United States Senate

November 30, 2023

James D. Farley, Jr.
President and Chief Executive Officer
Ford Motor Company
One American Road
Dearborn, MI 48126

Dear Mr. Farley,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Mary Barra
Chair and Chief Executive Officer
General Motors Company
300 Renaissance Center
Detroit, MI 48265

Dear Ms. Barra,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Noriya Kaihara
President and Chief Executive Officer
American Honda Motor Co., Inc.
1919 Torrance Blvd
Torrance, CA 90501

Dear Mr. Kaihara,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

José Muñoz
President and Chief Executive Officer
Hyundai Motor America, Inc.
10550 Talbert Avenue
Fountain Valley, CA 92708

Dear Mr. Muñoz,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

SeungKyu Yoon
President and Chief Executive Officer
Kia Motors America, Inc.
111 Peters Canyon Road
Irvine, CA 92606

Dear Mr. Yoon,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Tom Donnelly
President and Chief Executive Officer
Mazda Motor of America, Inc.
7755 Irvine Center Drive
Irvine, CA 92618

Dear Mr. Donnelly,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Dimitris Psillakis
President and Chief Executive Officer
Mercedes-Benz USA, LLC
One Mercedes-Benz Drive
Sandy Springs, GA 30328

Dear Mr. Psillakis,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Jérémie Papin
Chairperson
Nissan North America, Inc.
One Nissan Way
Franklin, TN 37067

Dear Mr. Papin,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Mark Stewart
Chief Operating Officer
Stellantis North America, LLC
1000 Chrysler Dr.
Auburn Hills, MI 48326

Dear Mr. Stewart,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id. See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Thomas J. Doll
President and Chief Executive Officer
North American Subaru, Inc.
One Subaru Drive
Camden, NJ 08103

Dear Mr. Doll,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Elon Musk
Chief Executive Officer
Tesla, Inc.
13101 Harold Green Road
Austin, TX 78725

Dear Mr. Musk,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access information on users' connected phones, such as location data, contacts, music listening habits,

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id. See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Tetsuo "Ted" Ogawa
President and Chief Executive Officer
Toyota Motor North America, Inc.
6565 Headquarters Drive
Plano, TX 75024

Dear Mr. Ogawa,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Pablo Di Si
President and Chief Executive Officer
Volkswagen Group of America, Inc.
2200 Woodland Pointe Avenue
Herndon, VA 20171

Dear Mr. Di Si,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id*. *See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

information on users' connected phones, such as location data, contacts, music listening habits, call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

November 30, 2023

Sebastian Mackensen
Chief Executive Officer
BMW of North America, LLC
300 Chestnut Ridge Road
Woodcliff Lake, NJ 07675

Dear Mr. Mackensen,

As cars increasingly become high-tech computers on wheels, they produce vast amounts of data on drivers, passengers, pedestrians, and other motorists, creating the potential for severe privacy violations. This data could reveal sensitive personal information, including location history and driving behavior, and can help data brokers develop detailed data profiles on users. In fact, a recent report from Mozilla revealed unfettered data collection and privacy intrusions across huge swaths of the automobile industry.[1] These business practices must end. In light of these concerning reports, I am writing to request additional information about your company's policies on data collection, use, and disclosure. I also urge your company to implement and enforce strong privacy protections for consumers to ensure that cars do not become another critical area where privacy is disappearing.

Advances in car technology can bring new benefits, but as every component of a vehicle — from the steering wheel to the seats — becomes increasingly computerized, these innovations enable automakers to collect and transmit large amounts of data on drivers, passengers, and even individuals outside the vehicle. Today, cars have effectively become smartphones on wheels. Car manufacturers, dealers, car technology developers, and other entities rely on an increasing number of sensors and devices to produce and collect troves of data. Telematics devices and location services track users' driving behavior and real-time location.[2] New technologies can detect drivers' eye movements and even their heartbeat, which could allow third parties to collect physical and mental health data.[3] Automakers and technology developers may access information on users' connected phones, such as location data, contacts, music listening habits,

---

[1] Jen Caltrider et al., *It's Official: Cars are the worst product category we have ever reviewed for privacy,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter Caltrider 1].

[2] Jen Caltrider et al., *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ [hereinafter Caltrider 2].

[3] *Id. See, e.g.,* Brian Dolan, *Toyota demos ECG Sensing Steering Wheel,* MobiHealthNews (July 26, 2011), https://www.mobihealthnews.com/12128/toyota-demos-ecg-sensing-steering-wheel.

call logs, and text messages.[4] Furthermore, exterior-facing cameras can record individuals outside a car, enabling manufacturers to access personal information unrelated to the vehicle or its users.[5]

Beyond just collecting this data, automakers have integrated wireless technologies into vehicles to transfer the data onto their own servers. Bluetooth technology, for example, was an early connectivity feature that allowed users to interact wirelessly with their car's hardware. But carmakers have used Bluetooth to expand their surveillance to include information that has nothing to do with a vehicle's operation, such as data from smartphones that are wirelessly connected to the vehicle.[6] Manufacturers have more recently developed the ability to wirelessly collect user data by integrating into vehicle dashboards services that require long-range network connectivity, like live traffic updates and weather information. Subsequent advances such as on-board GPS services, over-the-air vehicle software updates, and infotainment centers that operate like a smartphone with a full suite of apps further increase the types of data vehicles collect and the frequency of user data dissemination to manufacturers and third parties.[7]

This broad data collection poses serious privacy risks. Carmakers can learn intimate and sensitive information about drivers, passengers, and individuals outside the vehicle. Physical sensors in a car, such as eye sensors, steering wheel heart-health readers, and sensors in the vehicle seats, can provide intrusive looks into a person's physical or mental health, stress levels, or emotional state.[8] Location data can be used to discern an individual's hobbies, workout schedule, or even sexual orientation and sexual activity.[9] One manufacturer even states that it may collect "information about your race or ethnicity, religious or philosophical beliefs, sexual orientation, sex life and political opinions" and "trade union membership" — information that has nothing to do with driving a car.[10] Carmakers magnify these privacy risks by selling this

---

[4] Caltrider 2, *supra* note 2; Joseph Menn, *California Privacy Regulator's First Case: Probing Internet-Connected Cars,* Wash. Post (July 31, 2023), https://www.washingtonpost.com/technology/2023/07/31/cppa-privacy-car-data/.

[5] *See e.g.,* Steve Stecklow et al., *Tesla Workers Shared Sensitive Images Recorded by Customer Cars,* Reuters (Apr. 6, 2023), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[6] *See, e.g.,* Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks,* The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[7] *See* Privacy4Cars, *Privacy4Cars' Five Levels of Vehicle Connectivity*, https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/ (last visited Oct. 26, 2023).

[8] *See* Caltrider 2, *supra* note 2.

[9] *See* Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go,* Vice Media Group (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo.

[10] Hibaq Farah and Jasper Jolly, *From Sex Life to Politics: Car Driver Data Grab Presents 'Privacy Nightmare', Says Study,* The Guardian (Sept. 6, 2023), https://www.theguardian.com/business/2023/sep/06/cars-collect-extensive-personal-data-on-drivers-study-warns.

personal information to data brokers.[11] By combining data collected from the vehicle with information from third-party sources such as a user's browsing history or social media profile, data brokers can develop an in-depth driver profile and make inferences about nearly any aspect of a user's life. This combination of data sources creates significant privacy risks for drivers, passengers, and the public.

Automakers and data brokers can then profit from this data in numerous ways. One manufacturer, for example, has suggested linking vehicles to the user's lending institution, a repossession agency, and police authorities.[12] This action would allow the manufacturer to employ a series of escalating penalties — from loss of window control and air conditioning to potentially locking the driver out of the car or even directing the car to drive to an impound lot — if the driver misses a car payment. Car manufacturers have also suggested using the data for targeted advertising, such as displaying an intrusive ad on a vehicle dashboard.[13] This data collection can thus have significant financial benefits for manufacturers. In the past, automakers only sold vehicles and collected payments — and perhaps received additional maintenance payments in the future — but today's data collection creates a lucrative new source of recurring revenue.[14] For that reason, automakers have significant incentives to continue collecting large amounts of data from the public.

Even more worrisome, as carmakers have expanded their data collection practices, consumers have largely been left in the dark. In September, Mozilla released several reports based on its review of 25 car brands' privacy policies.[15] The results are alarming: All 25 brands — across 15 different automakers — failed to meet Mozilla's minimum privacy and security standards overall, with most receiving failing grades in the categories of data use, data control, track record of past data breaches, and security.[16] In fact, Mozilla found that all 25 brands collect more personal data than necessary to provide their services to customers, that most share (84 percent) or even sell (76 percent) customer data, and that the brands do not give drivers the right to delete their personal data (92 percent).[17] Finally, due in part to the lack of industry

---

[11] *See* Otonomo, *Investor Presentation— February 2021*, https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf (last visited Oct. 26, 2023); Michele Bertoncello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data,* McKinsey & Company (Feb. 11, 2021), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

[12] Jen Caltrider et al., *After Researching Cars and Privacy, Here's What Keeps Us Up at Night,* Mozilla Foundation (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/ [hereinafter Caltrider 3].

[13] *See* Bertoncello, *supra* note 11; *see, e.g.,* Mapbox, *Mapbox Debuts MapGPT, Allowing Automakers to Take Control of Their Voice Assistants,* Cision US Inc. (Oct. 4, 2023), https://www.prnewswire.com/news-releases/mapbox-debuts-mapgpt-allowing-automakers-to-take-control-of-their-voice-assistants-301946800.html.

[14] Bertoncello, *supra* note 11.

[15] *See e.g.,* Caltrider 1, *supra* note 1; Caltrider 2, *supra* note 2; Caltrider 3, *supra* note 12.

[16] Caltrider 1, *supra* note 1.

[17] *Id.*

transparency about privacy and data storage practices, Mozilla could not confirm that any of the brands met its minimum standards for the security of customer data.[18] If Mozilla's researchers had difficulty understanding these privacy policies, consumers — who rarely read such policies and lack the expertise of privacy researchers — are surely even more confused.

These practices are unacceptable. Although certain data collection and sharing practices may have real benefits, consumers should not be subject to a massive data collection apparatus, with any disclosures hidden in pages-long privacy policies filled with legalese. Cars should not — and cannot — become yet another venue where privacy takes a backseat. As more and more cars become computers on wheels, automakers must implement strong privacy policies to protect users. To help understand your companies' data practices and privacy policies, I request you answer the following questions in writing by December 21.

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?

---

[18] *Id.*

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?

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

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?

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?

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.

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?

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?

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?

Thank you for your prompt attention to this issue.

Sincerely,

Edward J. Markey
United States Senator