a device identifier in a hashed (i.e., unidentified) format so that we can understand, on an aggregated basis, how many customers choose to connect their phone to the vehicle.

Thus, for example, Ford does not collect, or otherwise have access to, personal information in connection with a customer's use of third-party phone-based platforms and apps, such as Apple CarPlay, Android Auto, or any other web-based entertainment services (e.g., Spotify) that customers may use in equipped Ford or Lincoln vehicles.

Customers may sometimes choose to transfer certain phone data to the vehicle to support desired features, such as downloading their phone contacts to simplify the dialing process when using Bluetooth to make hands-free phone calls. These phone contacts remain on-board the vehicle. If a customer chooses to use the voice assistant feature in equipped vehicles, and agrees to download their contacts, those contact names (but not phone numbers) may be provided directly to Ford's voice recognition service provider to improve the voice assistant's ability to recognize and respond to contact-related voice commands (e.g., "Call Jeanine"). Ford does not have access to this data.

Additionally, customers who connect their phones to an equipped Ford or Lincoln vehicle may choose to enable the 911 Assist feature, which allows a call to be made from the consumer's phone directly to the local emergency services provider (known as a public safety answering point, or PSAP) after certain triggering events like an airbag deployment or other indications of a vehicle crash. As part of that call, the phone may provide its location, carrier, and callback number to the PSAP for use in responding to the emergency and assisting the customer. The callback number is provided so the PSAP can attempt to call the customer back if the initial call is interrupted. During this call, the PSAP is given the option to request vehicle location. The data provided to the PSAP, including vehicle location, is not shared with Ford.

Camera Data. Certain Ford and Lincoln vehicles are equipped with external front, rear, and side cameras that support vehicle and safety features, such as crash avoidance, lane assist, and parking assist features. Other than the one exception described below, no images or videos from these external-facing cameras are off-boarded from the vehicle to Ford.

In certain equipped vehicles with a new trailer hitch assistance feature, cropped images from the external rear-facing vehicle camera are collected during trailering events. These images are cropped to focus solely on the vehicle's trailer hitch area and exclude or remove any license plate or other information *before* being offboarded to Ford for internal use in improving Ford's trailering features.

Additionally, Ford and Lincoln vehicles equipped with BlueCruise – Ford's hands-free highway driving technology – include an internal camera focused on the driver's eyes and face. This camera is used to estimate driver attentiveness because BlueCruise will not allow the system to function unless it determines the driver is attentive to road conditions while driving hands-free. This camera is only active while the driver chooses to use BlueCruise. No images or videos are offboarded from this in-vehicle camera to Ford.

Data Sharing. Finally, Ford generally may share connected vehicle data with 1) dealers or independent repair companies for repair purposes; 2) service providers; or 3) third parties when it is at the direction of our customers. For example, some customers authorize Ford to share connected vehicle data with their insurance company so that they can enjoy discounted insurance premiums. Ford may also share connected vehicle data with law enforcement in response to valid legal process or in the case of exigent circumstances. For example, Ford recently aided the FBI and New York law enforcement to locate a suspect in the kidnapping of a 9-year girl who was abducted while bike riding near her family's campsite. The search area had encompassed over 46 miles and involved 400 personnel from law enforcement, fire departments, and private search and rescue groups. Ford was able to provide the vehicle's location, which resulted in the arrest of the 46-year-old suspect and the safe return of the child, who was found in good health, to her family. As another example, Ford also aided law enforcement in locating a missing person who was believed to be at risk of self-harm (i.e., the individual had a known history of depression, had recently lost his job, and had left what was understood to be a suicide note for his son), allowing police to establish contact with the missing individual and escort him to a psychiatric hospital.

Ford does not sell connected vehicle data to data brokers. Indeed, one of Ford's concerns with the currently proposed REPAIR Act (H.R. 906) is that Section 3(a)(2)(B) of the bill seeks to establish a third-party "standardized access platform" for the apparent intent of selling connected vehicle data to third parties for *any* purpose, including the third party's own commercial purposes. This provision would, in effect, establish a data broker with which all auto manufacturers would be required to share connected vehicle data. We believe that such a provision would be antithetical to most of our customers' wishes. We view this provision to be particularly concerning from a privacy perspective in light of the lack of a federal privacy law that would protect our customers in states without a comprehensive privacy law.[5] We ask that you join us in objecting to this bill. Ford strongly supports enacting a federal privacy law as well as a federal law that would provide for the *safe* and *secure* right to repair for consumers.

Thank you again for your interest in this important topic. We appreciate the opportunity to engage with you and other policymakers on these important issues.

Regards,

Christopher A. Smith
Chief Government Affairs Officer
Ford Motor Company

[5] Ford also has significant cybersecurity and safety concerns related to the REPAIR Act's requirement for auto manufacturers to provide "open" access to connected vehicle data.

25 Massachusetts Avenue, NW
Suite 400
Washington, DC 20001

December 21, 2023

[redacted]

Edward J. Markey
United States Senate
255 Dirksen Senate
Office Building
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter regarding consumer data privacy and the protection of personal information, both of which are important to General Motors Company ("GM") as we pursue our vision of a world with zero crashes, zero emissions and zero congestion. Central to that vision is utilizing vehicle connectivity to bring safety and convenience to our customers as we keep them in control of their connectivity, maintain transparency in our data practices, and safeguard personal information.

GM has the ability to collect certain user data from vehicles within the GM family of brands if a customer chooses to opt-in to connectivity and consents to the corresponding data collection, as outlined in GM's US Connected Services Privacy Statement. If customers choose to do this, they have access to an array of Connected Services that include safety, convenience, and infotainment features such as OnStar Safety & Security, in-vehicle applications, navigation, and remote vehicle access. GM is proud of its long history as a leader in providing customers with the latest in-vehicle and connected technology, having introduced the first in-vehicle telematics system in 1996.

Safety benefits
We believe that connectivity is essential to enabling critical safety services. With OnStar Safety & Security, for example, customers have around-the-clock access to advisors to help with roadside assistance or navigation. In a crash, medical emergency, weather event, or other times of need, specially trained OnStar emergency advisors will contact the appropriate 911 agency to request assistance to be sent to the location of the emergency and will stay on the line with the customer until help arrives. GM also provides OnStar Crisis Assist Services, where advisors provide critical information, special routing and communication facilitation to help all our customers stay in touch with loved ones in the event of severe weather, a natural disaster or other crisis.

Infotainment and convenience
Connectivity of the vehicle also enables convenience features, such as Wi-Fi hotspot, smart navigation, and entertainment applications via the infotainment unit. Customers with a connected vehicle can also use GM's mobile applications to issue remote commands to the vehicle, such as remote start in cold weather, check vehicle status for safety and service issues, and schedule service appointments.

Diagnostics and operational information
Connectivity further enables GM to collect vehicle diagnostic and operational information about the vehicles it manufactures. Such data is vital to GM's ability to proactively identify potential issues within

GM vehicles, including critical safety issues, and provide the necessary support, service, and customer outreach to address such issues. Finally, the collection and analysis of vehicle data from today's vehicles is a critical component to improving the quality, safety, and security of the next generation of GM vehicles.

GM provides the following responses to the questions in your letter dated November 30, 2023. As requested, these responses are limited to GM's data practices related to new model vehicles offered for sale by GM dealers, which presently includes MY23 and MY24 Buick, Cadillac, Chevrolet and GMC vehicles ("Vehicles"), except where noted below. These responses exclude vehicle data collected from Vehicles pursuant to development or testing initiatives as part of GM's non-retail company car programs.

GM is responding on behalf of itself and the following subsidiaries and affiliates: General Motors Holdings LLC, General Motors LLC, OnStar, LLC, BrightDrop LLC, General Motors Energy LLC, GM Defense LLC, General Motors Financial Company, Inc., and OnStar Insurance, LLC. GM is not responding on behalf of Cruise LLC, as Cruise LLC vehicles are not available to retail customers.

All references to "owner" are limited to the individual that owns or leases a Vehicle. All references to "user" are limited to an individual that is operating a Vehicle.

GM has diligently prepared this response. Given the time period provided to respond to this inquiry, GM may supplement this response as necessary.

1. **Does your company collect user data from its vehicles, including but not limited to the actions, behaviors, or personal information of any owner or user?**

Central to GM's approach is keeping customers in control of their connectivity, maintaining transparency in our data practices, and safeguarding personal information.

If a customer opts in to Connected Services, then yes, GM collects vehicle data.

In a set of rare cases where safety is concerned, we also currently have the ability to collect limited data from Vehicles whose owners have not opted-in to Connected Services to respond 1) if a user initiated an OnStar button press and 2) for safety-related alerts in specific models.

   a. **If so, please describe how your company uses data about owners and users collected from its vehicles. Please distinguish between data collected from users of your vehicles and data collected from those who sign up for additional services.**

Depending on vehicle hardware and software availability, GM currently uses data collected from Vehicles whose owners have opted in to Connected Services. Here are some examples of how that data would be used:

- To support the Connected Services that the owner requests to receive from GM.
- To provide functionality for GM in-vehicle applications and to understand the use of certain in-vehicle applications.
- To provide functionality within GM mobile applications.
- To administer in-vehicle infotainment profiles.
- To communicate with owners about their Connected Services or other available Connected Services.

- To respond to safety-related alerts in specific models.
- To facilitate over-the-air updates.
- To research and develop new products or services; evaluate and improve products or services; and identify and troubleshoot issues.
- To comply with legal or regulatory requirements; to protect its rights; and to detect, investigate, and prevent fraud or other illegal activity.
- For purposes of participation in low carbon fuel standard programs.
- To ensure safe operation of vehicles, provide owners service-related notifications on behalf of GM and its dealers.
- With separate consents from the owner, OnStar Insurance may provide offers of auto insurance discounts to eligible drivers and to provide insurance quotes.

As mentioned above, in a set of rare cases where safety is concerned, we also currently have the ability to collect limited data from Vehicles whose owners have not opted-in to Connected Services to respond 1) if a user initiated an OnStar button press and 2) for safety-related alerts in specific models.

b. Please identify every source of data collection in your new model vehicles, including each type of sensor, interface, or point of collection from the individual and the purpose of that data collection.

Vehicles contain many discrete electronic control units ("ECU") and sensors, all of which generate data in the normal course of vehicle operation. This data can be broadly categorized as follows: (i) raw data; (ii) data generated algorithmically from raw data; and (iii) data regarding the performance of the component itself, such as diagnostic codes. Vehicles also contain infotainment and rear seat media systems that have the ability to collect information from users.

A certain subset of this vehicle data (depending on vehicle model, connectivity type, and particular Connected Services enabled on the vehicle) may be collected by GM using connectivity. For certain Vehicles, when authenticated users of GM's mobile applications connect their phone to their vehicle, a limited set of this vehicle data is collected by GM through the mobile application. GM may also collect data directly from users via interactions with OnStar Advisors.

Regarding the purpose of data collection, please see GM's response to question 1(a).

c. Does your company collect more information than is needed to operate the vehicle and the services to which the individual consents?

No, please see GM's response to question 1(a), which explains how GM uses vehicle data.

d. Does your company collect information from passengers or people outside the vehicle? If so, what information and for what purposes?

Depending on vehicle hardware and software availability, GM currently collects the following vehicle passenger information from Vehicles:

- GM collects analytics data related to the use of certain in-vehicle applications to improve the quality, safety, and security of our products and services and for research. GM collects this data based on utilization of in-vehicle applications, whether initiated by users or passengers.

- If a passenger creates an in-vehicle infotainment profile, GM collects profile name, authentication information, vehicle setting and application preferences, and installed applications. This data is used to create a GM account and configure a Vehicle for the passenger for next user log in.
- The existence of a passenger in a specific seat, based on whether a seat belt is engaged.

GM does not currently collect information on people outside the vehicle.

e. Does your company sell, transfer, share, or otherwise derive commercial benefit from data collected from its vehicles to third parties? If so, how much did third parties pay your company in 2022 for that data?

If an owner opts in to Connected Services, GM has the ability to share data collected from Vehicles with third parties, as outlined in our US Connected Services Privacy Statement. For example, data might be shared to help emergency responders respond more quickly and accurately, to support in-vehicle services utilized by the owner, and where the owner directs GM to do so (such as helping owners optimize their charging patterns). For those limited data shares where there is a commercial benefit attributable directly to the data sharing, the impact to GM's overall 2022 revenue was de minimis.

f. Once your company collects this user data, does it perform any categorization or standardization procedures to group the data and make it readily accessible for third-party use?

No.

g. Does your company use this user data, or data on the user acquired from other sources, to create user profiles of any sort?

GM does not use vehicle data it collects, or vehicle data acquired from other sources, to create a user specific profile or engage in user profiling except in the case of OnStar Insurance, which uses vehicle data to optimize offers and related marketing for programs, services, and discounts for customers who opt-in to these limited marketing offers.

h. How does your company store and transmit different types of data collected on the vehicle? Do your company's vehicles include a cellular connection or Wi-Fi capabilities for transmitting data from the vehicle?

For most Vehicles, internal vehicle data transmission is handled by GM's Vehicle Intelligence Platform, which was designed with cybersecurity principles in mind, resulting in enhanced security controls such as vehicle network message authentication. Depending on the specific hardware and software configurations of an ECU, data may be stored within an ECU directly. Data is also stored in centralized locations within the vehicle as that data is being prepared to be offboarded.

Depending on vehicle hardware and software availability, encrypted data may be transmitted from the vehicle in the following ways:

- Using the vehicle's embedded cellular connectivity.
- When a user connects the vehicle to an external Wi-Fi network, using Wi-Fi.

- For certain Vehicles, when authenticated users of GM's mobile applications connect their phone to their vehicle, using that phone's connectivity.

2. Does your company provide notice to vehicle owners or users of its data practices?

Yes, we are guided by transparency and keeping the customer informed. With this, GM's US Connected Services Privacy Statement describes how GM collects, uses, and discloses vehicle data obtained from Vehicle through the use of Connected Services.

GM mobile applications, in-vehicle applications and rear seat media systems include supplementary privacy statements describing the data practices for those specific applications, which expressly incorporate the US Connected Services Privacy Statement. GM also provides California residents with GM's California Privacy Statement.

GM Owner's Manuals describe that if Connected Services are enabled, data may be collected by GM in accordance with the GM US Connected Services Privacy Statement.

GM also has embedded additional information on data practices directly within the user experience of its products and services.

GM provides the OnStar Insurance Driver Program Terms and OnStar Insurance Privacy Statement, both of which describe how OnStar Insurance may use vehicle data to provide offers of auto insurance discounts and to provide insurance quotes following separate opt-in from the owner.

3. Does your company provide owners or users an opportunity to exercise consent with respect to data collection in its vehicles?

Yes, central to GM's approach is keeping customers in control of their connectivity, maintaining transparency in our data practices, and safeguarding personal information. Owners must opt-in to Connected Services. In a set of rare cases where safety is concerned, we also currently have the ability to collect limited data from Vehicles whose owners have not opted-in to Connected Services to respond 1) if a user initiated an OnStar button press and 2) for safety-related alerts in specific models.

a. If so, please describe the process by which a user is able to exercise consent with respect to such data collection. If not, why not?

GM collects user data from Vehicles through the use of Connected Services. At the point of new vehicle sale or lease, the owner is presented with information about Connected Services and prompted to accept or decline the US Connected Services Privacy Statement. Owners who elect not to complete this process at the dealership or through other GM provided channels then have 30 days to accept the US Connected Services Privacy Statement or cellular connectivity is disabled. In order to connect a disabled vehicle, the owner must contact GM to re-activate the vehicle by double pressing the OnStar blue button from inside the vehicle and speaking with an advisor, who will send the consumer the US Connected Services Privacy Statement for review and acceptance as part of Connected Services being activated.

GM also provides separate consents for specific service offerings that may collect additional vehicle data, such as Smart Driver.

When users use GM in-vehicle applications, they must accept the applicable privacy statement for that application.

GM Vehicles with Android-based infotainment systems also utilize Android run-time application permissions ("Permissions"), which is a system that prevents in-vehicle applications from accessing certain vehicle data such as vehicle location and contacts stored in the infotainment head unit ("IHU"), unless a consumer expressly grants an application permission to access the data.

If a user connects a Vehicle to an external Wi-Fi network, the user must review and accept the US Connected Services Privacy Statement prior to connection.

If a user creates an in-vehicle profile, the user must review and accept the US Connected Services Privacy Statement prior to profile creation.

When a user's phone is paired with the vehicle, the user must approve the connection before vehicle data is collected for certain Vehicles.

b. If users are provided with an opportunity to exercise consent to your company's services, what percentage of users do so?

A small percentage of new vehicle owners do not opt-in to receive Connected Services.

c. Do users lose any vehicle functionality by opting out of or refusing to opt-in to data collection? If so, does the user lose access only to features that strictly require such data collection, or does your company disable features that could otherwise operate without that data collection?

If an owner does not elect to receive Connected Services, vehicle features and services that require connectivity to operate are not available, with the exception of safety-related alerts in certain vehicles.

Vehicles also include a location services setting, accessible via the IHU settings menu, that allows a user to disable sharing of vehicle location outside the vehicle. When disabled, vehicle location information will continue to be shared for emergency services and Super Cruise, if equipped.

If a user declines the privacy statement for a GM in-vehicle application, the application will not be accessible. If a Permission is declined for a GM in-vehicle application, the services requiring that permission will have diminished functionality.

4. Can all users, regardless of where they reside, request the deletion of their data? If so, please describe the process through which a user may delete their data. If not, why not?

A user can delete personal information stored in the vehicle infotainment and telematics systems through the infotainment system's Settings menu.

Beyond the vehicle, GM complies with all laws and regulations that require GM to delete personal information upon request, subject to legal requirements to maintain data. To exercise their rights, customers can go to gm.com and scroll to the bottom of the page. Click on the link for "Your Privacy Choices & Opt-Out Rights" and complete a Request to Delete.

5. **Does your company take steps to anonymize user data when it is used for its own purposes, shared with service providers, or shared with non-service provider third parties? If so, please describe your company's process for anonymizing user data, including any contractual restrictions on re-identification that your company imposes.**

GM utilizes some or all of the following deidentification processes where applicable: One-way encryption and/or secure hashing of unique identification numbers, removal of unique identifiers or personal information, and/or blurring of personal information.

Additionally, where GM discloses deidentified data to third parties, it includes contractual prohibitions restricting the recipient from re-identifying the data and requires data recipients to comply with applicable law.

6. **Does your company have any privacy standards or contractual restrictions for the third-party software it integrates into its vehicles, such as infotainment apps or operating systems? If so, please provide them. If not, why not?**

Yes, GM has policies and procedures requiring privacy and cybersecurity requirements and obligations to be incorporated into agreements with third parties that integrate software into Vehicles.

When GM is integrating software into Vehicles, GM cybersecurity will review the specific nature of the software and the functionality and data processing of the corresponding ECUs and then determine the appropriate standard technical requirements to apply to that component and the third-party supplier.

Third-party developers of in-vehicle applications must agree to GM's Developer Agreement, which contains standard privacy and security requirements and obligations and data use restrictions.

GM is not providing confidential and proprietary third-party agreements.

7. **Please describe your company's security practices, data minimization procedures, and standards in the storage of user data.**

GM's cybersecurity organization is governed by an independent office led by the Chief Cybersecurity Officer, reporting to GM's Executive Vice President of Legal, Policy, Cybersecurity and Strategic Initiatives as well as to the Risk and Cybersecurity Committee of the GM Board of Directors, which is responsible for overseeing the Company's key strategic, operational, and cybersecurity risks. Cybersecurity risk is managed across all aspects of GM and its third-party suppliers and vendors and is integrated into the Company's overall risk management program. Risks are evaluated quarterly, leveraging national standards such as the NIST Cybersecurity Framework and industry best practices developed collaboratively with organizations such as the Automotive-ISAC (Information and Sharing Analysis Center).

To ensure appropriate company senior leadership visibility and oversight, the Cybersecurity Management Board brings together senior executive management across the company to provide guidance and monitor overall company cybersecurity risk. Each quarter, the Risk and Cybersecurity Committee and Cybersecurity Management Board reviews the company's cybersecurity maturity scorecard, cybersecurity threat and appropriate incident information, and discusses various topics, including:

- Implementation and maturity of the company's cybersecurity program, risk management framework, including cybersecurity risk policies, procedures, and governance;

- Cybersecurity and privacy risk including potential impact to the company's employees, customers, supply chain, joint ventures, and other stakeholders;
- Intelligence briefings on notable cyber events impacting the industry; and
- Cybersecurity budget and resource allocation, including industry benchmarking and economic modeling of various potential cybersecurity events.

GM maintains a dedicated product cybersecurity team charged with the management of appropriate and layered cybersecurity controls across the connected vehicle to safeguard GM customers. Leveraging global standards such as ISO (International Standards Organization), SAE (Society of Automotive Engineers), and NHTSA (National Highway Traffic Safety Administration) Cybersecurity Best Practices, the team performs ongoing risk assessment, vulnerability management, and risk reduction activities. GM's Vehicles use NIST recommended encryption standards to secure user data and services, end-to-end, in transit, and at rest both within Vehicles and the GM back office.

GM has implemented a layered security approach to protect IT applications that process and store information received from vehicles, including access controls, continuous access reviews, data loss prevention, and encryption at rest and in transit.

GM follows a global privacy program framework that focuses on policies, procedures, tools, guidance, and training. As part of GM's program, GM conducts privacy impact assessments on information processing activities throughout the data lifecycle.

a. Has your company suffered a leak, breach, or hack within the last ten years in which user data was compromised?

GM has not had any material cybersecurity incidents in the last ten years.

b. If so, please detail the event(s), including the nature of your company's system that was exploited, the type and volume of data affected, and whether and how your company notified its impacted users.

Not applicable.

c. Is all the personal data stored on your company's vehicles encrypted? If not, what personal data is left open and unprotected? What steps can consumers take to limit this open storage of their personal information on their cars?

Yes, personal information stored on Vehicles is encrypted.

8. Has your company ever provided to law enforcement personal information collected by a vehicle?

In accordance with our terms, conditions, policies, and applicable law, GM will review each request individually to assess the circumstances and the nature of the request before providing vehicle data to law enforcement. With a focus on protecting customer data, GM will not produce vehicle data to law enforcement unless in response to (i) a warrant or court order supported by a showing of probable cause, (ii) A court order issued under 18 U.S.C. Section 2703(d), (iii) exigent circumstances, or (iv) subscriber consent. This is disclosed within GM's Privacy Statement and further explained on a dedicated law enforcement webpage on the OnStar website.

a. If so, please identify the number and types of requests that law enforcement agencies have submitted and the number of times your company has complied with those requests.

GM receives various types of requests from law enforcement agencies, including those that are integral to providing safety and security Connected Services. GM does not track law enforcement requests by whether vehicle data was part of the request.

b. Does your company provide that information only in response to a subpoena, warrant, or court order? If not, why not?

See above.

c. Does your company notify the vehicle owner when it complies with a request?

Not as part of GM's standard response process. Law enforcement routinely directs GM not to notify the vehicle owner, including through the use of sealed court orders.

* * * * *

And finally, GM remains supportive of ambitious, comprehensive federal privacy legislation which standardizes consumer rights to access, delete, and correct information across the country, enhances consumer privacy protections, and fosters US competitiveness and innovation. GM has comprehensive policies and procedures to comply with the variety of applicable state privacy regulations. As states continue to pass and enact comprehensive privacy laws, the patchwork of compliance grows ever more complicated and efforts to advance piecemeal or sector-specific privacy obligations only further complicates compliance. We are encouraged by Congress' attention to privacy and share the urgency for codifying a national privacy law which governs all actors of the economy and across all states, while at the same time advances consumer rights and promotes innovation.

Ultimately at GM, we are working towards a future of zero crashes, zero emissions and zero congestion. And we're doing this while allowing customers to control their connectivity, maintaining transparency in our data practices, and safeguarding personal information.

Thank you for the opportunity to answer your questions.

Sincerely,

Omar A. Vargas
General Motors Vice President, Global Public Policy
omar.vargas@gm.com

HONDA

American Honda Motor Co., Inc.
1001 G Street, N.W. Suite 950
Washington, D.C. 20001
Phone (202) 661-4400
Fax (202) 661-4459

December 21, 2023

The Honorable Edward J. Markey
255 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Markey:

Thank you for providing American Honda Motor, Inc. (Honda) the opportunity to respond to issues related to consumer privacy protection.

Honda believes in treating the data collected by our vehicles in a safe and responsible manner. The foundation of our relationship with each customer is trust in the quality and reliability of our products and our brand. As we move into the connected world, this includes trust that we will maintain cybersecurity to manage and protect any personal information provided by our customers to us or our partners and trust that we will use personal information in a thoughtful and transparent manner.

Please see our responses to your questions attached. Given the context of your request, our responses focus on personal information generated by and/or collected through vehicles and their related connected services.

Thank you again for giving us the opportunity to discuss this increasingly important topic. If you would like more information about Honda's vehicle data privacy practices, we encourage you to review Honda's Vehicle Data Privacy Notice available at https://www.honda.com/privacy/connected-product-privacy-notice.

Sincerely,

Jennifer Thomas
Vice President, Corporate Affairs
American Honda Motor, Inc.

Honda Responses

1. Does your company collect user data from its vehicles, including but not limited to the actions, behaviors, or personal information of any owner or user?

Honda collects information from vehicles including:

- "Vehicle Operation and Performance Information" such as:
    - Oil life, odometer mileage, fuel level, miles remaining to empty, dashboard warning lamps, tire pressure, battery life and charge status, coolant temperature, engine rotations per minute, diagnostic trouble codes, and vehicle maintenance status;
    - Trip log information, including trip start and end time, trip start and end location, trip distance, and fuel consumed;
    - Airbag system status and deployment information.
- "Driver Behavior Information" such as vehicle speed, pedal positions, engine speed, direction and time of travel during a crash event, steering angle, yaw rate, vehicle control and Honda Sensing/Acura Watch system settings and usage.
- "Precise Geolocation Information" meaning the exact location of a vehicle at a specific point in time or over a period of time accurate within an area equivalent to a circle with a radius of 1,850 feet or less.
- "Non-Precise Geolocation Information" meaning the approximate location of a vehicle at a specific point in time or over a period of time accurate within an area greater than an area equivalent to a circle with a radius of 1,850 feet or less.

Honda also collects certain information related to the use of connected services, including:

- Identifiers such as the consumer's name, login username & password, device identifier, and contact information such as the consumer's address, email address, and phone number;
- Audio, electronic, visual, or similar information such as calls and other communication recordings and associated logs with our customer service team or service providers or communications using Connected Vehicle Technologies and Services (as defined in Honda's Vehicle Data Privacy Notice);
- Information about use of Connected Vehicle Technologies and Services such as
    - Search content;
    - HondaLink and AcuraLink account access information, including information about any calls made using the Connected Vehicle Technologies and Services;
    - Call history information, including the date, time, and duration of a call;
    - Navigation system settings and usage;
    - Audio system settings and usage;
    - Voice commands given (which may include audio recordings);
    - Connectivity systems (e.g., embedded TCU, Wi-Fi hotspot) settings and usage;

For more details, please see Honda's Vehicle Data Privacy Notice.

a. If so, please describe how your company uses data about owners and users collected from its vehicles. Please distinguish between data collected from users of your vehicles and data collected from those who sign up for additional services.

Category of Data	Purposes of Processing
Vehicle Operation and Performance Information; Driver Behavior Information	• Provide the Connected Vehicle Technologies and Services; • Communicate with the consumer; • Evaluate and improve quality, performance, and design of vehicles and systems • Facilitate provision of software updates and enhancements to Connected Vehicle Technologies and Services; • Help maintain and provide alerts regarding the maintenance of the vehicle; • Provide customer service and product support; • Perform market research; • Facilitate safety, diagnostics, warranty, maintenance, recall, and compliance programs; • Develop future goods and services; • Prevent fraud or misuse; • Comply with legal and contractual requirements; • Protect our rights and property or the rights and property of others; • Help protect the safety of drivers or others in the vehicle; and • For any other purpose for which we obtain consent.
Geolocation Information	• To provide information to and assist incident responders or roadside assistance providers if the vehicle is in a crash or someone presses an assist button in the vehicle; • To provide information to and assist law enforcement agencies in situations we believe to constitute "exigent circumstances" where a person's life or safety is deemed at immediate risk; • With the owner's consent, to assist law enforcement with locating a vehicle that has been reported as stolen or missing; • With the owner's consent, to immobilize a vehicle that has been reported as stolen or missing; • With the owner's registration, request, consent, or activation, to facilitate certain services that rely on or utilize Geolocation Information such as traffic, map, navigation, driver behavior or geo-fencing features; • To perform business operations including research, development, and data analytics; • To provide warranty repair services; and

	• Any other purpose with the owner's consent or activation of vehicle functions or Connected Vehicle Technologies and Services that utilize Precise Geolocation Information. Honda reserves the right to use geolocation data to assist in locating and recovering the vehicle or communicating with the owner if they breach the terms of the agreements covering the leasing or financing of the vehicle (to the extent permitted by the owner's agreement with the lease or finance company). Honda does not use Precise Geolocation Information for marketing purposes or disclose it to third parties (excluding service providers) without owner's consent.
Data from Connected Vehicle Technologies and Services	• Provide the Connected Vehicle Technologies and Services; • Communicate with the consumer; • Evaluate and improve quality, performance, and design of vehicles, systems, and Connected Vehicle Technologies and Services; • Facilitate provision of software updates and enhancements to Connected Vehicle Technologies and Services; • Help maintain and provide alerts regarding the maintenance of the vehicle; • Provide customer service, sales, and product support; • Perform market research; • Facilitate safety, diagnostics, warranty, maintenance, recall, and compliance programs; • Develop future goods and services; • Prevent fraud or misuse; • Comply with legal and contractual requirements; • Engage in dispute resolution; • Protect our rights and property or the rights and property of others; • Help protect the safety of drivers or others; and • For any other purpose for which we obtain consent. Honda uses limited data (such as name and contact information) for marketing purposes. It does not use search history, voice commands, call history information, navigation settings, or similar data for marketing purposes.

b. Please identify every source of data collection in your new model vehicles, including each type of sensor, interface, or point of collection from the individual and the purpose of that data collection.

Honda collects vehicle and/or connected services data via: (i) the infotainment system, (ii) smart devices (e.g., mobile phone) that have a connected service application, such as HondaLink or AcuraLink, installed thereon (iii) connectivity systems (e.g., embedded TCU, Wi-Fi hotspot), (iv) vehicle sensors (e.g., odometer, tire pressure monitors, battery charge sensors, accelerometers, speedometer), (v) GPS unit, and (vi) customer usage of smartphone data.

c. Does your company collect more information than is needed to operate the vehicle and the services to which the individual consents?

Honda engages in deliberative processes outlined in the privacy principles to calibrate the collection of vehicle data to the business purposes for which the vehicle data is collected. These business purposes may extend beyond mere operation of the vehicle or provision of the connected services requested by the consumer. For example, Honda may use certain vehicle data to perform recall and warranty repair operations.

d. Does your company collect information from passengers or people outside the vehicle? If so, what information and for what purposes?

Honda does not intentionally collect data from passengers or people located outside the vehicle; however, incidental collection may occur if a passenger uses a connected service. For example, if a vehicle is involved in a crash and the passenger uses a connected service to speak with a Honda representative to obtain assistance, Honda may capture a recording of that conversation.

Many Honda vehicles are equipped with outward facing cameras that could capture video footage of persons outside the vehicle. These cameras help drivers view their surroundings (e.g., back-up and lane change images). All processing of video footage occurs on-vehicle and Honda does not collect such video footage.

e. Does your company sell, transfer, share, or otherwise derive commercial benefit from data collected from its vehicles to third parties? If so, how much did third parties pay your company in 2022 for that data?

Honda may disclose certain vehicle data to third parties who are not its service providers including Honda Motor Co., Ltd, Honda R&D Co., Ltd, Honda/Acura dealerships, its affiliate American Honda Finance Corporation ("AHFC"), and consumer goods or services companies such as satellite radio providers and connected vehicle data services and analytics platforms. Honda may also disclose vehicle data to third parties with the consumer's permission, such as disclosure to an insurance company in connection with an insurance discount program in which the consumer has enrolled. In limited circumstances, Honda may also disclose vehicle data to third parties with whom Honda has a relationship to facilitate research and development of products, services, infrastructure, and other technologies for Honda and others.

In 2022, Honda did not receive direct monetary compensation in exchange for vehicle data disclosed to third parties who are not its service providers.

f. Once your company collects this user data, does it perform any categorization or standardization procedures to group the data and make it readily accessible for third-party use?

Honda does not categorize or group identifiable vehicle data for the purpose of making it readily accessible for third-party use.

g. Does your company use this data, or data on the user acquired from other sources, to create user profiles of any sort?

Honda does not use vehicle or connected services data for "profiling" purposes at the individual level. For purposes of this response, Honda uses the California Consumer Privacy Act's definition of "profiling" meaning any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. Notwithstanding the foregoing, consumers can often customize a profile on their vehicle for settings such as seat position, favorite radio stations, and navigation favorite locations. Similarly, consumers may create a user profile within the HondaLink or AcuraLink applications that retains their contact information, communication preferences, associated vehicles, and other information necessary or advisable to make use of the applications more convenient.

h. How does your company store and transmit different types of data collected on the vehicle? Do your company's vehicles include a cellular connection or Wi-Fi capabilities for transmitting data from the vehicle?

Honda generally collects vehicle data via cellular connectivity, with potential software installation verification done via Wi-Fi. Honda stores vehicle data in its servers, the servers of its parent company Honda Motor Co., Ltd, or in cloud storage facilities operated by large internationally recognized cloud storage providers. Select Honda vehicles include Wi-Fi capabilities for consumer use that operate by creating a small Wi-Fi hotspot for the vehicle that transmits externally by cellular connection.

2. Does your company provide notice to vehicle owners or users of its data practices?

Honda maintains a comprehensive Privacy Notice, as well as a Vehicle Data Privacy Notice tailored to data collected by Honda from vehicles and connected services, on its website www.honda.com. The owner's manual provided with each new vehicle also contains information about how consumers can access these notices. Certain Honda vehicle models also provide in-dash instructions about how consumers can access the privacy notices.

3. Does your company provide owners or users an opportunity to exercise consent with respect to data collection in its vehicles?

Yes, with regard to certain data and services and as required by applicable law.

a. If so, please describe the process by which a user is able to exercise consent with respect to such data collection. If not, why not?

Honda provides geolocation-based services in many vehicles that require the consumer's consent for use including, without limitation, navigation, continuously updated traffic information, notification when the vehicle enters or exists a geofence, vehicle location, stolen vehicle location (may include disclosure to law enforcement if requested by the consumer), remote immobilization, and satellite radio services. Geolocation information may be shared with service providers and third parties (e.g., SiriusXM for satellite radio) in connection with the function of such services.

Honda also provides certain safety-related geolocation-based services in many vehicles such as automatic crash notification and emergency calling. Given the nature of these services, consumers provide consent for Honda's collection and disclosure of geolocation data (e.g., to first responders) when accepting the service rather than at the time of the crash or other safety-related incident.

Honda obtains consent for subscription-based services as part of the enrollment process and obtains consent for other data collections through in-vehicle and in-application interfaces.

Additionally, at each ignition ON cycle, a customer notification is provided which either links the user to data privacy settings or instructions on how to navigate to those settings. Points at which a consumer may exercise consent related to vehicle and connected services data collection and usage are explained in the "Your Choices Regarding Covered Information" section of Honda's Vehicle Data Privacy Notice.

b. If users are provided with an opportunity to exercise consent to your company's services, what percentage of users do so?

Honda does not track the percentage of consumers who exercise particular consent options.

c. Do users lose any vehicle functionality by opting out of or refusing to opt in to data collection? If so, does the user lose access only to features that strictly require such data collection, or does your company disable features that could otherwise operate without that data collection?

If a consumer does not provide, or withdraws, consent for data collection required for a particular connected service, the consumer cannot use such service. Honda does not, however, disable unrelated features or services based on the consumer's opt-out or failure to provide consent.

4. Can all users, regardless of where they reside, request the deletion of their data? If so, please describe the process through which a user may delete their data. If not, why not?

Complete deletion of all vehicle and connected services data is not currently possible within the United States. Federal regulations exist that require data from vehicles to be retained in certain circumstances (such as if a vehicle is involved in a crash). At a state level, consumer data laws

are not always consistent, including definitions of what types of data should be considered exempt from deletion when a vehicle owner submits a request to delete vehicle data.

In recent years, additional data retention requirements have been added by some states on vehicles equipped with highly advanced safety features. These new laws, combined with differences in scope and definition of existing state laws, can result in different outcomes depending on the jurisdiction of the request.

Additionally, a warrant or other court order may require the retention of data for a specific vehicle anywhere in the country. The details of the required retention of data can vary based on the state where the warrant or court order is issued.

Consumers may submit data deletion requests to Honda by toll-free phone and a website form as outlined in Honda's Privacy Notice. Honda evaluates each deletion request on a case-by-case basis.

Consumers are often concerned about deleting data that they sync to a Honda vehicle from their mobile phone such as their contact list and call history. This type of mobile phone profile data is stored in the on-board infotainment system and is not retrieved by, or capable of remote deletion by, Honda. To delete the consumer's mobile phone profile and associated data, the consumer must have physical access to the vehicle and follow the directions made available in their vehicle's owner's manual. Consumers may also contact Honda's customer care department if they have any questions.

Honda remains committed to complying with all applicable state and federal laws while also ensuring that data responsibility to our customers is a top priority for the company.

5. **Does your company take steps to anonymize user data when it is used for its own purposes, shared with service providers, or shared with non-service provider third parties? If so, please describe your company's process for anonymizing user data, including any contractual restrictions on re-identification that your company imposes.**

If Honda processes vehicle and connected services data for its own purposes, such as to facilitate recall and warranty operations and conduct research and development to improve its products and services, it generally does so in a form that is identifiable of a particular vehicle. Prior to disclosing vehicle data to a service provider or third party, Honda evaluates the business purpose for the disclosure and develops a business process that may, depending on the circumstances, involve anonymization of data disclosed. If a service provider or third party is provided anonymized data, it is Honda's policy to contractually prohibit such service provider or third party from reidentifying such anonymized data.

If a business unit desires to engage in a project involving anonymization or aggregation of vehicle or connected services data, the business unit must submit a proposal to Honda's Data Privacy Governance unit which will evaluate the proposed use of the data and the planned methods for anonymization or aggregation, and set relevant customized compliance controls and requirements within applicable laws and Honda's corporate policies. Such projects also must be approved by Honda's Architecture Review Board (a function of its Information Technology unit) and the Governance, Risk, and Compliance unit prior to commencement. Techniques for

anonymization that may be used include, but are not limited to, (i) replacement of identifiers with false identifiers or pseudonyms, (ii) substitution/deletion of values, and (iii) data generalization meaning modifying content to reduce the ability to determine individual characteristics (e.g., truncating GPS coordinates). Honda's goal is to ensure that any anonymization or aggregation which occurs is not reversable (i.e., Honda or the service provider/third party, as applicable, can no longer reasonably associate the deidentified data with a consumer).

6. **Does your company have any privacy standards or contractual restrictions for third-party software it integrates into its vehicles, such as infotainment apps or operating systems? If so, please provide them. If not, why not?**

If Honda integrates software provided by a service provider to Honda, Honda's policy is to impose on such service providers all necessary contractual restrictions on the collection and processing of vehicle data obtained via such software to comply with applicable laws and Honda's policies. For example, Honda prohibits the service provider from processing the data for the service provider's own commercial purposes, selling the data, or sharing the data for targeted advertising or cross-contextual behavioral advertising purposes.

Honda's in-vehicle infotainment systems may permit the consumer to use third-party web-based entertainment applications or connect their device for use of Apply CarPlay or Android Auto services. Honda does not collect data from the consumer's use of these applications or services, and does not have visibility into, or contractually regulate, the data which the third-party providers of these applications or services may collect. Use of such applications or services are governed by the contractual relationships between the consumer and the providers of such applications or services. Honda does not make vehicle usage data (e.g., telematics data) or data stored as part of the infotainment system (e.g., contacts, call history) available to such applications or services.

7. **Please describe your company's security practices, data minimization procedures, and standards in the storage of user data.**

Honda has taken most seriously the need to protect consumer privacy. Honda's Commitments Under the Privacy Principles:

- **Transparency**: Honda commits to providing Owners and Registered Users of connected vehicle services with ready access to clear, meaningful notices about its collection, use, and disclosure of Covered Information.

- **Choice**: Honda commits to offering Owners and Registered Users with certain choices regarding the collection, use, and disclosure of Covered Information.

- **Respect for Context**: Honda commits to using and disclosing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Owners and Registered Users.

- **Data Minimization, De-Identification & Retention**: Honda commits to collecting Covered Information only as needed for legitimate business purposes. Honda further

commits to retaining Covered Information for only as long as it determines necessary for legitimate business purposes.

- **Data Security**: Honda commits to implementing reasonable measures to protect Covered Information against unauthorized access or use.

- **Integrity & Access**: Honda commits to implementing reasonable measures to maintain the accuracy of Covered Information and further commits to offering Owners and Registered Users reasonable means to review and correct Personal Subscription Information that they provide during the subscription or registration process for Vehicle Technologies and Services.

- **Accountability**: Honda commits to taking reasonable steps to ensure that it and other entities that receive Covered Information adhere to the Privacy Principles.

Specific sections from the Privacy Principles addressing the security of information are listed below:

Section III covers Security Practices -

III. HOW WE COLLECT INFORMATION

- **From You**: We may ask you to provide us with Personal Information when you communicate with us online or offline including in connection with servicing, events, surveys, and marketing or promotional programs. You are not required to provide us your Personal Information; however, if you choose not to provide the requested information, you may not be able to use some of the features of the Sites or Services or we may not be able to fulfill your requested interaction. We may also capture your contact information, such as phone numbers and email addresses, when you contact us.
- **Third-Party Data Sources**: We may collect Personal Information from third-party data sources such as marketing agencies and partners, data brokers, analytics firms, government agencies, third-party businesses that provide products or services to our customers, and affiliates not governed by this Privacy Notice.
- **Dealerships**: American Honda and its dealers are distinct and independently owned and operated legal entities with separate privacy policies and obligations. We may collect Personal Information from dealerships with whom you interact. For example, if you purchase or service a vehicle at a dealership, the dealership may share your Personal Information with us.

Section V Covers Data Minimization -

Generally, we use Personal Information for business purposes, such as to:

- Provide you with access to and use of our Sites and Services;
- Facilitate or fulfill the information, products, or services you requested;
- Communicate with you about your products, services, or account;

- Market our products to you, including interest-based advertising;
- Market other companies' products or services to you;
- Operate information security and anti-fraud programs;
- Perform business operations, including the improvement of our products, Sites, and Services; conduct surveys, research, and data analytics; and other normal business activities;
- Facilitate the relationship you have with your independent Honda or Acura dealer;
- Respond to governmental and other legal requests or to comply with applicable laws;
- Communicate with you about your vehicle warranty, safety, and recall information;
- With your consent, to assist law enforcement with locating a stolen or missing vehicle (as further outlined in our Vehicle Data Privacy Notice); and
- As described to you at the point of collection, with your consent, or as otherwise required or permitted by applicable laws.

Standards in the storage of user data requires all stored personally identifiable information (PII) data to be encrypted on Honda databases.

a. Has your company suffered a leak, breach, or hack within the last ten years in which user data was compromised?

No user data collected from vehicles has been the subject of a leak, breach, or hack.

b. If so, please detail the event(s), including the nature of your company's system that was exploited, the type and volume of data affected, and whether and how your company notified its impacted users.

Not applicable

c. Is all the personal data on your company's vehicles encrypted? If not, what personal data is left open and unprotected? What steps can consumers take to limit this open storage of their personal information on their cars?

Vehicle data stored onboard is not encrypted. Data stored includes:

- Bluetooth ID of a phone which has been paired,
- previous navigation destinations,
- audio presets, and
- vehicle preferences and settings.

Phone data, navigation destinations, audio presents, and vehicle preferences and settings can be deleted via the infotainment system at any time.

Following the privacy guidelines, users can also choose not to upload this information to the system or can perform a reset of the device to clear stored data.

Event data recorder (EDR) data is not encrypted but is only accessible by a special EDR Retrieval tool used by law enforcement and manufacturers.

8. Has your company ever provided to law enforcement personal information collected by a vehicle?

Yes.

a. If so, please identify the number and types of requests that law enforcement agencies have submitted and the number of times your company has complied with those requests.

It is not possible to share a specific figure as Honda does not retain long-term records on requests related to an individual vehicle from law enforcement agencies. On average, however, Honda receives approximately one request per month. The majority of these requests are questions about connected functionality of a model/model year, rather than a specific vehicle. After receiving this information, most of these requests conclude without an ask for any specific vehicle's data.

b. Does your company provide that information only in response to a subpoena, warrant, or court order? If not, why not?

Historically, Honda has required a warrant or other court order to disclose personal information collected by a vehicle. However, recent changes to Illinois state law will soon require all automakers to implement a system that allows warrantless access to location data by law enforcement officers in certain circumstances. Honda is working with our service providers to comply with this new law.

c. Does your company notify the vehicle owner when it complies with a request?

As Honda historically requires a warrant or other court order for law enforcement requests for data, each request is evaluated on a case-by-case basis.

December 21, 2023

The Honorable Edward Markey
United States Senate
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey,

Please see the following in response to your recently submitted questions to Hyundai Motor America ("Hyundai") regarding our data practices and privacy policies. Please note that our Privacy Policy located on HyundaiUSA.com was updated.

1. **Does your company collect user data from its vehicles, including but not limited to the actions, behaviors, or personal information of any owner or user?**

   Hyundai vehicles equipped with Bluelink® include a telematics module (with 4G LTE connectivity for current models) and other in-vehicle technologies and services that may generate and transmit vehicle data. As part of the vehicle purchase process, owners and lessees can choose whether or not to enroll a vehicle in Bluelink® connected services. If Bluelink is not chosen, Bluelink's vehicle data is not transmitted to Hyundai.

   The telematics module is activated for vehicles enrolled in Bluelink® connected services and certain data generated by in-vehicle systems and technologies ("vehicle data") may be transmitted to and collected by Hyundai. Once a vehicle is enrolled in Bluelink® connected services, certain vehicle data collected by Hyundai from the vehicle may be linked with a vehicle's MyHyundai primary and secondary subscriber account.

   a. **If so, please describe how your company uses data about owners and users collected from its vehicles. Please distinguish between data collected from users of your vehicles and data collected from those who sign up for additional services.**

      Hyundai collects vehicle data from vehicles that are enrolled in Bluelink® connected services. The Hyundai Vehicle Technologies and Services Privacy Notice describes how Hyundai uses data collected from vehicles as part of the vehicle technologies and services.

      In general, Hyundai uses vehicle data in order to provide and support the vehicle technologies and services, enable emergency and roadside services, communicate with and respond to requests from owners, lessees and Bluelink® subscribers, analyze, develop and improve our vehicle technologies and services, and ensure the ongoing security, operation and functionality of the vehicle technology and services, as well as for safety, recall and warranty purposes. In some cases, vehicle data may be used to send alerts, recommendations and targeted offers to owners, lessees and Bluelink® subscribers, such as service-related offers and discounts provided in Vehicle Health Reports.

Hyundai Motor Company
Washington Office
660 N. Capitol Street, NW, Suite 800
Washington, DC 20001
T +1 202 629-1555
F +1 202 629-1071
www.hyundai.com

b. Please identify every source of data collection in your new model vehicles, including each type of sensor, interface, or point of collection from the individual and the purpose of that data collection.

Bluelink® equipped vehicles include various in-vehicle systems and technologies that may generate and transmit vehicle data, including onboard sensors and diagnostic tools, system-control modules), advanced driver assistance systems (ADAS), external-facing cameras and event recorders, as well as a GPS tracking unit, a telematics module, and the vehicle head unit.

As described in the Hyundai Vehicle Technologies and Services Privacy Notice, vehicle data, including location data and vehicle, performance and driving data may be generated and transmitted from a Bluelink® enabled vehicle to Hyundai. Vehicle data collected by Hyundai includes vehicle performance, diagnostic and service-related data, such as odometer, mileage, MPG and emissions data, diagnostic trouble codes, engine performance, and other diagnostic data; service and maintenance history; weather, temperature and other driving conditions; geolocation and trip data; fuel levels and refueling activity; battery levels and status; and other mechanical and operational data.

c. Does your company collect more information than is needed to operate the vehicle and the services to which the individual consents?

No. Hyundai collects vehicle data from vehicles that are enrolled in Bluelink® connected services. This includes vehicle data generated by in-vehicle systems and technologies to Hyundai that is needed to operate and enable the vehicle technologies and services, support advanced driver-assistance systems and other safety features, optimize, improve and develop vehicle technologies and services, enable communications, alerts, and over-the-air firmware updates to be sent to vehicles, and ensure the ongoing security, availability and integrity the services, as well as data that is used for quality, safety, warranty, and similar purposes.

In addition, certain vehicle data is collected pursuant to Hyundai's regulatory obligations, including under the Vehicle Safety Act.

d. Does your company collect information from passengers or people outside the vehicle? If so, what information and for what purposes?

No. For operational and safety purposes, some Hyundai vehicles include front and rear-facing external cameras, including backup cameras and cameras that support autonomous or semi-autonomous vehicle features, such as crash avoidance and adaptive cruise control. However, the camera images are not transmitted from the vehicle to Hyundai. Further, Hyundai does not collect vehicle data about individual passengers and is not able to identify or link vehicle data to particular passengers or people outside of the vehicle.

e. Does your company sell, transfer, share, or otherwise derive commercial benefit from data collected from its vehicles to third parties? If so, how much did third parties pay your company in 2022 for that data?

Hyundai does not sell vehicle data to data-brokers or third parties not associated with an opt-in service. Some of the vehicle technologies and services are provided or supported by third parties who may receive vehicle data as part of their provision of the particular feature, service or application, or in order to respond to a request from owners or users of the vehicle technologies and services. Third party services include, for example, Wi-Fi Hotspot, enhanced navigation and traffic services, and emergency and roadside services. When subscribers use or sign up for these services, data may be transmitted to or collected by these third parties to enable the provision of the respective services. Information about certain diagnostic trouble codes may also be shared with Hyundai franchised dealers in order to enable the dealers communicate with owners about and provide maintenance and services.

In addition, Bluelink® offers Driving Score and usage-based insurance (UBI), which is powered by Verisk Insurance Solutions. Certain vehicle data is transmitted to Verisk only for vehicle owners subscribed to Driving Score, so that Verisk can generate the Driving Score which is not shared by Hyundai with third parties other than Verisk. Drivers currently enrolled in Driving Score may also choose to separately opt in to receive offers and information about vehicle insurance discount and offers or request UBI quotes from participating insurers. Subscribers may also turn off these services at any time in their MyHyundai account, which stops transmission of vehicle data to Verisk. Hyundai may receive a fee per lead for insurance discount offers sent to drivers who have opted in to receive these offers and when a driver requests a UBI quote from an insurer and expressly authorizes and directs Verisk to provide their UBI data to the insurer.

f. Once your company collects this user data, does it perform any categorization or standardization procedures to group the data and make it readily accessible for third-party use?

Hyundai does not standardize or group vehicle data for purposes of selling it to third parties. Hyundai may make available certain vehicle diagnostic trouble codes available to the vehicle's assigned dealership in order to enable the dealer to communicate with the vehicle owner about service-related issues. Hyundai also makes the diagnostic trouble codes available to independent repair facilities as required by law or agreement.

g. Does your company use this user data, or data on the user acquired from other sources, to create user profiles of any sort?

As part of the Bluelink® services, enrolled subscribers receive monthly Vehicle Health Reports, which are generated from vehicle data and include subscription information, status check of key safety, electrical and powertrain systems, maintenance needed, outstanding safety recalls for vehicle, Driving Score (if

applicable). Vehicle Health Reports may also include personalized offers (*e.g.*, discounted oil change) and other news and updates.

h. How does your company store and transmit different types of data collected on the vehicle? Do your company's vehicles include a cellular connection or Wi-Fi capabilities for transmitting data from the vehicle?

Hyundai vehicles equipped with Bluelink® include a telematics module with 4G LTE connectivity for current models for vehicular telematics data. An active Bluelink® subscription is required for data transmission from and to vehicles.

Certain vehicle models and trims also include Wi-Fi Hotspot capability, which provides in-vehicle internet access. Wi-Fi Hotspot requires a separate activation and a subscription with Verizon Wireless®. Vehicle data is not transmitted to or collected by Hyundai via a vehicle's Wi-Fi Hotspot.

2. Does your company provide notice to vehicle owners or users of its data practices?

Yes, Hyundai provides notice to vehicle owners and users, as well as other consumers, of the rights and choices they have regarding their personal information and vehicle data and Hyundai's data practices.

Hyundai's online privacy hub: From the Hyundai Your Privacy at a Glance homepage (https://www.hyundaiusa.com/us/en/privacy-at-a-glance), consumers can find an overview of Hyundai's privacy practices and their privacy rights and choices, including with regard to vehicle data, and links to the Hyundai Motor America Privacy Policy, as well as the Hyundai Vehicle Technologies and Services Privacy Notice. Consumers can also access the Hyundai Personal Information Request portal where they can submit a privacy request (*e.g.*, to delete their personal information) and their MyHyundai privacy settings where they can apply certain privacy settings (*e.g.*, turn off Driving Score or opt out of marketing emails) and initiate a request to cancel or renew their Bluelink® services subscription.

Hyundai Vehicle Technologies and Services Privacy Notice: Hyundai provides the Hyundai Vehicle Technologies and Services Privacy Notice (https://www.hyundaiusa.com/us/en/vehicle-technologies-services-privacy), which describes how we collect, use, disclose, and process personal information related to the Bluelink® connected services. The Hyundai Vehicle Technologies and Services Privacy Notice is proactively provided during Bluelink® enrollment, posted on Hyundai's website, and linked to the MyHyundai mobile application. A link to the privacy notice is also made available on the vehicle's Monroney Label, in the vehicle Owner's Manual and glovebox materials, in the in-vehicle navigation screen, and from Hyundai's Your Privacy at a Glance homepage.

Hyundai Motor America Privacy Policy: Hyundai also provides consumers with notice of Hyundai's privacy practices through the Hyundai Motor America Privacy Policy (https://www.hyundaiusa.com/us/en/privacy-policy), which describes how we collect,

use, disclose and otherwise process personal information about consumers, as well as the rights and choices consumers have regarding their personal information.

3. **Does your company provide owners or users an opportunity to exercise consent with respect to data collection in its vehicles?**

   Yes.

   a. **If so, please describe the process which a user is able to exercise consent with respect to such data collection. If not, why not?**

      Owners and lessees can choose whether or not they want to enroll in Bluelink® connected services as part of the new vehicle purchase process. Hyundai obtains consent to collect vehicle data from Bluelink® subscribers as part of enrollment, as well when a subscriber logs into the MyHyundai mobile application for the first time.

      Once enrolled, vehicle owners and lessees can cancel Bluelink® services at any time to stop remote transmission of information from their vehicles, as set forth in the Hyundai Vehicle Technologies and Services Privacy Notice (available at www.hyundaiusa.com/us/en/vehicle-technologies-services-privacy#services), as well as the Hyundai Connected Services Agreement. Hyundai also offers Bluelink® subscribers and MyHyundai account holders a number of privacy options for opted-in services.

   b. **If users are provided with an opportunity to exercise consent to your company's services, what percentage of users do so?**

      Around 95% percentage of new owners or lessees enroll for Bluelink® services within the first month of purchase. 57% of the Bluelink-equipped vehicles produced since 2016 have an active Bluelink subscription.

   c. **Do users lose any vehicle functionality by opting out of or refusing to opt-in to data collection? If so, does the user lose access only to features that strictly require such data collection, or does your company disable features that could otherwise operate without that data collection?**

      If an owner/lessee declines to enroll in Bluelink® connect services, vehicles technologies and services that require an active telematics connection will not be available, including remote services, such as remote start and lock/unlock, car finder, geofencing and location alerts, as well as Automatic Collision Notification, over-the-air updates, vehicle health report, and automated collision assistance, enhanced roadside assistance and SOS emergency assistance. Certain vehicle services and safety features (where included) remain available, including in-vehicle navigation (not including name, point of interest and address search lookup features), backup camera and collision avoidance/lane departure warnings, event data recording are still available.

4. **Can all users, regardless of where they reside, request the deletion of their data? If so, please describe the process through which a user may delete their data. If not,**

why not?

Yes. Consumers, including owners, lessee, and Bluelink® subscribers, can request deletion of their personal data by Hyundai and submit access, correction, opt-out and other privacy rights requests to Hyundai by submitting a personal information request (a) online at https://owners.hyundaiusa.com/us/en/privacy/data-request.html, or (b) by calling Hyundai Customer Care Center at (800) 633-5151 (toll free). Under certain legal exemptions, we cannot delete certain data; however, we do not market to individuals who have requested deletion of their personal data.

5. **Does your company take steps to anonymize user data when it is used for its own purposes, shared with service providers, or shared with non-service provider third parties? If so, please describe your company's process for anonymizing user data, including any contractual restrictions on re-identification that your company imposes.**

   Yes, under certain circumstances Hyundai may de-identify or otherwise anonymize personal data. For example, in accordance with state privacy laws, Hyundai may de-identify personal data pursuant to a deletion request. In such cases, Hyundai has implemented safeguards to prevent reidentification, including contractual requirements and restrictions on relevant service providers and third parties.

6. **Does your company have any privacy standards or contractual restrictions for the third- party software it integrates into its vehicles, such as infotainment apps or operating systems? If so, please provide them. If not, why not?**

   Yes, as a signatory to the Alliance for Automotive Innovation's Consumer Privacy Protection Principles, we require contractual abidance to these principles. Hyundai has established privacy standards that include standard and regulatory-required privacy, security and commercial contract terms for third-party vendors, including software providers.

7. **Please describe your company's security practices, data minimization procedures, and standards in the storage of user data.**

   Hyundai has established and follows security standards for the storage of vehicle data. For example, vehicle data stored onboard are encoded and encrypted. Vehicle data, which is transmitted to Hyundai over a 4G LTE wireless network, is encrypted and subject to robust access controls and other security controls.

   a. **Has your company suffered a leak, breach, or hack within the last ten years in which user data was compromised?**

      No.

   b. **If so, please detail the event(s), including the nature of your company's system?**

      Not applicable.

c. Is all the personal data stored on your company's vehicles encrypted? If not, what personal data is left open and unprotected? What steps can consumers take to limit this open storage of their personal information on their cars?

All user personal data stored on Hyundai vehicles are encrypted and encoded. Consumers can delete vehicle data within the vehicle's head unit (*i.e.*, phone call history, contacts, navigation history).

8. Has your company ever provided to law enforcement personal information collected by a vehicle?

Hyundai is committed to maintaining the privacy of its customers. When Hyundai receives legal process for personal information collected by a vehicle, our legal team reviews the requests to ensure that the requests have a valid legal basis. If they do, we comply by providing data responsive to the request.

a. If so, please identify the number and types of requests that law enforcement agencies have submitted and the number of times your company has complied with those requests.

In the past three years, Hyundai has received approximately 60 requests pursuant to exigent circumstances, search warrants, customer consent, and subpoenas. We have provided data in response to approximately 50 of those requests.

b. Does your company provide that information only in response to a subpoena, warrant, or court order? If not, why not?

Non-public information about Hyundai customers will not be released to law enforcement except in response to appropriate legal process such as a search warrant, court order, or subpoena, or in response to an Exigent Circumstance. Under Hyundai's Exigent Circumstances policy and process, a verified law enforcement agent must attest to a claimed threat of imminent risk of death or serious personal injury.

c. Does your company notify the vehicle owner when it complies with a request?

Hyundai reserves the right to notify our customers when it complies with such requests, except where providing notice is explicitly prohibited by the legal process itself.

Hyundai remains committed to privacy and transparency for its customers. Thank you for your attention to this important topic.

Sincerely,

Robert R. Hood
Vice President of Government Affairs
Hyundai Motor

Hyundai Motor Company
Washington Office
660 N. Capitol Street, NW, Suite 800
Washington, DC 20001
T +1 202 629-1555
F +1 202 629-1071
www.hyundai.com

Kia Corporation Washington DC Office
601 New Jersey Avenue, NW, Suite 800
Washington, DC 20001
T (202) 503-1515

December 21, 2023

Sen. Edward J. Markey
255 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Markey:

Thank you for your November 30, 2023, letter to Kia America, Inc.'s ("Kia") Chief Executive Officer, SeungKyu Yoon, concerning Kia's policies and practices on data collection, use, and disclosure. Mr. Yoon has asked me to respond to your letter on his behalf. Kia appreciates your interest in protecting the privacy of consumers and the security of their data, as well as your recognition that advances in car technology—which often depend on user data—can bring new benefits, including improvements in safety and elevating the ownership experience.

Kia takes the privacy of its consumers and security of their data seriously, and shares many of your concerns. Kia is constantly looking for ways to improve its own privacy and security practices, and encourages others to do the same. For example, Kia is a member of the Alliance for Automotive Innovation ("Auto Innovators"), and has publicly committed to the Privacy Principles for Vehicle Technologies and Services, which contain significant—and what we consider to be critical—obligations for automakers related to transparency, choice, respect for context, data minimization, data security, integrity and access, and accountability. Kia is aware of reports suggesting that these principles are not being upheld by automakers. As Kia has concerns about the accuracy of that reporting, it appreciates the opportunity to bring greater clarity to topics raised in that reporting.

Kia also takes this opportunity to express its support for a cross-sectoral federal privacy law, which is necessary for ensuring that consumer privacy is protected in a consistent and meaningful way. Although Kia is regularly updating its own policies and practices as new laws take effect, Kia has concerns that the current patchwork of state laws creates inconsistent or conflicting privacy-related obligations. And some state laws, depending on how they are implemented, could also lead to unanticipated, negative consequences related to data privacy. For example, while the Massachusetts Data Access Law (passed via an after-market industry sponsored ballot initiative in 2020 and currently codified at Chapter 93K of the Massachusetts General Laws) claimed to provide consumers with more choice when it comes to repairing their vehicles by requiring open access to vehicle telematics data, in practice, the law runs the risk of forcing automakers to degrade their cybersecurity infrastructures in order to comply with the law. Moreover, the ballot initiative was intentionally written in the broadest possible way so that any entity—including those not subject to the same privacy laws and privacy principles by which OEMs are bound—can force consumers to hand over any data "related to" their vehicle, for an indefinite period of time. This places automakers in an untenable position where, on the one hand, they need to prioritize consumer privacy and data security, but on the other, need to make consumer data more accessible in ways that risk compromising the security of that data. Indeed, Kia believes that the Massachusetts Data Access Law is preempted by the National Traffic and Motor Vehicle Safety Act, and further believes that federal privacy legislation is needed now more than ever to address these complex challenges.

Kia Corporation Washington DC Office
601 New Jersey Avenue, NW, Suite 800
Washington, DC 20001
T (202) 503-1515

With all this in mind, Kia hopes that this response to your letter provides you and your staff with a clearer understanding of Kia's practices relating to data collected from its vehicles, and how Kia implements its ongoing commitment to transparency, customer choice, and data security.

I. Vehicle Data Practices

A core value of Kia is to empower its customers through transparency and choice. Through Kia Connect Services, Kia offers owners a range of optional, driver-convenience services, which are not required to operate a Kia vehicle but are designed to enhance the ownership experience. Depending on the vehicle, such services may include (i) Find My Car, which allows users to locate their Kia vehicles within a certain area; (ii) Remote Start with Climate Control, which remotely turns on and enables certain climate preferences within a Kia vehicle via the user's key fob or through the Kia Connect mobile application; (iii) Kia Digital Key, which allows a Kia Connect user to utilize a compatible smartphone or smartwatch to access, start, and drive their vehicle; (iv) Last Mile Navigation, which allows a Kia Connect user to receive the remaining directions to their requested destination on their phone if they have parked their Kia vehicle between six-tenths kilometers and two kilometers of the requested destination; (v) Connected Routing, which provides users with the most likely efficient route from the Kia vehicle's current location to the requested destination using real-time and historical traffic data; (vi) Stolen Vehicle Recovery and Vehicle Immobilization, which, subject to certain conditions, may allow Kia to locate a Kia vehicle reported as stolen and/or immobilize the Kia vehicle in the event it is reported as stolen and law enforcement requests immobilization in their recovery efforts; and several other features.

To obtain these and other services, an owner must enroll his or her vehicle in Kia Connect Services, which requires the owner to affirmatively agree to the Kia Connect Terms of Service and acknowledge the Kia Connect Privacy Policy. The Kia Connect Privacy Policy contains a description of Kia's data privacy practices and use of data collected from vehicles enrolled in Kia Connect Services. The policy is accessible through a variety of channels, including on the Kia Owner's Portal website located at www.owners.kia.com, and in the Kia Connect Privacy Portal located on the same website. Kia vehicles over the last several model years also provide a notice of vehicle data collection, with reference to the Kia Connect Privacy Policy, on the vehicle's infotainment screen upon start of the vehicle. Links to Kia's privacy policies are also included in email communications sent to customers. Kia is proud of the commitments it makes, and the transparency it provides, to consumers through its Kia Connect Privacy Policy.

---

1. As you may be aware, there is pending litigation over the validity of this law in federal court, which was filed in 2020 and included a trial that concluded in July 2021. Some OEMs, including Kia, have ceased providing connected car services for vehicles sold in Massachusetts while awaiting the court's ruling, which has not yet been issued.
2. Kia previously discovered an inadvertent collection of limited infotainment system-related data from certain vehicles. Kia did not use this data for any purpose, issued a software patch to address the issue, and implemented deletion procedures for affected data.

Kia Corporation Washington DC Office
601 New Jersey Avenue, NW, Suite 800
Washington, DC 20001
T (202) 503-1515

For vehicles enrolled in Kia Connect Services, Kia collects various data through a cellular connection. The data collected may vary depending on the vehicle model and year, and the particular services selected by the owner, but generally includes a Kia vehicle's geolocation data in the form of GPS coordinates and other vehicle measurements connected to a VIN, such as data elements relating to a vehicle's steering wheel, gear, odometer reading, battery charge levels, tire pressure, gas levels, acceleration and breaking, lights, ignition (including time it is turned on and off), air conditioner, and similar consumer controlled vehicle data points. Some vehicle models also transmit data regarding movement inside a locked vehicle and whether doors are left open, both of which enable various safety-related services that customers may request.

Kia uses the data collected through Kia Connect Services to provide requested services to customers, to respond to customer claims, and/or for quality and safety purposes. Kia does not sell or use the data for marketing purposes but may disclose limited data elements to service providers in order to provide services requested by the owner. This includes, for example, a roadside assistance service provider, who requires the vehicle's geolocation to assist with the user's issue, and vehicle voice assistant service providers. In addition, Kia may disclose limited data to certain third parties as part of its Crash Notification Assist service, including police, fire department, or ambulance providers, to enable such providers to find a user and respond to a user's emergency. Kia may also disclose data to third parties where the information is necessary to perform an audit, legal, operational, or other similar service for, or on behalf of, Kia, or where such information disclosure is necessary to comply with any applicable laws, regulations, subpoenas, court orders, warrants, governmental requests, or legal process. Over the past year, Kia received approximately 29 requests pursuant to legal process, mostly related to homicide investigations and other violent crimes, and, after reviewing the legal sufficiency of each request, provided some vehicle data in response to 25. When Kia does respond to such requests, Kia is often unable to notify the individual of its disclosure due to court orders prohibiting such notice.

Depending on the vehicle, users may be able to connect their mobile phones to the vehicle infotainment system through Bluetooth or a USB cable, and utilize features from their phone, such as Apple Car Play or handsfree calling. If the vehicle is enrolled by the owner in Kia Connect Services, Kia may collect limited personal information from a connected mobile device in the course of providing the Kia Connect Services. This information generally includes limited mobile device information, which generally describes mobile device identifier data, such as an IP address assigned to a phone, an International Mobile Equipment Identity number, a mobile device's hardware, including its phone type, mobile network information, and time of day. Kia

---

3. In accordance with federal law, all currently-produced Kia vehicles are equipped with an Event Data Recorder and an On-Board Diagnostic port that allows access to data from the engine control unit, engine transmission, the anti-lock braking and stability control systems, the steering system, the tire pressure monitoring system, and other mechanical systems. The data collected by these components is not transmitted to Kia, and can only be offboarded with proper tools and physical access to the vehicle.
4. A vehicle enrolled in Kia Connect Services will collect the same data, regardless of who is driving the vehicle or utilizing the Kia Connect Services.
5. Contrary to recent reporting by Mozilla, Kia does not collect information on sexual activity or orientation through Kia Connect Services. Mozilla's contrary assertion was based on a misreading and misinterpretation of Kia's privacy policies.

does not collect text messages, call logs, browsing data, or other similar types of information from a connected phone, and does not collect information from mobile phones connected in vehicles that are not enrolled in Kia Connect Services.

Depending upon the make, model, and year of the Kia vehicle, some users of Kia Connect Services are provided with a calendar sync feature, which allows them to link calendar event data from the native calendar application on their phone to their Kia vehicle. Calendar event information generally includes the date, timestamp, location, and title of a calendar event as provided in the native calendar application. If utilized, Kia collects this information to notify users through their Kia vehicle of upcoming calendar events.

Kia does not intentionally collect information from people outside the vehicle. However, certain Kia vehicles enrolled in Kia Connect Services have a 360 View feature, which allows customers to capture a limited number of photographic images from external cameras on all four sides of equipped Kia vehicles via the Kia Access app. This feature allows Kia Connect users to remotely examine the surrounding area of their vehicle, for safety. Images taken through the 360 View feature, which may capture people in proximity to the vehicle, are transmitted to Kia, but are not used or otherwise processed by Kia for any internal purposes, and the images are not disclosed to any individual or third party other than the Kia Connect user whose Kia vehicle took the image.

Kia does not use the data collected pursuant to Kia Connect Services to create user profiles or to infer characteristics about consumers. Nor does Kia deidentify, aggregate, or perform categorization or standardization procedures to group data collected from its vehicles for third-party use.

II. Kia Data Security Practices

Kia takes important steps designed to maintain the confidentiality, integrity, and availability of vehicle data collected pursuant to Kia Connect Services. For instance, Kia uses a private network server to store all data collected from its vehicles, and encrypts such data both in transit and at rest. In addition, Kia's contracts with service providers include data processing restrictions, which are written within the contracts themselves. Kia's agreement with its IT managed service provider, Hyundai AutoEver America ("HAEA"), also mandates that HAEA require all of its workers and subcontractors that process personal information on Kia's behalf to comply with applicable data protection and privacy laws. Kia also utilizes multiple third-party cybersecurity software to monitor for system vulnerabilities and to detect potential security events impacting stored vehicle data. Moreover, consistent with the principle of data minimization, Kia retains data collected by its vehicles in accordance with Kia's internal retention policies and procedures, as discussed in the Kia Connect Privacy Policy.

Kia continues to update its policies and procedures as existing laws change and new laws come into effect. For example, Kia is constantly monitoring the ever-evolving state of privacy laws in the United States. As more individual states provide consumers with new privacy rights and impose additional obligations on businesses, Kia takes the steps necessary to ensure

Kia Corporation Washington DC Office
601 New Jersey Avenue, NW, Suite 800
Washington, DC 20001
T (202) 503-1515

compliance. In the context of consumer rights requests, this includes updating external and internal policies and procedures, providing eligible consumers with a mechanism to exercise their rights, and responding to requests in a manner that complies with the law. For example, where required by state law, customers may submit requests for Kia to delete personal data through one of the two designated submission methods described in the Kia Connect Privacy Policy (as well as in the Kia Privacy Policy available on the main Kia.com website): (i) through Kia's online request portal or (ii) by calling a toll-free phone number. Subject to certain limited exceptions authorized by law, Kia deletes the requested data once it receives a valid deletion request.

* * *

In closing, Kia would like to again emphasize its commitment to protecting the privacy of its customers and their data, and is grateful to have had the opportunity to respond to your letter. Kia is pleased to enhance the safety and customer experience of Kia vehicles by offering owners optional services through Kia Connect Services. Whether it is automatically connecting a driver to emergency services after an airbag deploys, warming up the car in the morning before taking the kids to school, or providing the most direct route possible when there is a ten-hour road trip ahead, it is the Kia Connect technology that makes all of this possible. The majority of owners of eligible Kia vehicles take advantage of these types of features by enrolling in Kia Connect Service and consenting to the associated data collection.

Thank you again for allowing us to comment on this important topic, and we hope that you find this information helpful in better understanding Kia's policies and practices on data collection, use, and disclosure. If you seek additional information, please do not hesitate to contact me.

Sincerely Yours,

Christopher Wenk
Vice President of Government Affairs
Kia Corporation

6. As noted above, due to the Massachusetts Data Access Law, Kia Connect Services are currently unavailable in model year 2022 and newer Kia vehicles that are purchased or sold in Massachusetts.

December 21, 2023

The Honorable Edward J. Markey
United States Senate
255 Dirksen Office Building
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter to Mazda North American Operations President and Chief Executive Officer Tom Donnelly, dated November 30, 2023, regarding data practices and privacy policies. Mr. Donnelly has forwarded your letter to me and asked that I respond for Mazda.

Thank you again for the opportunity to discuss this matter.

Sincerely,

Daniel V. Ryan
Vice President – Government and Public Affairs
Dryan2@mazdausa.com

Mazda Motor of America, Inc. dba Mazda North American Operations ("Mazda" or "we") has received your office letter dated November 30, 2023, inquiring more about Mazda's privacy policies and practices regarding data collected from connected cars. Mazda is committed to being transparent with our consumers and understand our responsibility to safeguard data while implementing safety and the latest technology for the American public. Mazda appreciates the direct dialogue with your office and respectfully submits this letter in response to your inquiry letter.

Mazda fully understands the responsibility we have regarding safeguarding personal information and other data which may be generated by a connected car. First, Mazda's connected cars sold in the U.S. currently do not collect any biometric data. Further, all cars sold today in the U.S. by Mazda do not have interior cabin cameras. To enable certain safety features (such as lane assist, driver drowsiness alert, etc.), a few of our connected cars may rely on facial data point detection but all such data securely remain in the consumer's vehicle (similar to data locally stored on a consumer's personal computer) and is not transmitted outside of the car or remotely collected by Mazda. Mazda invests tremendous resources into our cybersecurity practices to secure data in connected cars. To date, Mazda has not experienced any material breach or hack into its connected car software and none requiring any consumer notices required under applicable law.

To enable other services for the consumer like "Find My Car", Mazda's connected cars collect event-triggered geo-location data only upon ignition off and when certain safety alerts are triggered by the vehicle and is not collected on an ongoing basis. Mazda collects a limited amount of data from our connected cars which we term "Default Data". Mazda uses such default data for various internal legitimate purposes such as safety analysis, research & development to create better cars, enhance security practices, comply with the law and to provide the services back to the consumer. Currently, Mazda only shares the connected car data with law enforcement with the written permission of the car owner or where Mazda is required to by law or court order, including the new Illinois Car Theft law HB2245/625 ILCS 5/4- 110-111 to take effect January 1, 2024. Mazda does not sell Default Data and, without the consumer's express prior written consent, does not share Default Data with third parties for such third party's use.

All the information provided in our letter is publicly published for our U.S. consumers on our general privacy policy found here (https://www.mazdausa.com/site/privacy) and our Car Connectivity Privacy Policy found here (https://www.mazdausa.com/site/privacy-connectedservices). Most of the connected car features and functionality require affirmative user set up. Additionally, the owner's manual for the specific model of connected car further describes which type of data must be collected to enable certain features and functionalities in the connected car.

Mazda North American Operations

1025 Connecticut Ave., NW Suite 910
Washington, DC 20036
TEL: 202.467.5097

Lastly, at all times Mazda provides our U.S. consumers with the option of turning off all connectivity to their Mazda cars. The process to make such election is described on our Car Connectivity Privacy Policy for the U.S. consumer (https://www.mazdausa.com/site/privacy-connectedservices).

Mazda is committed to full transparency for our U.S. consumers as to what data our connected cars collect and how we use it. Mazda is a voluntary member of the Alliance for Automotive Innovation and is a signatory to the Consumer Privacy Protection Principles for connected cars (https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf). In the development of all new connected car features, Mazda continues to comply with these Consumer Privacy Protection Principles as well as U.S. data privacy laws.

Mazda North American Operations

1025 Connecticut Ave., NW Suite 910
Washington, DC 20036
TEL: 202.467.5097

Mercedes-Benz

Jake Jones
Vice President - External Affairs

U.S. Senator Edward J. Markey (D-MA)
255 Dirksen Senate Office Building
Washington, DC 20510

January 11, 2024

Re: Mercedes-Benz Data Privacy Request

Dear Senator Markey,

On behalf of Mercedes-Benz, thank you for your Nov. 30 letter to Dimitris Psillakis, the President and Chief Executive Officer of Mercedes-Benz USA, LLC (MBUSA). We thank you for the opportunity to highlight our company's data privacy and protection policies and practices and how they are designed to effectively safeguard the privacy of our valued customers. MBUSA considers the safeguarding of data protection rights a high priority and key to retaining customer trust and loyalty while also delivering exceptional services and the world's most desirable vehicles. As such, data management and governance is an integral part of our identity as the foremost luxury brand in the world.

At MBUSA, our commitment to ensuring the highest standards of privacy protection for our customers who use our vehicles and related services is reflected in our data privacy policies which are based on the key pillars of customer choice, benefit, transparency, security, and ethics. Our polices are designed to be transparent, comprehensive, and in compliance with all applicable laws and regulations. Further, they are easily accessible by our customers at the point of service and via various platforms including our website (https://www.mbusa.com/en/mercedes-me-connect#how-to-activate), a privacy center located on our customer mobile application, Mercedes me Connect, the automotive head unit, and in the operator manuals. These various avenues provide customers readily available opportunities to learn about the information we collect, how MBUSA uses that information and options to exercise customer choice.

MBUSA is committed to using data responsibly and the following highlights key components of our approach to protecting customer data.

1. Transparency: MBUSA acts responsibly when collecting, storing and using data. Adequate transparency regarding the handling of data is indispensable. We want our customers to know what kind of data we collect, when and for what purpose. As noted, we provide them with extensive information including, for example, in sales literature, on the vehicle homepage, applications, and operating instructions/manuals.

2. Consent/Customer Choice: It is equally important to us that our customers have the choice which services they want to use and which data they want to share – either through consent, by contract or at the push of a button. This choice allows them to selectively enable services in the Mercedes me app and to disable them again at any time, for instance.
3. Data Security: High security standards for our customers similarly apply to data security in our vehicles to protect personal information collected through the MBUSA platform.
4. Compliance: Mercedes sets high standards for itself by implementing and complying with comprehensive data management and protection policies as well as all applicable local laws, including the General Data Privacy Regulation (GDPR) and California Consumer Privacy Act (CCPA).

As an automaker, we are cognizant of the many technological advancements in our industry which reinforce the continued need for robust data protection protocols. At Mercedes, our commitment to data protection does not begin at the point of sale but in the early phases of the automotive production process. When our engineers develop new services and products, they meet with their colleagues from the corporate data protection and legal departments so that they can identify the best solutions for ensuring the protection of customer data. Data protection is thus a key consideration throughout the auto manufacturing process.

Thank you again for providing MBUSA the opportunity to highlight the various policies and procedures in place to protect our customers' privacy. Should you or your staff have additional questions, please do not hesitate to contact me at Jake.Jones@mercedes-benz.com.

Best Regards,

Jake Jones

Jake Jones, Vice President of External Affairs
Mercedes-Benz North America

NISSAN
GROUP OF NORTH AMERICA

December 21, 2023
Our Ref: W-2351-B

Senator Edward J. Markey
255 Dirksen Senate
Office Building
Washington, DC 20510

Dear Senator Markey,

Nissan North America, Inc. ("Nissan," "the Company," "we" or "us") welcomes the opportunity to respond to your letter dated November 30, 2023 (the "Letter") and your questions regarding Nissan's consumer data privacy practices.

Nissan takes privacy and data protection for consumers and our employees very seriously. We are confident that our practices meet legal requirements, privacy concerns and public expectations, despite representations that were included in the Mozilla Foundation's recent report about Nissan and other automotive manufacturers. We can understand the reason for your outreach, as the descriptions in Mozilla's publication were articulated in a way very likely intended to raise alarm. We note from the outset, however, that most of the inflammatory statements in that document lacked context, did not accurately represent statements Nissan made in its Privacy Notice, or were based on a material misreading of the Privacy Notice.

When Nissan collects or shares personal data, we comply with all applicable laws and the *Privacy Principles for Vehicle Technologies and Services*,[1] and we prioritize transparency. Nissan is continually evaluating and recalibrating our approach to consumer privacy issues and disclosures to ensure that we are achieving our goal of transparently disclosing to our customers what personal information we collect and what we do with it so that individuals can make informed choices about how to manage data about them.

Strict compliance with various states' definitions and disclosure requirements constrains the clarity of the Privacy Notice.

Regarding our Privacy Notice,[2] it is important to note from the outset that while transparency to consumers is a goal of privacy policies, a patchwork of state privacy laws (the "Privacy Laws") largely dictates their content. As a result, consumers are not the only audience, and privacy notices continue to grow in length and complexity to address the secondary audience of state Attorneys General and regulatory bodies. This can impede clarity, because the definitions used in these laws – as well as their specific requirements – are not always consistent. The ideal way to avoid the tension between an understandable notice and a notice that meets lengthy and increasingly complex legal requirements would be for Congress to enact a national privacy law that provides a single source of consistent protections to consumers with clearer (and simpler) disclosure requirements that do not leave companies guessing at the best ways to marry different definitions together for consumers across the country.

In this particular case, it would seem beneficial to explain two apparent misunderstandings associated with our Privacy Notice. First, because California's CCPA also covers personal data collected in the employment context, we drafted the Privacy Notice to cover both consumers and employees in the same document. Health

[1] https://www.autosinnovate.org/initiatives/innovation/automotive-privacy
[2] https://www.nissanusa.com/privacy.html

diagnosis data or sexual orientation are not types of data that we regularly or actively collect from consumers. But they are types of data we nonetheless needed to list, due to the broad disclosure obligations and definitions present in certain Privacy Laws, to the extent that this information comes to us from employees to whom we provide benefit programs. We can assure you that our connected vehicles don't collect or infer these types of data and no part of our business actively seeks those types of data regarding consumers.

This potential misunderstanding will be rectified in a revised Privacy Notice which we expect to post by the end of the week. In that revised Privacy Notice, we have used more customer-friendly language to more clearly delineate the categories of personal data processed from various sources and outline more individualized uses. Further, we will fully separate our consumer Privacy Notice from our employee and contractor-specific notice, and information concerning personal data collected in the employment context no longer will appear in our consumer Privacy Notice. We anticipate that this will ameliorate some of your clarity concerns.

Another potential misunderstanding relates to what data we might "sell," as that term is defined in various state Privacy Laws. The current Privacy Notice includes a table that describes the "Business or Commercial Purposes for Collection" as well as third parties to whom the information is disclosed. There also is a separate table later in the Privacy Notice that specifically details the situations in which personal data is sold or disclosed for targeted advertising along with the relevant business purpose. In contrast to recent media reports, Sensitive Personal Data is not a category of data listed as something that Nissan sells or discloses for targeted advertising and, indeed, we do not.

We appreciate your encouragement for strong privacy protections in this industry and others. Nissan has spent considerable time and resources implementing a strong privacy program, and we are continually evaluating and adjusting our practices in order to responsibly balance business needs with responsible corporate stewardship. Nissan uses personal data either for purposes that are disclosed within the Privacy Notice or otherwise based on consent. We use typical personal information like identifiers (name, address, VIN, email, etc.) most commonly for various business and marketing purposes. For data that is more sensitive (e.g., precise geolocation from connected vehicles) and might require opt-in consent under various laws, we ensure that our uses are outlined in the terms users accept when they enroll, and that we tailor our uses in ways that consumers would expect due to the nature of the service.

We outline some of these in more detail in our responses below.

Nissan's Responses to your Requests

In addition to the above, please note the following requested information with regard to Nissan's data practices. For each, please note that the information may change rapidly and these responses are a snapshot as of the date of this response and are intended to address our regular practices at this point in time.

1. *Does Nissan collect user data from vehicles? What is the nature of the data collected, and how it is generated, used, transmitted, and disclosed?*

The nature of the data transmitted by and collected from a vehicle depends on a number of important factors; most importantly whether the customer has chosen to enroll the vehicle in connected services. If a customer is enrolled in connected services, telematics data is transmitted to Nissan from a cellular transmitter in the vehicle. If, however, a customer is not enrolled, data sharing is deactivated and Nissan does not collect telematics data from the vehicle in question. When a user opts into the service and enrolls, vehicles collect a variety of information about the functioning of vehicle components, environmental factors, and vehicle activity/location. Enrolled connected vehicles generate hundreds of data elements. The types of *personal*

data that connected vehicles generate are limited to items such as VIN, geolocation, and journey trip data. Examples of additional data types that might be collected by connected vehicles are the speed of the vehicle, seatbelt engagement, charging duration and location, and malfunction or diagnostic information. Most telematics data points are related to the vehicle itself rather than the driving of the car, and driver activity parameters like speed or cornering are not used to create profiles on drivers.

We disclose connected vehicle data, depending on the type, as allowed by law or with appropriate consent. Most disclosures of connected vehicle data are directly related to our business functions, which might be fulfilled by our vendors or Service Providers (as that term is contemplated by applicable Privacy Laws). Nissan has an intake process for all vendors which might receive Nissan confidential data or personal data. We do not categorize or standardize data to make it "ready" for commercial use. Connected car data flows to a platform which is designed to make distribution of data easier for consumption, but as noted above, most third party "disclosures" are to Service Providers with contractual restrictions in furtherance of our own business purposes and not for monetary remuneration.

2. *Does Nissan provide notice to vehicle owners or users of its data practices?*

Nissan provides notice to vehicle owners and users of its data practices in a variety of ways. These include through its Privacy Notice, at multiple online touchpoints, as well as in individualized enrollment terms or opt-in consent for the receipt of messages at the point of collection for personal data associated with various enrollments or account creation pages. We also provide Terms and Conditions for our apps (e.g., MyNissan) and connected vehicles services (e.g., NissanConnect Services) that address data practices.

3. *Does Nissan provide owners or users an opportunity to exercise consent with respect to data collection in its vehicles? Describe the nature of such consents, how commonly they are exercised, and the loss of any vehicle functionality associated with a failure to opt-in?*

Nissan's business depends on more than just owners operating vehicles, and not all types of data collection require consent. Ensuring that we have the data necessary to proactively address issues with our vehicles is a purpose that is directly related to customer satisfaction and safety. Nissan collects information much like other manufacturers do—in order to provide customer support, improve our products, perform contracts, market products and services and comply with the law. Because Nissan's services and obligations are robust, including the provision of data-reliant services to drivers and purchasers, providing data and services in the event of an emergency, etc., the information collected is also robust. We believe all such information collected is related to such services and obligations, fits within the descriptions found in the Privacy Notice, and is compliant with our obligations under applicable Privacy Laws.

Customers who enroll in connected services (and thereby consent to the terms) opt into data transmission, including data some Privacy Laws view as particularly sensitive, such as geolocation. If a car gets sold and there is no enrollment, or an enrollment terminates, we disable the data sharing function in the vehicle itself, but it will remain "connected" for purposes of things such as over the air software updates. Additionally, even enrolled users can limit data sharing to what is strictly necessary for Nissan to provide connected services through the in-vehicle menu.

There are no restrictions on consumers' ability to operate Nissan vehicles if they do not opt-in to sharing personal or sensitive personal data. They may not, however, be able to utilize connected vehicle or other services to the extent such services rely on precise geolocation.

4. *Does Nissan allow all users to delete personal data? What are the mechanisms by which they can do that?*

We provide personal data deletion rights to residents of states where that is a legal requirement, subject to stated exemptions from deletion in those Privacy Laws. Our process is clearly articulated in the Privacy Notice to ensure consumers can find the portal and freely exercise their rights. Unless and until federal privacy legislation is passed, we have concerns about selecting an arbitrary standard for providing individual rights for individuals in states without defined requirements.

Having said that, however, any vehicle owner has the ability to erase all data that is stored on their vehicle and perform a factory reset through on-board menus. Customers with our app can also perform a remote data wipe of the data stored on their vehicle from their mobile device.

5. *Does Nissan take steps to anonymize data? How do those apply to internal or external uses of consumer data?*

We have multi-disciplinary teams in place that are continually evaluating our data uses and disclosures in order to ensure that we are responsible stewards of consumer data and uses comport with the purposes we explain in our Privacy Notice. We have policies in place addressing purpose limitations, usage restrictions, and retention. Nissan also has a process to review any particularly sensitive data use cases in order to determine whether additional masking or anonymization might be appropriate.

With respect to external recipients of data, we limit the transmission to what is necessary or contracted for to provide the requested service. There are times when service providers or vendors receive only pseudonymized data or a data set that does not contain any personal data at all.

6. *Does Nissan have any privacy standards or contractual restrictions that are placed on third party recipients of our data?*

Nissan vets all of its vendors and holds Service Providers to contracted privacy and security standards that depend on the nature of the data they receive. In the case of any vendor that receives personal data, those companies must agree to terms ensuring adequate privacy and security protections for the data in question (many of which are mandated by state Privacy Laws).

Documentation that a particular company receives is fact specific and depends upon the nature of the service being provided and the data at issue, but Nissan has processes in place to ensure transfers of consumer data are flagged for review by appropriate parties and are well thought out in advance.

7. *Describe Nissan's security practices, data minimization procedures, and standards in the storage of user data?*

Nissan takes pride in our security practices and employs various technical, administrative, and organizational safeguards in order to protect consumer data from misuse or unauthorized access or acquisition. Nissan uses industry standard or better technical implementations such as encryption of our consumer data in transit and at rest, and vehicles also employ encryption technology. We also employ various administrative and organizational safeguards and access controls to limit access to necessary personnel and as appropriate for business need. Nissan currently has data usage policies and procedures in place that implicate data uses and

involve retention or minimization, or usage restrictions as a component of the analyses. Our policies include provisions stating that personal data is to be collected and used solely in line with legitimate stated purposes, must be limited to the minimum necessary to pursue the relevant purpose, and must be stored and retained only for the duration necessary, at which time it must be anonymized or deleted. We also have processes in place that are intended to facilitate cross functional evaluation of new data gathering, uses, and vendors.

Over the past 10 years, Nissan has not had a breach in the U.S. that created a material negative impact on business operations or resulted in access to user vehicle data.

8. Has Nissan provided law enforcement personal information collected by a vehicle?

Since 2020, Nissan has responded to law enforcement requests for customer vehicle data—which in some instances included location data—exclusively in response to valid compulsory process, and in fewer than 100 instances. Nissan's practice is to comply with all relevant privacy statutes, criminal procedure statutes, and valid court orders concerning disclosure of law enforcement requests to relevant parties. In most instances, where Nissan is responding to valid compulsory process to provide customer vehicle data, Nissan is precluded from notifying a customer of such requests by statute or court order.

In closing, we appreciate the opportunity to address these matters directly with you. We trust that this response shows that Nissan takes the concerns raised in your Letter seriously, and that Nissan has made a good faith attempt to describe its privacy practices in a way that is transparent and understandable to consumers, while at the same time making best efforts to create a proactive privacy program that complies with various state Privacy Laws.

Sincerely,

Tracy Woodard
Director, Government Affairs
Nissan North America, Inc.

January 12, 2024

The Honorable Edward J. Markey
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey,

Thank you for your letter dated November 30, 2023, regarding privacy and vehicles. I am responding on behalf of Mark Stewart, Chief Operating Officer for Stellantis North America.

Stellantis is committed to protecting customers' privacy and personal data, while also providing customers with clear information about this matter. Stellantis aims to maintain a relationship founded on trust by adhering to data protection rules and specific privacy principles including transparency, data minimization, purpose limitation, integrity and confidentiality, and privacy by design and by default.

Personal data also includes vehicle data, which may be collected with secure processes and used for a variety of purposes, but only when required or permitted by law or authorized by customers. This may include regulatory or safety purposes, such as to send recall notices, process recall and warranty claims, or identify potential safety issues that may require a remedy or recall. Data may also be used to support services that consumers have requested, including providing roadside assistance or locating lost or stolen vehicles.

Our Privacy Policy details our collection, use, and disclosure of personal information involving our websites, mobile applications, online services, and other touchpoints with consumers.[1] The Privacy Policy addresses issues that you raised in your letter, including but not limited to a description of information that may be collected from individuals, how that information may be aggregated and de-identified, and our security practices pertaining to data, among other topics.

Additionally, our Connected Services Privacy Notice explains our privacy practices related to optional connected services for our vehicles.[2] The Connected Services Privacy Notice clearly describes numerous topics for consumers, including how data may be collected in relation to connected services, the purposes of use and processing of such data, and relevant rights and choices that are available for consumers. This includes instructions for consumers about how they can disable certain services involving data, deactivate connected services, stop the collection of relevant data, and more.

Stellantis is a member of the Alliance for Automotive Innovation ("Auto Innovators"), which sent your office a letter in December describing steps automakers have taken to protect consumers' privacy,

[1] *FCA US Privacy Policy*, FCA US LLC (Jan. 1, 2023), https://www.chrysler.com/crossbrand_us/privacy.
[2] *FCA Connected Services Privacy Notice for Chrysler, Dodge, Fiat, Jeep, and Ram*, FCA US LLC (Jan. 1, 2023), https://www.driveuconnect.com/connectedservices/privacy.html.

Public Affairs NA
50 F Street, NW, Suite 710 – Washington, DC – 20001- USA
www.stellantis.com

including by adopting the Privacy Principles for Vehicle Technologies and Services.[3] Furthermore, Auto Innovators supports the enactment of a federal privacy law to ensure consistent and uniform privacy protections for consumers nationwide.

We welcome the opportunity to continue discussing with your office opportunities to protect consumers' privacy in the automotive industry and beyond. Thank you for giving us the opportunity to clarify our position on this important issue.

Sincerely,

Shane Karr
Sr. Vice President, Public Affairs North America

[3] *Consumer Privacy Protection Principles*, ALL. FOR AUTO. INNOVATION (Mar. 2022), https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

North American Subaru, Inc.
c/o Subaru of America
One Subaru Dr.
Camden, NJ 08103
856-488-8500
856-488-8669 fax

December 21, 2023

The Honorable Ed Markey
255 Dirksen Senate Office Building
Washington, D.C. 20150

Dear Senator Markey,

Thank you for your letter requesting information on Subaru's vehicle data practices and privacy policies.[1] Customer privacy is important to Subaru. Since the launch of its Starlink telematics service ("Starlink")[2] in 2015, Subaru has implemented strong privacy practices to protect customer vehicles from privacy harms and to put customers in control. The most important one is choice: customers must affirmatively choose to enroll their vehicle in the Starlink subscription service before any telematics data is collected by Subaru. Customers can then cancel their Starlink subscription at any time, which would immediately stop Subaru's collection of telematics data. And all customers, regardless of where they reside, can request the deletion of their vehicle data.

The data generated from a Subaru vehicle falls within three general categories: telematics data that is collected through Starlink, data that remains within the vehicle, and data transmitted from the vehicle to third-party infotainment application providers (such as satellite radio).[3] Starlink telematics data is collected only if a customer enrolls the vehicle in a Starlink subscription plan and consents to the data collection. Data that remains in the vehicle cannot be remotely accessed, and is retrieved locally by Subaru only in narrow circumstances and only after obtaining a signed written consent from the vehicle owner.[4] Data transmitted to third-party infotainment application providers is not accessible by Subaru and is subject to the third party's respective terms and conditions and privacy policies. In short, Subaru utilizes an "opt in" approach to data collection in which the customer remains in control.

Starlink Telematics Data Collection

Vehicle telematics data is not collected by Subaru unless the customer voluntarily enrolls the vehicle in Starlink. Starlink is not enabled by default. Rather, all customers must successfully enroll in Starlink before it can be activated. Before enrolling in Starlink, customers have an opportunity to review Subaru's privacy policy and the

[1] Subaru of America, Inc. ("Subaru") is the provider of Subaru's Starlink telematics services. Toyota Motor North America, Inc. ("Toyota") is the provider of telematics services to the Subaru Solterra. Telematics data collected from the Subaru Solterra is subject to Toyota's terms of use and privacy policy.
[2] Starlink is not associated with SpaceX's Starlink service.
[3] Subaru also receives vehicle maintenance and purchase data from retailers, but that data is not transmitted by the vehicle.
[4] Subaru retailers and third-party repair shops are able to access vehicle diagnostic and repair information.

Starlink terms and conditions, both of which explain Subaru's data collection practices. In addition, each new vehicle's Monroney Label provides a clear and conspicuous QR code that links to Subaru's privacy policy. This allows customers to review the privacy policy before deciding to make an offer to purchase a new vehicle. Customers can choose not to enroll in Starlink and avoid the collection of telematics data, and they can also cancel their Starlink subscription at any time. The decision to unsubscribe or not enroll in Starlink would not affect the vehicle's crash avoidance or crashworthiness capabilities. For example, Subaru customers—regardless of Starlink subscription status—would receive the safety benefits provided by EyeSight, which include Advanced Adaptive Cruise Control, Lane Departure & Lane Sway Warnings, Pre-Collision Breaking, and Pre-Collision Throttle Management. Customers who are not Starlink subscribers will still enjoy many of convenience and entertainment options available with Subaru vehicles, such as in-vehicle navigation, SiriusXM Radio, Apple CarPlay, and Android Auto.

After a customer enrolls the vehicle in Starlink and consents to the data collection, Subaru will then collect data from the vehicle to deliver the Starlink telematics services, further enhance occupant and vehicle safety, and improve the services we provide to our customers. Subaru collects this data when a customer initiates a Starlink service (such as remote vehicle locator, stolen vehicle recovery, or trip logs), when a Starlink service is triggered by the vehicle (such as automatic collision notification and assistance, rear seat reminder, or diagnostic alerts), and at ignition off events. Subaru does not collect any personal information from passengers except in the unfortunate circumstance when in-vehicle roadside assistance or emergency services are needed. This information is not collected by the vehicle, but rather by our call center to aid with the emergency response. Subaru does not collect personal information from people outside the vehicle.[5]

Subaru does not collect information beyond what is outlined in the privacy policy and Starlink terms and conditions.

Data That Remains in the Vehicle

Regardless of Starlink subscription status, Subaru vehicles collect certain data that remains within the vehicle. For example, data collected by the Driver Monitoring System ("DMS") stays solely within the vehicle. This data can include name information if the driver chooses to create a profile and enter a name. It can also include data that is used to warn drivers if they appear distracted. This data cannot identify any individual. Drivers can disable the DMS and delete a driver profile at any time. In addition, the event data recorder ("EDR") collects data upon the triggering of collision or near-collision events. EDR data would be accessed locally by Subaru only upon a separate written consent signed by the vehicle owner. Data used to support Bluetooth calling, Apple CarPlay or Android Auto stay solely within the vehicle. This data is accessible only to the driver and occupants, and only if the vehicle is paired with the phone. Drivers can delete phone profiles at any time, which will delete any data stored in the vehicle associated with that phone. Likewise, Subaru's in-vehicle navigation system stores location and trip data, and that data also remains solely within the vehicle. Drivers can disable in-vehicle navigation and delete historical trips at any time.

Vehicle Data Transmitted to Third-Party Infotainment Application Providers

Subaru also partners with third parties to provide infotainment applications to the vehicle owner. These relationships do not involve the sharing of Starlink telematics data. Each new vehicle is equipped with SiriusXM to receive satellite radio and a built-in WiFi hotspot provided by AT&T. Subaru does not collect any data

[5] Subaru's EyeSight system will record images outside the vehicle upon the triggering of automatic emergency braking or sudden braking, which, depending on the situation, may contain a still image of persons outside the vehicle. This data remains in the vehicle and is only collected by Subaru after obtaining the vehicle owner's signed written consent, and Subaru would have no way to identify anyone in the image.

concerning the use of SiriusXM. Customers have to enroll separately with AT&T to activate the WiFi hotspot. It is not on by default. Subaru does not collect any data transmitted through the activated AT&T WiFi hotspot. Rather, the use of and data collected by these services are subject to SiriusXM's or AT&T's terms of service and privacy policies. New vehicles are also equipped with Apple CarPlay and Android Auto. The use of those services are governed by Apple CarPlay's and Android Auto's respective privacy policies and terms of service.

Right to Delete Applies to All Customers

Subaru provides all customers with the right to delete their personal/vehicle information, including in states where Subaru is not legally required to do so. Customers can exercise this right by calling a toll-free number or submitting a "Right to be Forgotten" request through an easy-to-use online form: https://www.subaru.com/support/consumer-privacy.html. Upon verifying that the customer submitting the form is the vehicle owner, Subaru will process their Right to be Forgotten request and delete their vehicle information (subject to any exceptions provided by law).

Vehicle owners can clear all the data stored in the vehicle by performing a factory reset. Subaru also requires its retailers to perform a factory reset before a car can be resold.

Safeguarding Vehicle and User Data

Subaru safeguards the vehicle data in-transit and at rest. Starlink telematics data is transmitted only over a private cellular network.[6] It is encrypted during transit. All Starlink telematics data collected by Subaru is stored in an encrypted environment. Further, Subaru has committed to the Automotive Consumer Privacy Protection Principles that were established in 2014. In these Privacy Principles, Subaru committed to retaining personal information collected from a vehicle only as needed for legitimate business purposes, and implementing reasonable measures to protect this information against loss and unauthorized use. In addition, Subaru's systems are compliant with the New York Department of Financial Services Cybersecurity Regulations. Subaru also participates in the Automotive Information Sharing and Analysis Center (Auto-ISAC) that shares and analyzes intelligence about emerging cybersecurity risks to the vehicle.

Subaru carefully selects its service providers and partners who receive vehicle data. Where possible, Subaru anonymizes, pseudonymizes, or aggregates vehicle data. Subaru has contractual restrictions with its service providers prohibiting the ability to re-identify any anonymized or aggregated personal data. Subaru does not combine the Starlink telematics data with data collected by third parties to create user profiles. Subaru did not receive any compensation from third parties for Starlink telematics data in 2022.

Law Enforcement Requests

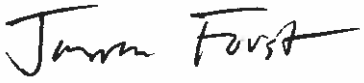
Other than certain carjacking scenarios that involve an imminent risk to human life, Subaru requires a search warrant, subpoena or court order from law enforcement before disclosing any vehicle data. Subaru does not have a policy to notify customers when it complies with a law enforcement request. Since 2021, Subaru has received approximately 30 law enforcement requests for various types of telematics data.

The cornerstone of Subaru's vehicle privacy philosophy is choice. Customers must voluntarily choose to enroll their vehicle in a Starlink subscription before Subaru collects any telematics data and can cancel their Starlink subscription at any time to stop telematics data collection. And all customers can request deletion of their vehicle data.

[6] Vehicles are also equipped with WiFi connection capabilities. This allows vehicle owners to connect to WiFi to download large navigation files and over-the-air updates. No vehicle data is transmitted to Subaru over WiFi.

Thank you.

Sincerely,



Joanna Foust
Vice President, Government and Regulatory Affairs
North American Subaru, Inc.

1 Tesla Road, Austin, TX 78725

January 8, 2024

The Honorable Edward J. Markey
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter dated November 30, 2023, and the opportunity to share information regarding Tesla's established privacy program and corresponding data protection measures. Customer data privacy is important to Tesla and embedded in each product, service, and feature by design.

Tesla's mission is to accelerate the world's transition to sustainable energy. To accomplish our mission, Tesla produces and sells five fully electric, light-duty zero emission vehicles (ZEVs)— the Model 3 midsized sedan, the Model Y compact sport utility vehicle (SUV), the Model S full-size sedan, the Model X SUV, and the Cybertruck—as well as one fully electric, heavy-duty ZEV: the Semi. To achieve the unparalleled performance of our vehicles—acknowledged by the Environmental Protection Agency (EPA) in its 2023 Automotive Trends Report for having the lowest carbon dioxide emissions (0 g/mi) and highest fuel economy (119 miles per gallon equivalent) of all large vehicle manufacturers in Model Year (MY) 2022—Tesla designs, develops, and manufactures all five ZEVs with advanced drivetrain electronics that make Tesla vehicles capable of our best in industry efficiency.

Privacy from day one

Customer privacy is enormously important to Tesla. To that end, Tesla has pioneered applying privacy preserving techniques to its vehicle engineering process (see www.tesla.com/privacy). To continuously improve our vehicles, privacy preservation allows Tesla to learn about how the vehicles are performing without being able to identify specific vehicles or the people using them by default. These important multi-layered measures include for example, transforming the information shared with Tesla such that we cannot reproduce the true data (e.g., pseudonymization, anonymization, encryption), as well as adding information to a dataset to prevent reverse engineering (known as 'adding noise' or 'differential privacy').

In practice, this means that from the moment a customer takes delivery, Tesla does not associate individual vehicle data with a customer's identity or account by default. As a result, Tesla does not have knowledge of a specific customer's activities, location or a history of where they have been.

Moreover, a customer's in-vehicle infotainment experiences are also protected. From features such as voice commands to surfing the web on the touchscreen to their AM radio listening habits (on the free, universally available (by default) TuneIn streaming app), customer information is kept private and secure, ensuring the infotainment data collected is not linked to the customers identity or account. Specifically, the vehicle is configured to only be eligible to associate data to the customer (i.e., personal data) in the occurrence of five enumerated events transparently described in Tesla's Privacy Notice (collision, request for repair, roadside assistance, remote service diagnosis, or customer consent). See Privacy Notice section "Information We May Collect", sub-section "1. Vehicle Data".

In addition, a copy of the vehicle data associated with a customer from those described limited cases, can be requested at any time (www.tesla.com/support/privacy), even if a customer is a resident of a US State that does not have a formal legal requirement for such a capability.

Transparent communication of our data protection measures

Our Privacy Notice (www.tesla.com/legal/privacy) is designed to provide transparency into our data practices in a format that is easy to read and navigate. The notice includes sections describing Tesla's approach regarding how we collect, use, share, and safeguard customer information in order to offer the most seamless vehicle and energy experience imaginable. As described in our Privacy Notice, we do not sell customer personal data to anyone for any purpose. The Privacy Notice is provided to consumers at various stages of interaction including for example, (a) during the checkout process before finalizing the vehicle purchase, (b) when a consumer creates a Tesla Account (see www.tesla.com/support/how-create-or-delete-tesla-account), (c) before downloading the Tesla mobile app from the app store, and (d) within the Tesla mobile app itself after its been downloaded. The notice is also easily accessible from a number of other locations, including the footer section of each page of Tesla's website (www.tesla.com), Tesla email communications, the Tesla vehicle owner's manual, as well as directly from the vehicle's center touchscreen (via Controls > Software > Privacy).

It can be challenging for companies to satisfy all readers when it comes to a Privacy Notice. Most customers likely seek a short summary that is easy to understand. While we aim to be concise, applicable regulations ask companies to meet our legal obligations by describing our privacy and data protection measures in sufficient detail. With that in mind, in addition to Tesla's Privacy Notice, supplementary web pages have been developed to further communicate Tesla's commitment to data privacy. For example, an overview of Tesla's privacy practices with a corresponding video via www.tesla.com/privacy, a privacy notice summary via www.tesla.com/legal/privacy, as well as a dedicated privacy support pages (such as www.tesla.com/support/privacy) to address frequently asked questions. Tesla also serves customers with pop-up notices using the vehicle's touchscreen when a feature involves data privacy (for example, requesting explicit consent to enable Sentry Mode, Tesla's security system).

In addition, we limit how, and with whom, we share consumer personal information. Depending on the consumer's purchase, service, or request, certain consumer personal information may be shared with service providers, affiliates, or third parties that the consumer authorizes. Entities that Tesla may share consumer personal information with includes, for example, a third-party payment processor (to complete a vehicle purchase), our business affiliate such as Tesla Insurance Services (to complete a consumer's request for insuring their vehicle), a third-party financial institution (if a consumer requests a quote for financing), vehicle repair estimates (when scheduling third party service for a vehicle), and other similar services requested by the consumer.[1]

Where Tesla contracts with a third-party vendor or service provider to process consumer personal information, the data relationship outlining information collected, processed, and how it must be handled, is formalized via a Data Processing Agreement (DPA). Tesla's standard DPA specifically enumerates, among other things, that the personal information shared is only provided for the intended limited business purpose, obligates the third party to provide the same level of privacy protection, grants Tesla the ability to take reasonable steps to ensure compliance or prevent unauthorized use, and requires the third party to notify Tesla if it can no longer meet its obligations.

[1] See 'Sharing your information' section for more details: https://www.tesla.com/legal/privacy#sharing-yourinformation.

With regard to US law enforcement agency requests for vehicle data, Tesla has established process guidelines to ensure our privacy commitment to customers is transparent and in line with expectations.[2] Tesla has a centralized process for receiving, tracking, processing, and responding to legal requests from government and law enforcement agencies. Requests require a valid subpoena, warrant, court order or similar legal instrument. When appropriate, Tesla raises objections to, challenges or rejects requests.

Synonymous privacy rights for customers regardless of their location

Tesla provides customers with the ability to exercise control over their personal data. This includes default settings which require consent, such as for fleet learning.[3] For example, in order for camera recordings to be shared with Tesla for the purpose of fleet learning, customers must consent to Data Sharing. Consent can be withdrawn at any time and controlled using the data sharing settings of the vehicle's touchscreen (Software > Privacy > Data Sharing).

Even if a customer chooses to consent, fleet learning camera recordings remain anonymous and are not linked to a customer's account or vehicle identification number (VIN), except in the occurrence of a safety critical event (such as a collision or airbag deployment). Therefore, absent a safety critical event, when Tesla receives a clip it does not know from which vehicle it came from. Further privacy measures include certain blurring of fleet learning recordings to obfuscate faces in the clip, which bolsters the security and protection of external camera data.

In addition, Tesla's privacy policies follow data minimization principles ensuring only limited camera data for fleet learning is collected. By adopting this framework, Tesla vehicles do not continuously record their environment nor are clips continuously shared with Tesla. Instead, fleet learning is only utilized using specific triggered events determined by Tesla. For example, to improve the recognition of traffic cones by Tesla's neural network, a request may be sent to some vehicles to find a clip using the vehicle's external cameras the next time it passes by traffic cones (i.e., the triggered event being the presence of a traffic cone). Absent a specific triggered event, however, Tesla vehicles do not share camera data.

In furtherance of Tesla's transparency principle, data which is held on Tesla servers and associated with a Tesla account or VIN may be requested by that customer at any time. Tesla provides individuals with the ability to request access to their personal data through multiple channels. As described in our Privacy Notice, these channels include:

- Submitting a data privacy request online via www.tesla.com/support/privacy
- Emailing Tesla's dedicated Data Protection Office
- Writing to us at Tesla Inc, Attn: Legal – Privacy, PO Box 15430, 240 Francisco Lane, Fremont, CA 94539, United States.

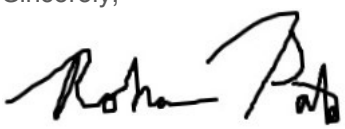
Similarly, a customer may also request deletion of their Tesla account and associated personal data at any time through multiple channels including: Online via https://www.tesla.com/contactus, via Tesla mobile app (Instructions available on https://www.tesla.com/support/how-create-or-delete-tesla-account), by emailing Tesla's dedicated Data Protection Office, or writing to us by mail: Tesla Inc, Attn: Legal – Privacy, PO Box 15430, 240 Francisco Lane, Fremont, CA 94539, United States.

[2] See Tesla Legal Process Guidelines (https://ts.la/ler-guidelines)
[3] Full list of features that require consent can be found by navigating on the touchscreen to Software > Privacy > Data Sharing.

TESLA

We hope this letter provides additional information regarding Tesla's privacy program as well as associated data privacy and protection measures.

Sincerely,



Rohan Patel
Vice President, Public Policy & Business Development

TOYOTA

TOYOTA MOTOR NORTH AMERICA, INC.

WASHINGTON OFFICE
325 7th STREET, NW, SUITE 1000, WASHINGTON, DC 20004

TEL: (202) 775-1700
FAX: (202) 822-0928

December 21, 2023

The Honorable Edward Markey
U.S. Senate
255 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Markey:

I am writing in response to the letter you sent to Toyota Motor North America, Inc. ("Toyota"), dated November 30, 2023, regarding our vehicle data handling practices.

Toyota's approach to consumer privacy and handling vehicle data is based on our organizational culture – "The Toyota Way."[1] "*Respect for People"* is a pillar of The Toyota Way and has long guided our approach to data privacy. As you may know, Toyota played an instrumental role in efforts by the auto industry in 2014 to develop a self-regulatory code of conduct to govern the collection and use of vehicle data. Toyota pledged to meet or exceed the commitments contained in this code of conduct, known as *Automotive Consumer Privacy Protection Principles* ("Privacy Principles"), which establish baseline protections for data collected through in-car technologies. For example, the Privacy Principles require automakers to provide clear and meaningful privacy notices to consumers and to use vehicle data in ways that are consistent with the context in which the data was collected.

Toyota has built upon the work of the Privacy Principles in various ways. Reflecting our culture of *Respect for People*, when the California Consumer Privacy Act ("CCPA") took effect in 2020, Toyota voluntarily extended CCPA consumer privacy rights to all United States consumers, instead of only providing them to California residents. Data-driven technological advances have delivered—and will continue to deliver—significant benefits for our customers, including enhanced safety, improved vehicle performance, and a better driver experience. Toyota likewise has continued to find innovative ways to be transparent with consumers about our data handling practices and to provide them with the information they need to make informed choices. Toyota informs consumers through numerous notice methods, including through owner's manuals and a publicly-available web-based privacy portal, the "Privacy Hub," that contains comprehensive and user-friendly information about our data collection and handling practices and consumers' privacy rights. Another consumer tool is the Data Privacy Portal on the Toyota and Lexus apps which provides users transparency and control over how their connected vehicle data is used – including options to share data where beneficial to them including the ability to easily de-enroll should they choose. Toyota regularly updates its privacy notice regarding our handling of vehicle data, the

[1] *See* https://www.toyota-global.com/company/history_of_toyota/75years/data/conditions/philosophy/toyotaway2001.html.

"Connected Services Privacy Notice," which can be found at https://www.toyota.com/privacyvts and https://www.lexus.com/privacyvts. In addition, Toyota installs a sticker in plain sight in all new vehicles sold in the United States that explains in clear and simple terms that data collection in the vehicle is active at the time of sale and explains how the consumer can terminate data collection.

We provide the below responses to your questions. The information provided in these responses is current, based on the information Toyota's headquarters had as of the time of this response.

1. **Does your company collect user data from its vehicles, including but not limited to the actions, behaviors, or personal information of any owner or user?**
    a. **If so, please describe how your company uses data about owners and users collected from its vehicles. Please distinguish between data collected from users of your vehicles and data collected from those who sign up for additional services.**
    b. **Please identify every source of data collection in your new model vehicles, including each type of sensor, interface, or point of collection from the individual and the purpose of that data collection.**
    c. **Does your company collect more information than is needed to operate the vehicle and the services to which the individual consents?**
    d. **Does your company collect information from passengers or people outside the vehicle? If so, what information and for what purposes?**
    e. **Does your company sell, transfer, share, or otherwise derive commercial benefit from data collected from its vehicles to third parties? If so, how much did third parties pay your company in 2022 for that data?**
    f. **Once your company collects this user data, does it perform any categorization or standardization procedures to group the data and make it readily accessible for third-party use?**
    g. **Does your company use this user data, or data on the user acquired from other sources, to create user profiles of any sort?**
    h. **How does your company store and transmit different types of data collected on the vehicle? Do your company's vehicles include a cellular connection or Wi-Fi capabilities for transmitting data from the vehicle?**

Response to Question 1: All new Toyota and Lexus vehicles sold in the United States are capable of transmitting data to and from the vehicle to support services on the vehicle ("Connected Services"). Toyota may collect, use, store, and share the following types of data from vehicles, as described in further detail in the "Collect & Use," "Store," and "Share" sections of the Connected Services Privacy Notice. We provide below a summary of our data processing practices.

- Vehicle Information. Toyota may collect the vehicle's make, model, year, body type, VIN and other information linked to the vehicle so we can verify the vehicle type and provide Connected Services.

- Location Data. Toyota may collect and use the vehicle's latitude and longitude and/or other location information ("Location Data") to deliver Connected Services and for quality confirmation, data analysis, research, and product development. We may record and transmit Location Data when a consumer contacts us for emergencies, roadside assistance, stolen or missing vehicles, missing persons, and destination services, or when automatic collision notification is triggered on the vehicle (when an airbag sensor is activated or a severe rear-end collision occurs). We may share Location Data with emergency responders, law enforcement, affiliates and service providers acting on our behalf, as well as any compatible third-party services or device the consumer authorized to receive Location Data.

- Remote Data. At last ignition off, Toyota may collect the "Real Time Status" of the vehicle (i.e., vehicle location, status of powered doors, windows, hood, trunk, sunroof, hazard lights, odometer reading, oil life, fuel economy, trip distance, and distance to empty). We may share this data with the consumer's compatible connected device.

- Driving Data. Toyota may collect driving behavior data ("Driving Data") which includes the acceleration and speed at which the vehicle is driven, use of the steering and braking functionality in the vehicle, and vehicle operation data (e.g., sensor readings). Driving Data is used to deliver Connected Services, and for quality confirmation, data analysis, research, and product development. We may share Driving Data with our affiliates and business partners so we can work together to provide Connected Services and for product improvement.

- Profile Data. If the vehicle is equipped with the ability to create and save user profiles, Toyota may collect in-vehicle preferences (i.e., a consumer's linked Apple Music or Amazon Music account), favorites (i.e., a consumer's saved locations on maps or preset radio stations), and usage history (i.e., a consumer's search and routing history on maps). This information is used to deliver Connected Services tailored to the consumer's profile.

- Interior Image Data. If the vehicle is equipped with advanced driver assistance features, interior, driver-facing camera(s), and sensors are used to collect information about the status of the driver and other vehicle inhabitants ("Interior Image Data"). Interior Image Data is used to ensure safety and vehicle control, such as checking that the driver is paying attention to the road and wearing a seatbelt before enabling certain automated driving operations. Interior Image Data will only be stored on the vehicle and is not transmitted to Toyota.

- Exterior Image Data. If the vehicle is equipped with advanced driver assistance features, external camera(s) and sensors are used to record and evaluate the vehicle's surroundings ("Exterior Image Data"). This data is used to improve and develop advanced driver assistance and safety features. Toyota may share Exterior Image Data with our affiliates and business partners to help improve and develop advanced driver assistance features. Please note that Toyota applies privacy-enhancing technology, as explained in our response to Question 5, to protect the privacy of individuals outside the vehicle.

- Facial Geometric Features. If the vehicle is equipped with face scanning features, interior, driver-facing camera(s) and sensors are used to scan the driver's face and create a computer-generated code linked to the driver's facial features ("Facial Geometric Features"). This data is not readable by humans, and it is used to verify the driver's identity and load their saved user profile on the vehicle. Facial Geometric Features will only be stored on the vehicle and are not transmitted to Toyota. Toyota does not collect a drivers' heartbeat in any current production model.

- Vehicle Health Data. Toyota may collect "Vehicle Health Data," which may include odometer readings, fuel level, oil life, Diagnostic Trouble Codes, and related data from the vehicle's on-board diagnostic system to identify malfunction events. We may use Vehicle Health Data to tell a consumer when the vehicle is due for maintenance or service; to provide vehicle health reports (maintenance and malfunction statuses, and service campaign and safety recall information) and vehicle alerts (notifications when the vehicle reports malfunction-related events); and to contact the consumer. We may share Vehicle Health Data with the consumer, with our parent company and affiliates, and with the consumer's compatible connected device.

- Multimedia Screen Data. Toyota may collect and use "Multimedia Screen Data" (how a consumer interacts with the infotainment screen) for quality confirmation, data analysis, research and to improve functionality and product offerings, and to provide Connected Services. We may share Multimedia Screen Data with our parent company for quality confirmation, data analysis, research and to improve functionality and product offerings and compatible third-party services and devices.

- Voice Recordings. If anyone in the vehicle speaks with the response center for purposes of emergency services, roadside assistance, stolen vehicle locator, destination assist, or any other reason, Toyota may collect "Voice Recordings" to deliver Connected Services and for quality assurance. We do not extract an identifier template, such as a voiceprint, using Voice Recordings. We may share Voice Recordings with our service providers in order to provide Connected Services.

- Voice Services. In select models with hands-free control of in-car multimedia and a linked smartphone, Toyota may collect Voice Recordings and Voice Recording transcriptions to deliver Connected Services and to improve the quality and performance of voice services.

- Device Data. If consumers use the Toyota or Lexus vehicle applications or enroll in Wi-Fi connectivity services, Toyota may receive the consumer's device ID and other information about the consumer's device and app in order to provide these Connected Services.

- Account Information. When a consumer enters or updates their name, address, phone number, email address, language preference and other information linked or directly related to the consumer, Toyota creates or updates the consumer's account so that we can provide Connected Services and communicate with the consumer. We may share this data with emergency responders, our affiliates, our parent company, and our service providers.

In the context of vehicle ownership, Toyota only sells (as that term is defined under applicable privacy laws, such as the CCPA) consumers' personal information in one instance: to a third party who provides a satellite radio subscription service, in order to offer consumers a free trial of satellite radio subscription service and for related post-trial marketing campaigns. Consumers may opt-out of such sale or sharing of their personal information on Toyota's Privacy Hub.

You can learn more about Toyota's data handling practices in connection with vehicle data in our Connected Services Privacy Notice.

2. **Does your company provide notice to vehicle owners or users of its data practices?**

Response to Question 2: The Connected Services Privacy Notice provides notice to consumers regarding Toyota's handling of vehicle data. The Privacy Hub provides further information to consumers on Toyota's privacy practices and consumers' privacy rights and a place where consumers can exercise their privacy rights.[2]

In addition to the Connected Services Privacy Notice, Toyota provides the following additional notices to consumers regarding our handling of vehicle-originated data:

- Toyota and Lexus Apps. When consumers download and enroll to use Toyota and Lexus vehicle applications, they can access information regarding data transmission from the vehicle, a link to the Connected Services Privacy Notice, and an opportunity to accept or decline transmission of data from the vehicle. While using the Toyota or Lexus app, users obtain similar information and choices about their vehicle data via the Data Privacy Portal.

- In-Vehicle Sticker. New Toyota and Lexus vehicles contain a sticker placed near the infotainment screen or SOS button, which states that vehicle data transmission is on, the purposes for such transmission, and refers consumers to the Connected Services Privacy Notice if they would like more information. The sticker also states that vehicle data transmission can be disabled by pressing the vehicle's SOS button, which connects the driver to a customer service representative. Toyota presented this sticker to the Federal Trade Commission in 2019, as an example of Toyota's commitment to transparency related to data collection.

- Owner's Manual. Toyota provides information about the transmission of data from the vehicle and how to opt-out of transmission in the owner's manuals for Toyota and Lexus vehicles that are equipped with Connected Services.[3] For example, the relevant owner's manuals disclose that the vehicle is equipped with sophisticated computers that will record certain data, and to learn more, consumers can visit the Connected Services Privacy Notice.

[2] Toyota's Privacy Statement, https://www.toyota.com/support/privacy-notice/, is found on all Toyota websites and applies to consumer data that does not originate from a vehicle, including information Toyota collects as part of its technology platforms (e.g., websites, interactive features, applications, and mobile applications), offline, and from other parties. Lexus provides a similar Privacy Statement on its website, https://www.lexus.com/privacy.

[3] *See*, *e.g.*, 2023 Toyota Tundra Owner's Manual, available at https://www.toyota.com/owners/warranty-owners-manuals/digital/tundra/2023/.

- Post-Sale Email Communications. After the purchase of a new Toyota or Lexus vehicle equipped with Connected Services, a consumer receives a post-sale email communication that describes the data Toyota collects from the vehicle. The post-sale email communication also includes the web address for the Connected Services Privacy Notice.

3. **Does your company provide owners or users an opportunity to exercise consent with respect to data collection in its vehicles?**
    a. **If so, please describe the process by which a user is able to exercise consent with respect to such data collection. If not, why not?**
    b. **If users are provided with an opportunity to exercise consent to your company's services, what percentage of users do so?**
    c. **Do users lose any vehicle functionality by opting out of or refusing to opt in to data collection? If so, does the user lose access only to features that strictly require such data collection, or does your company disable features that could otherwise operate without that data collection?**

Response to Question 3:
Toyota informs consumers through numerous notice methods, including through owner's manuals and a publicly-available web-based privacy portal, the "Privacy Hub," that contains comprehensive and user-friendly information about our data collection and handling practices and consumers' privacy rights. Another consumer tool is the Data Privacy Portal on the Toyota and Lexus apps which provides users transparency and control over how their connected vehicle data is used – including options to share data where beneficial to them including the ability to easily de-enroll should they choose. Toyota regularly updates its privacy notice regarding our handling of vehicle data, the "Connected Services Privacy Notice," which can be found at https://www.toyota.com/privacyvts and https://www.lexus.com/privacyvts. In addition, Toyota installs a sticker in plain sight in all new vehicles sold in the United States that explains in clear and simple terms that data collection in the vehicle is active at the time of sale and explains how the consumer can terminate data collection.

Also, under certain circumstances, Toyota provides consumers with a separate notice and an opportunity to exercise consent. For example, unless Toyota obtains the consumer's consent, we will not provide the consumer's Location Data or Driving Data to other parties for their own purposes or use the Location Data/Driving Data for our marketing purposes. Some of Toyota's Connected Services that rely on the collection of vehicle data are services to which the consumer subscribes and are therefore subject to the consumer's opt-in consent. To see more about how we use, store, share and secure data from vehicles equipped with connected services, please go to our "Connected Services Privacy Notice" at https://www.toyota.com/privacyvts or https://www.lexus.com/privacyvts.

- Wi-Fi Connectivity. Certain vehicles offer a trial of Wi-Fi connectivity, which provides up to ten compatible devices with in-vehicle wireless connectivity. If a consumer provides opt-in consent, Toyota may disclose the consumer's Account Information, Vehicle Information (e.g., VIN) and Device Data to a Wi-Fi provider for Wi-Fi connectivity services.

- Clean Assist. Owners of eligible vehicles may choose via the Toyota or Lexus vehicle application to opt-in to the "Clean Assist" program, through which Toyota is participating in environmental initiatives, such as the *California Air Resources Board's Low Carbon Fuel Standard* program to reduce California transportation emissions. If a consumer opts-in, the consumer's Vehicle Health Data, Location Data, and Account Information will be used in order for Toyota to match the electricity from the vehicle charging with eligible incentive programs, such as California-sourced Renewable Energy Certificates.

- External Vehicle Video Capture. Owners of certain vehicles equipped with "Toyota Safety Sense" may also opt-in to participate in "External Vehicle Video Capture," a feature which uses sensors and/or image data from the vehicle's exterior to help improve automated driving operations and safety features for Toyota vehicles, as well as to develop high-definition maps. If a consumer opts-in, the External Vehicle Video Capture feature may share the consumer's Vehicle Health Data, Location Data, and Exterior Image Data, and Exterior Image Data with our affiliate Woven by Toyota to help improve automated driving operations and safety features for Toyota vehicles. Woven by Toyota may also use de-linked Exterior Image Data of certain road features (e.g., images of road signs) and their locations to develop high-definition maps.

- Usage-Based Auto Insurance. If a consumer chooses to opt-in for usage-based insurance products and services, the consumer's Driving Data and Location Data will be used to deliver usage-based insurance services, and for quality assurance, analysis, research, and product development. If a consumer provides express prior consent, Toyota may share the consumer's Location Data and Driving Data with our affiliates and non-affiliated insurance companies to provide usage-based insurance information and offers.

- Face Identification. Certain vehicles equipped with an interior, driver-facing camera use sensor and/or image data from the vehicle's interior to scan the consumer's face when the consumer opens the vehicle's door. If the consumer opts-in and links their user profile using the in-vehicle "Setup Face" process, the "Face Identification" feature may use the consumer's Facial Geometric Features and Profile Data to verify the consumer's identity and load the saved user profile on the vehicle. Facial Geometric Features will only be stored on the vehicle and are not transmitted to Toyota.

Regarding feature functionality, those features requiring data collection will lose functionality if the customer disables data transmission.

4. **Can all users, regardless of where they reside, request the deletion of their data? If so, please describe the process through which a user may delete their data. If not, why not?**

Response to Question 4: Consumers can exercise privacy rights related to their personal information, including deletion requests, through the "Your Privacy Choices" link in the footer of Toyota's website homepage, or by calling Toyota's toll-free number. Consumers may also call or send a letter to Toyota through the contact methods listed under "Contact Us" in the Connected Services Privacy Notice if they have any questions or need assistance. Toyota has voluntarily extended consumer privacy rights, including deletion requests, to all United States consumers. Once Toyota receives a deletion request, we will confirm receipt of the request within 10 business days, verify the consumer's identity, and respond to the request within 45 calendar days (unless we notify the requestor of a 45-day extension). Toyota also gives consumers the option to decline all wireless data transmission from their vehicle through the "Data Privacy Portal" in the Toyota and Lexus vehicle applications or by speaking with customer service, which can be reached through the press of a button in the vehicle.

5. **Does your company take steps to anonymize user data when it is used for its own purposes, shared with service providers, or shared with non-service provider third parties? If so, please describe your company's process for anonymizing user data, including any contractual restrictions on re-identification that your company imposes.**

Response to Question 5: When utilizing vehicle data for certain research and development purposes, Toyota may use the following techniques:

- Aggregation. Vehicle data may be aggregated so that the aggregated datasets relate to a broad group of vehicle owners. The aggregation process often involves a large population pool (such as all vehicles of a certain model year) so that the aggregated data is not linked or reasonably linkable to any consumer, household, or vehicle.

- Obfuscation. Exterior Image Data capturing faces and license plates goes through obfuscation. In the very limited cases where un-obfuscated images are required for research and development, strict access and security controls are in place.

- Masking. Vehicle data may be masked, so that the masked dataset does not identify a specific consumer, household, or vehicle.

Toyota employs individuals with training and knowledge of the aforementioned techniques during the research and development process.

6. **Does your company have any privacy standards or contractual restrictions for the third-party software it integrates into its vehicles, such as infotainment apps or operating systems? If so, please provide them. If not, why not?**

Response to Question 6: In its regular course of business, Toyota enters into a standard contractual addendum with service providers that have access to connected vehicle data. The addendum contains data privacy and security terms to protect consumers' data in accordance with best practices and requirements under applicable privacy laws.

7. **Please describe your company's security practices, data minimization procedures, and standards in the storage of user data.**
    a. **Has your company suffered a leak, breach, or hack within the last ten years in which user data was compromised?**
    b. **If so, please detail the event(s), including the nature of your company's system that was exploited, the type and volume of data affected, and whether and how your company notified its impacted users.**
    c. **Is all the personal data stored on your company's vehicles encrypted? If not, what personal data is left open and unprotected? What steps can consumers take to limit this open storage of their personal information on their cars?**

Response to Question 7: Toyota maintains a risk-based cybersecurity program that relies on technical, physical, and administrative controls. As described in our Connected Services Privacy Notice, we designed the Connected Services technology to provide data security based on fundamental security principles such as confidentiality, integrity, and availability. It employs layers of defense to drive strong safeguarding practices, such as, where appropriate, code and design reviews, security testing, firewalls, intrusion detection systems, signing and encryption.

We also actively engage with the security community. We operate a coordinated disclosure program that can be found at www.hackerone.com/toyota and play a leading role in the Automotive Information Sharing and Analysis Center (Auto-ISAC) since we helped create it in 2015. We also participate in international standards setting bodies for vehicle cybersecurity.

We maintain incident response plans that govern our response to cybersecurity incidents. This includes a process to respond to an incident impacting personal information, and addresses how we provide required or voluntary individual notifications.

As discussed above, the Connected Services Privacy Notice describes the use of personal data in the vehicle context. Relevant user manuals explain how user data can be deleted from a vehicle. Toyota maintains data retention policies that ensure compliance with all relevant legal obligations.

8. **Has your company ever provided to law enforcement personal information collected by a vehicle?**
    a. **If so, please identify the number and types of requests that law enforcement agencies have submitted and the number of times your company has complied with those requests.**
    b. **Does your company provide that information only in response to a subpoena, warrant, or court order? If not, why not?**
    c. **Does your company notify the vehicle owner when it complies with a request?**

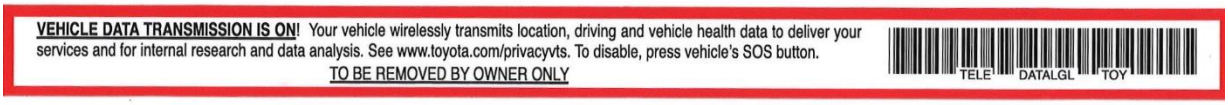
Response to Question 8: The Connected Services Privacy Notice describes the circumstances in which we will share vehicle data with law enforcement, including subject to user consent, appropriate legal process, or exigent circumstances. Toyota has received relevant requests from law enforcement and responded in accordance with this notice and governing law, including with respect to applicable non-disclosure requirements.

Sincerely,

Stephen J. Ciccone
Group Vice President
Government Affairs

Attachment

Toyota/Lexus data collection sticker



VOLKSWAGEN

GROUP OF AMERICA

VW CREDIT, INC.

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

December 21, 2023

The Honorable Edward J. Markey
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey:

Thank you for your Nov. 30th letter to our President and CEO, Pablo Di Si, regarding vehicle data privacy and security. We provide our responses below on his behalf. Consumer privacy is extremely important to Volkswagen Group of America, Inc. ("VWGoA"). We comply with applicable privacy laws, and we value providing transparency in our customer notices regarding our collection and use of data. In support of these principles, VWGoA has been a signatory to the Alliance for Automotive Innovation's ("AFAI") Consumer Privacy Protection Principles ("Principles") since their 2014 establishment.

In response to your questions, please see the information provided below. Please note that this information is with respect to our main U.S. vehicle brands, Volkswagen and Audi. Because your questions appear to focus on new technology, which is not typically available in older vehicle models, our responses generally relate to our newer model vehicles. In addition, we support the positions taken by the AFAI in their letter regarding your inquiry to the automakers, which supports a comprehensive federal privacy law that preempts the current patchwork of state laws, and that responds generally on behalf of the industry to the criticisms in the Mozilla Foundation report.

1. Does your company collect user data from its vehicles, including but not limited to the actions, behaviors, or personal information of any owner or user?

Yes, VWGoA's newer vehicles are equipped with technology that collects and stores, within the car, certain vehicle data, including geolocation information and information about certain user interactions with the car. These vehicles also are equipped with cellular gateways that, if enabled, may transmit a subset of that data to VWGoA's back-end platform, depending on the circumstances, the services, the models, and the brand. The data may be collected in a de-identified format, but the data may also be associated with a VIN or other identifier, which can be associated by VWGoA with a person or account. See response to Question 1b for further detail.

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

a. If so, please describe how your company uses data about owners and users collected from its vehicles. Please distinguish between data collected from users of your vehicles and data collected from those who sign up for additional services.

As noted above, applicable law likely considers most data collected from a vehicle associated to a VIN to be "personally identifiable information" because a VIN could be associated by us to a person. However, data associated with a VIN does not necessarily convey anything "about" owners and users. For example, signals conveying data about vehicle parts do not necessarily relate to the driver's or passengers' behavior. Still, at least some of the data derives from owners' and users' operation of the vehicle or its functions, and therefore could convey information about owners and users.

VWGoA uses personally identifiable information collected from vehicles for the following purposes: to provide customers with our products and services; for internal business purposes such as evaluating the usage, performance and safety of our vehicles; for legal, safety and security purposes; for marketing our products and services; and for other purposes at the individuals' request, such as providing vehicle data to a service offered by a third party. VWGoA may also de-identify data for these purposes after collection when it is not necessary for the use case to retain the VIN. VWGoA may initially collect data from the vehicles in a de-identified format, or it may de-identify or aggregate such data and use it for all of the above purposes, or to derive revenue. These general uses of collected data are detailed in our public brand privacy statements (available at vw.com/privacy and audiusa.com/privacy). Additionally, please see response to Question 7, below, regarding our data minimization practices.

Limited data may be collected from some of our cars before a consumer has subscribed to connected services, but that collection is specific to safety or driver-initiated functions that come standard on some cars, such as e-calls initiated by an accident or the ability to locate your car through our mobile app. That data is limited to information directly relevant to those functions.

However, most data can only be collected after our consumers affirmatively signed up for additional services and have reviewed and acknowledged our terms of service and privacy notices.

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

For vehicles enrolled in our connected services programs, VW Car-Net or Audi Connect, data is collected and used to provide those services. Data may also be collected for the purposes and in the manner outlined above, except, as required by the Principles, VWGoA will obtain affirmative consent from consumers to use geolocation information, biometrics, or driver behavior information (as defined by the Principles) as a basis for marketing or sharing such information with unaffiliated third parties for their own purposes.

b. Please identify every source of data collection in your new model vehicles, including each type of sensor, interface, or point of collection from the individual and the purpose of that data collection.

In our newer vehicles, data can be collected and stored within the car for a short period of time, from a variety of sensors or interfaces. See below for general categories and examples of data within each category:

- **VIN / IP-address / OEM-specific identifier**;
- **Connected services registration information:** certificates that enable connected services to interact with the vehicle (*e.g.*, remote lock/unlock, over the air updates), and device IDs for quick pairing of mobile devices to infotainment system;
- **Sensor Perception:** for example, status of a sensor, sensor-related information, lidar data, radar data, ultrasonic data, microphone data, weather/temperature/visibility/light conditions, tire pressure, sensor fusion data;
- **Vehicle Functions and Data:** for example, signals coming from parts or functions (activated by the driver, like climate controls, lights, door locks, seat buckles, mirror position, windshield wipers, or braking, or automatically such as lane assist, Speed Adaption System, Park Assist), such as behavior of a function, function status, internal function signals, hardware/software equipment and versions, certificates, battery charge level/condition, steering angle, steering wheel angle, acceleration values, pedal position, mileage data, speed, engine revolutions, rotations speed of wheels, status warning lights, information about the user's interactions with the native infotainment system, etc.;
- **Location Data:** GPS-position and direction of travel;

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

- **Derived vehicle data:** Data that is derived within the car from other signals, such as, for automated systems, information on object class (*e.g.*, vehicles, pedestrian, cyclist, animals, traffic lights, traffic signs), position/orientation as well as kinematic quantities;
- **Image / Video Data:** recordings by built-in externally facing cameras of the vehicle;
- **Meta data:** for example, calibration data, configuration data, error/diagnose data, time and date;
- **Derived Driver behavior/status:** for example, fatigue, response time, advanced distraction recognition.

As noted in response to Question 1, above, only a subset of this data will be collected from the car through the cellular gateway at any point in time. That subset will change depending on the service or use case for which the data is required. See response to Question 1a, above, for uses of data collected from the car.

c. Does your company collect more information than is needed to operate the vehicle and the services to which the individual consents?

Yes. VWGoA collects data for the purposes described in response to Question 1a, above.

It is worth noting that the Company's ability to collect data from our vehicles is critically important to support product safety and quality, and to improve services, as explained in the AFAI's December 2023 Memo to Interested Parties: "vehicle telematic data supports the proper functioning of a vehicle and its onboard computer systems. It produces information that affirmatively improves safety, can help support compliance with government safety rules, and enables a range of (optional) connectivity and personalization features for customers." Vehicle data collected by safety systems can also be useful to regulators like the National Highway Traffic Safety Administration in overseeing and investigating vehicle safety.

d. Does your company collect information from passengers or people outside the vehicle? If so, what information and for what purposes?

Some of VWGoA's cars have externally facing cameras, and technology in this area is quickly evolving. Backup cameras in existing cars do not store images, but rather provide a live image stream to assist with parking and reversing. In our newer cars, VWGoA may use images

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

collected from externally facing vehicle cameras used for automatic driver assistance system ("ADAS") functions, to a) support collision avoidance or other safety-related systems or features on the vehicle; b) for a public safety-related purpose (*e.g.*, vehicle theft, vehicle vandalism, vehicle crash, or to support infrastructure improvements) pursuant to any required consent by the vehicle owner or lessee ; c) for quality control, product improvement, or research if the vehicle owner or lessee has provided affirmative consent, or if the images and/or videos are obscured so as to not show a person's face or other identifiable physical characteristic.

Some of VWGoA's cars may collect information from passengers, such as when a passenger interacts with the infotainment screen. In many cases, VWGoA is aware only of the likely presence of a passenger, not their identity, such as the signal that indicates that a seat belt is buckled in a passenger seat.

e. Does your company sell, transfer, share, or otherwise derive commercial benefit from data collected from its vehicles to third parties? If so, how much did third parties pay your company in 2022 for that data?

VWGoA transfers data collected from vehicles to third-party service providers in relation to all of the uses referenced in our response to Question 1a. VWGoA may disclose data collected from vehicles to third parties who are not acting as service providers as defined by applicable law, such as our authorized dealers or other parties. These transfers are detailed in our privacy statements, and to the extent they include identifiable data, are subject to affirmative consent and/or subject to opt-out rights, as applicable. In most cases (*e.g*., in relation to authorized dealers), these transfers are not in exchange for revenue, but do provide commercial benefit. For example, we provide data to our authorized dealers to allow them to better service our vehicles, which improves customer safety and loyalty. Any revenue that is derived from these transfers represents an extremely small percentage of Company's overall revenue.

f. Once your company collects this user data, does it perform any categorization or standardization procedures to group the data and make it readily accessible for third-party use?

As noted above, data may be collected in a de-identified format, or we may in some cases remove identifiers from a dataset to de-identify data or eliminate certain fields from a dataset if not needed for the business purpose, *e.g.*, by abstracting GPS location to an area, rather than a specific location.

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

g. Does your company use this user data, or data on the user acquired from other sources, to create user profiles of any sort?

VWGoA uses some collected data to create profiles in order to better identify products and services likely to be of interest to groups of customers (*e.g.*, customers whose leases are almost expired or customers' vehicle maintenance patterns.) We do not use sensitive personal information to build customer profiles.

h. How does your company store and transmit different types of data collected on the vehicle? Do your company's vehicles include a cellular connection or Wi-Fi capabilities for transmitting data from the vehicle?

VWGoA brands contract with mobile network operators ("MNOs") to provide connectivity services. Separately, vehicle owners can subscribe directly with the MNO for Wi-Fi services in the car through the cellular connection.

2. Does your company provide notice to vehicle owners or users of its data practices?

Yes, through our brand-specific privacy statements referenced in the vehicle and online as well as within our mobile applications (myVW and myAudi), and upon signing up for connected services (Car-Net or AudiConnect). See vw.com/privacy and audiusa.com/privacy for our disclosures.

3. Does your company provide owners or users an opportunity to exercise consent with respect to data collection in its vehicles?

a. If so, please describe the process by which a user is able to exercise consent with respect to such data collection. If not, why not?

Yes. Many of our vehicles incorporate a "Privacy Mode" in the HMI, or dashboard interface, which offers consumers choices around the use and sharing of location and other vehicle data. For other vehicles, when subscriptions to connected services are cancelled, data collection is turned off. Additionally, consumers can exercise choice by enrolling or unenrolling in certain

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

data-driven services through the mobile apps (*e.g.,* myVW allows customers to enroll or unenroll from remote services and make selections within the DriveView program).

b. If users are provided with an opportunity to exercise consent to your company's services, what percentage of users do so?

We are unable to ascertain the percentage of users who opt out of data collection through Privacy Mode because we do not collect that signal continuously or in real time and the Mode can be turned off or on multiple times a day.

c. Do users lose any vehicle functionality by opting out of or refusing to opt in to data collection? If so, does the user lose access only to features that strictly require such data collection, or does your company disable features that could otherwise operate without that data collection?

VWGoA does not disable features or functionality unrelated to connected data when a vehicle owner opts out or chooses not to opt in to a connected services program. However, opting out of services, or opting out of data collection in relation to services, prevents the use of those services. For example, opting in to collection of location data is needed to provide navigation services built into connected service offerings as well as other location-based services, such as trip statistics and boundary alerts.

4. Can all users, regardless of where they reside, request the deletion of their data? If so, please describe the process through which a user may delete their data. If not, why not?

We will delete data collected from vehicles as provided by state law, so long as the requestor is not an active connected services subscriber and the deletion request is not incompatible with our provision of these services, or if the data is de-identified or otherwise exempted from deletion under applicable law (such as security or compliance). To avoid confusion about how such data deletion impacts active services, some of which are safety-related services, we require that owners first end their connected service subscriptions before submitting requests for vehicle data deletion.

Deletion requests are available through our data subject rights portal (privacy.vwgoa.com) or by calling our toll-free number in all states with data subject rights.

We currently offer deletion rights to residents of states where these rights are required, because



VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

those states have clear exceptions and limitations that balance consumer rights with the Company's ability to operate.

5. Does your company take steps to anonymize user data when it is used for its own purposes, shared with service providers, or shared with non-service provider third parties? If so, please describe your company's process for anonymizing user data, including any contractual restrictions on re-identification that your company imposes.

Yes. VWGoA minimizes the data shared with service providers and limits the retention of personally identifiable information maintained by service providers on our behalf to the extent commercially feasible. Our service provider contracts require that data be deleted or destroyed (or returned to us) at the end of an engagement rather than allowing ongoing retention or use of de-identified data. With respect to third parties (whether service providers or non-service providers) that receive de-identified and/or aggregated data, we contractually require that they do not attempt to re-identify the data.

Internally, our data de-identification process depends on the type of dataset and our intended use of the de-identified data. The process may include, for example, removing all personal identifiers and location information; aggregating data; truncating or obfuscating data like VINs; or reducing data precision so that location data is only provided to determine region or city.

6. Does your company have any privacy standards or contractual restrictions for the third-party software it integrates into its vehicles, such as infotainment apps or operating systems? If so, please provide them. If not, why not?

Third parties who develop integrated software for our vehicles are required by contract to meet privacy and security standards consistent with accepted practices within the industry. These requirements meet or exceed the requirements of law, and include concepts such as privacy-by-design principles, organizational controls, employee training, and identity/access management.

7. Please describe your company's security practices, data minimization procedures, and standards in the storage of user data.

For the protection of our customers and the public at large, the Company does not publicly disclose detailed information regarding its cybersecurity practices. However, cybersecurity is a topic that our

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

company takes seriously, and the Volkswagen Group continuously endeavors to further enhance across our products and services. With the increasing connectivity and intelligence of today's vehicle control systems, our company's design processes are continuously improved to address evolving cybersecurity risks. Vehicle design practices incorporate a wide range of regulatory requirements and best practices collected from a global landscape to account for the Volkswagen Group's international markets. Within this framework, a multitude of cybersecurity requirements, such as those outlined in the United Nations Economic Commission for Europe's Regulation 155 ("R155"), are accounted for in the vehicle's design. These design practices help our company to continuously update our vehicle designs to handle our customers' data responsibly, and VW and Audi have implemented cybersecurity management systems, *see R155*, that extend cybersecurity into both internal processes and supplier relationships. These processes enable the integration of a risk-based approach to cybersecurity within the vehicle design to guide the implementation of appropriate protections within vehicle systems, including protection of user data. This management system includes concepts such as vulnerability management, IT application and vendor security assessments, software security compliance audits, penetration testing, and identity/access management.

VWGoA strives to deploy data minimization principles to the extent commercially feasible in relation to collection of personally identifiable information from vehicles. Collection use cases are reviewed to determine whether the use case is achievable with de-identified, rather than personal, data, and to determine whether all of the data to be collected is necessary for the requested use case.

a. Has your company suffered a leak, breach, or hack within the last ten years in which user data was compromised?

Volkswagen Group of America is not aware of any cybersecurity incident in relation to VWGoA systems in the last ten years that resulted in the unauthorized access to personal information requiring notification to consumers or regulators under applicable law. We are aware of ransomware attacks or other cybersecurity incidents that have impacted certain VWGoA suppliers, but are aware of no cybersecurity incidents impacting suppliers that required VWGoA to notify consumers or regulators under applicable law, with the exception of the incident VWGoA reported to consumers and regulators on or around June 10, 2021.[1] To date, VWGoA is unaware of any cybersecurity

[1] *See, e.g.*, VWGoA's June 10, 2021 notification to Massachusetts' Attorney General and the Office of Consumer Affairs and Business Regulation, publicly available on the Commonwealth's website at "Data Breach Notification Letters June 2021 | Mass.gov."

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

incident related to VWGoA vehicles that has resulted in the unauthorized access to personal information.

b. If so, please detail the event(s), including the nature of your company's system that was exploited, the type and volume of data affected, and whether and how your company notified its impacted users.

Please see above.

c. Is all the personal data stored on your company's vehicles encrypted? If not, what personal data is left open and unprotected? What steps can consumers take to limit this open storage of their personal information on their cars?

Our technical development teams are responsible for categorizing all data stored or exchanged between engine control units in the vehicles based on the various cybersecurity risks identified between the responsible function owner and the cybersecurity advisors within our company. That risk-based function-by-function analysis identifies data that should be encrypted or protected from tampering, and such measures are then deployed during development. For the protection of our customers and the public at large, the Company does not publicly disclose detailed information regarding its cybersecurity practices, including what specific data is or is not encrypted in the vehicles.

8. Has your company ever provided to law enforcement personal information collected by a vehicle?

a. If so, please identify the number and types of requests that law enforcement agencies have submitted and the number of times your company has complied with those requests.

Yes. VWGoA started tracking the processing of subpoenas, warrants and court orders from law enforcement in 2021. As explained in response to Question 8b below, VWGoA requires a warrant or subpoena to comply with non-emergency law enforcement requests. Law enforcement occasionally does not follow up when informed of this requirement. We do not maintain records of the numbers of requests or inquiries (formal and informal) that we have not completed, because law enforcement did not issue a formal subpoena or warrant. As a result, we are providing information on the number

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

of responses we have completed for the VW and Audi brands for 2021, 2022, and 2023 (to date), only:

2021 – fewer than 20 responses

2022 – fewer than 25 responses

2023 – fewer than 45 responses

Depending on the circumstances, the vehicle, and the data available to us, our responses to law enforcement requests for vehicle data sometimes include only the cellular gateway SIM card identifier, because other vehicle data is unavailable to us for that VIN.

b. Does your company provide that information only in response to a subpoena, warrant, or court order? If not, why not?

VWGoA will disclose to law enforcement personal information related to a vehicle without the need for a properly served subpoena or warrant only if VWGoA has a good faith belief based on the information provided by law enforcement to VWGoA that "an emergency involving danger of death or serious physical injury to any person requires disclosure without delay" of records or communications relating to the emergency. In that event, VWGoA will verify that the request is coming from law enforcement and will provide vehicle data to law enforcement in response without a subpoena or warrant. This approach is required by law in Illinois. *Illinois Public Act 103-0300*. VWGoA takes this approach nationwide because it considers this approach as the best balance between protecting customer safety and protecting customer privacy. For non-emergency law enforcement requests, VWGoA requires a warrant or court order if the request from law enforcement is for U.S. historical vehicle location data for seven days or longer, or other sensitive personal information. If the request from law enforcement is for six days or fewer, for U.S. historical vehicle location data, or less sensitive personal information about the vehicle, VWGoA requires a subpoena.

c. Does your company notify the vehicle owner when it complies with a request?

Some cases include non-disclosure orders preventing such notice. Even in a case without a non-disclosure order, VWGoA does not currently notify owners of vehicles about specific law enforcement requests for their U.S. vehicle data, though we inform consumers in our privacy statements that we may disclose their information to law enforcement to comply with legal requirements. VWGoA discloses this position in its privacy statements for owners of Audi and VW

VOLKSWAGEN GROUP OF AMERICA
1950 Opportunity Way, Suite 1500
Reston, VA 20190

vehicles. Given that VWGoA receives so few law enforcement requests for vehicle data, and that VWGoA often does not have accurate, up to date contact information for consumers (or even knowledge that particular consumers are current owners of the vehicle), and such requests require timely responses, such a policy would be unduly burdensome in comparison to the benefit to consumers. VWGoA will continue to reevaluate this topic, especially if law enforcement demands for this data increase.

Sincerely,

Anna Schneider
SVP, Industry & Government Affairs

David Cox
Assistant General Counsel