FUTURE OF PRIVACY FORUM

1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

April 30, 2024

Via Electronic Mail

Marc Coldiron
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

To Whom It May Concern,

On behalf of the Future of Privacy Forum (FPF), we are pleased to submit comments in response to the Bureau of Industry and Security (BIS) and the United States Department of Commerce (DOC) Advanced Notice of Proposed Rulemaking (ANPRM) regarding Securing the Information and Communications Technology and Services (ICTS) Supply Chain of Connected Vehicles.[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.

FPF has significant expertise on issues around vehicles and privacy. Since 2014 FPF has organized a working group of experts on this topic and has contributed substantial research and analysis on potential privacy risks and mitigations for vehicles. In the ANPRM, BIS indicates that its proposal seeks to "narrowly address involvement by persons owned, controlled by, or subject to the jurisdiction or direction [of foreign adversaries] in the design, development, manufacture, or supply of ICTS integral to CVs where that involvement may create undue or unacceptable risk to U.S. national security."[2] FPF encourages BIS to include privacy across the vehicle space as a central component in its process. Specifically, FPF recommends:

1. **BIS should amend the definition of Connected Vehicles to ensure that future actions in this area include Connected Vehicles and emerging technologies, including Software-Defined Vehicles.**
2. **BIS should incorporate privacy protections for personal data and incorporate existing frameworks where relevant.**

[1] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15066 (Mar. 1, 2024) (to be codified at 15 CFR 7) https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles.
[2] *Id*.

3. **BIS should prioritize consistency with global frameworks on cross-border data transfers and coordinate with other U.S. agencies engaged in related, ongoing federal processes.**

I. Background and Introduction

In the Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, the Biden administration prioritizes the "unusual and extraordinary threat" related to "[t]he continuing effort of certain countries of concern to access Americans' sensitive personal data." Specifically, the Administration emphasizes the threat of such access to security, privacy, and human rights.[3] Directly related to the Executive Order, the Administration urges the Commerce Department to investigate connected vehicles and related national security risks.[4] In this ANPRM, BIS responds to the White Houses' call, starting a process to establish a rule regarding ICTS integral to connected vehicles. In evaluating the potential risks to US national security, BIS will determine requirements, restrictions, or overall prohibitions for the connected vehicle supply chain.

II. Recommendations

FPF strongly encourages BIS to be broadly inclusive of all types of vehicles and to centralize privacy in that process. Below, we provide specific recommendations to support this goal.

1. *BIS should amend the definition of Connected Vehicles to ensure that future actions in this area include Connected Vehicles and emerging technologies, including Software-Defined Vehicles.*

FPF urges BIS to ensure that the scope of its work in this area is inclusive of both current and emerging technologies. Within the complex vehicle data ecosystem, Connected Vehicles (CV) is often the umbrella phrase when referencing vehicles that include various technologies and

[3] Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, The White House (February 28, 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[4] Press Release, The White House, *Statement from President Biden on Addressing National Security Risks to the U.S. Auto Industry,* (Feb. 29, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/statement-from-president-biden-on-addressing-national-security-risks-to-the-u-s-auto-industry/.

connectivity features.[5] The White House specifically asks for BIS to investigate "connected vehicles", and in the ANPRM, BIS scope defines a connected vehicle as "an automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device." While the definition as written is likely inclusive of all current technology, we recommend that it be amended to encompass additional vehicle features that may raise substantial privacy and security risks.

Software-Defined Vehicles (SDVs) contain more software-focused features and capabilities than the traditional concept of a connected vehicle.[6] Both SDVs and CVs utilize software for communications, as encompassed by BIS's current definition. However, SDVs utilize internal software capabilities for functions well beyond communication, including starting the vehicle, checking for malfunctions, navigation, or operating an Advanced Driver Assistance (ADAS) or Driver Monitoring System (DMS). These systems collect data that may create privacy and security risks regardless of the external communication. Amending the definition to include reference to software that may be helping operate autonomous vehicle capabilities or general internal systems would ensure that future actions in this area account for new technologies and internal software capabilities.

2. *BIS should incorporate privacy protections for personal data and incorporate existing frameworks where relevant.*

Protections for individual privacy can provide a central role to ensuring that BIS is able to achieve its noted objectives in this process. BIS should consider the role of key data protection safeguards, including established best practices and risk management processes, for both sensitive and non-sensitive information in the CV sector.

---

[5] FPF's infographic "Data and the Connected Car" illustrates a network of carmakers, vendors, and others who support individuals' safety, logistics, infotainment, and security needs. New players in the ecosystem include infotainment service providers, driving assistance systems and services, road infrastructure managers, fleet managers, insurance companies, ride-sharing companies, and telecommunications operators. https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

[6] Deloitte China, *Software-Defined Vehicles – A Forthcoming Industrial Evolution*, Deloitte (2021), https://www2.deloitte.com/cn/en/pages/consumer-business/articles/software-defined-cars-industrial-revolution-on-the-arrow.html.

Data processing within CVs occurs in a complex ecosystem. The data that CVs collect may be necessary for vehicle functions, including safety functions, utilized for special features, like driver assistance or entertainment, or intended to help manufacturers with future research and development, among other things. Many data points may be utilized for multiple purposes. For instance, data on tire sensors or airbag deployment may be useful to develop improvements as well as to demonstrate compliance with regulations.

Some data that vehicles collect may have no privacy implications. For instance, data from technologies such as LiDar are focused on mapping, collect no personally identifying information, and serve an essential function in AV development.[7] However, other data can raise substantial privacy risks, particularly when car systems collect sensitive personal information, such as biometric data, or data that may reveal criminal offenses or infractions.[8] Geolocation data, as one example, can reveal a driver's life habits and allow the inference of the driver's residence, place of work, interests, and other sensitive details such as religion or sexual orientation.[9]

While some data may have a lower privacy risk if it is not directly indicative of or connected to a specific individual, the potential for identification must include the potential for linking various data points, including the Vehicle Identification Number (VIN). Multiple connected data points may not only identify a specific individual but can also be indicative of driving habits over time or other sensitive information.[10] In addition, data from cameras and other sensors may implicate privacy risks of those beyond the owner of a vehicle, including other drivers, vehicle passengers, and bystanders located outside the vehicle.

Today, the U.S. does not have a comprehensive federal privacy law to provide protections in the processing of personal data by businesses. In lieu of a federal law, The Automotive Alliance for Innovation (AAI) established privacy principles with which member vehicle manufacturers

---

[7] Chris Teauge, *What Is Lidar and Why It's Important for Autonomous Vehicles,* Newsweek, (2021), https://www.autoweek.com/news/a36190274/what-lidar-is/.

[8] Adonne Washington, *Vehicle Safety Systems: Privacy Risks and Recommendations,* The Future of Privacy Forum, (Mar. 21, 2024), https://fpf.org/wp-content/uploads/2024/03/FPF-Vehicle-Safety-Systems_March2024-FINAL.pdf.

[9] Betsie Estes, Geolocation—The Risk and Benefits of a Trending Technology, ISACA, (Sept. 26, 2016), https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/geolocationthe-risk-and-benefits-of-a-trending-technology

[10] C-319/22, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CJ0319.

adhere.[11] The voluntary principles serve as a guidepost with a focus on transparency, data security, data minimization, and consent. BIS should consider how these and other privacy practices can minimize risks to personal data when transferred to other countries. The European Data Protection Board (EDPB) recognized the importance of privacy protections for CVs in adopted Guidelines 01/2020 on processing personal data in the context of CVs and mobility-related applications.[12] For instance, the EDPB has identified geolocation data, biometric data, and data that could reveal offenses of traffic violations as categories of high-risk personal data.

3. *BIS should prioritize consistency with global frameworks on cross-border data transfers and coordinate with other U.S. agencies engaged in related, ongoing federal processes.*

In the vehicle market, where many CV manufacturers source, assemble, and sell their products globally, international regulatory regimes are a vital consideration. Today, vehicle manufacturers must comply with a complicated web of regulatory requirements and restrictions, including limitations on the collection and transfer of data across geographic borders.[13]

While export controls have been a long-standing fixture in U.S. law and policy, the U.S. has not historically limited cross-border data transfers of personal data in any significant manner.[14] However, BIS has published its ANPRM at a time of significant regulatory change in the United States. The Biden Administration's recent Executive Order proposes to limit large-scale transfers

[11] Alliance for Automotive Innovation, *Consumer Privacy Protection Principles: Privacy Principles for vehicle Technologies and Services,* Alliance for Automotive Innovation, (Nov. 12, 2014 revised Mar. 2022), https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

[12] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, European Data Protection Board (Adopted on March 9, 2021), https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf.

[13] Most privacy laws include restrictions on transferring personal data across international borders. Some jurisdictions are regulating the transfer of any data generated by "connected products," regardless of whether it is linkable to individual natural persons. EU Reg, 2023/2854; *see also* Art. 45, Regulation (EU) 2016/679 (General Data Protection Regulation), available at https://gdpr-info.eu/art-45-gdpr.

[14] Todd Daubert, *US Data Transfers Update,* Oct. 28, 2022), https://www.dentons.com/en/insights/articles/2022/october/28/us-data-transfers.

of specific kinds of personal data to specifically designated "countries of concern."[15] The U.S. Department of Justice (DOJ) is currently undergoing a rulemaking process under that Executive Order to determine the precise rules and requirements for entities to comply with these new requirements.[16] At the same time, Congress recently passed an appropriations bill that included the "Protecting Americans' Data from Foreign Adversaries Act of 2024." This new law, enforceable by the U.S. Federal Trade Commission (FTC) sets forth additional limitations on the cross-border transfer of certain personal data.

CV manufacturers will likely be implicated by each of these regulatory proceedings. BIS should work with partners at DOJ, FTC, and other federal agencies, to maximize, to the extent possible, regulatory consistency and minimize unnecessary confusion or uncertainty for CV manufacturers seeking to comply with new requirements.

III. Conclusion

The Future of Privacy Forum appreciates this opportunity to comment on these issues and the Commerce Department's efforts.

We welcome any further opportunity to provide resources or information to assist this vital effort. If you have any questions regarding these comments and recommendations, please contact Adonne Washington at awashington@fpf.org (cc:info@fpf.org).

Sincerely,

Adonne Washington, *Policy Counsel Mobility, Location & Data*
Lee Matheson, *Senior Policy Counsel, Global*
Angela Guo, 2024 Spring *Legal Intern*

The Future of Privacy Forum - https://fpf.org/

---

[15] Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, The White House (February 28, 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[16] Stacey Gray, *Future of Privacy Forum DOJ ANPRM Comment,* The Future of Privacy Forum, (Apr. 19, 2024), https://fpf.org/wp-content/uploads/2024/04/FPF-Comment-DOJ-ANPRM-Bulk-Sensitive-Personal-Data-April-19-2024.pdf.