

April 30, 2024

Alan F. Estevez  
Under Secretary of Commerce for Industry and Security  
Bureau of Industry and Security  
1401 Constitution Avenue NW  
Washington, District of Columbia 20230

**RE: Comments of ACT | The App Association on the Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles [Docket No. 240227- 0060]**

Dear Mr. Estevez:

ACT | The App Association (App Association) writes in response to the Department of Commerce's (DOC's) Bureau of Industry and Security (BIS) request for comments on the advance notice of proposed rulemaking (ANPRM) on securing the information and communications technology and services (ICTS) supply chain for connected vehicles.<sup>1</sup>

**I. Introduction and Statement of Interest**

The App Association is a global policy trade association for the small business technology developer community. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. App developers like our members also play a critical role in developing connected vehicle innovations throughout ICTS connected vehicle supply chains. The value of the ecosystem the App Association represents—which we call the app economy—is approximately \$1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the \$8 trillion internet of things (IoT) revolution.<sup>2</sup>

**II. Connected Vehicles are Part of a Broader Digital Ecosystem of Applications and Services**

The App Association appreciates BIS' request for input on the ICTS supply chain for CVs in the United States, and shares the goal of realizing strong, sustainable, and secure ICTS supply chains across sectors. App Association members develop software and connected hardware at key points throughout ICTS connected vehicle supply chains. Connected vehicles leverage GPS, radar, photos, and other data points securely and appropriately collected, which App Association members often leverage to innovate and compete.

---

<sup>1</sup> 89 FR 15066.

<sup>2</sup> ACT | The App Association, State of the App Economy (2022), <https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL.pdf>.

As BIS considers new rules for the security of the ICTS supply chain, the App Association urges consideration of the reality that connected vehicles are a part of the broader digital economy. Many connected vehicles on the road today have access to and make use of third-party applications and services, and this will only increase as the digital ecosystem around connected vehicles develops. BIS should be mindful that, while focused on security, its rules could amount to harmful digital trade barriers if not drafted with appropriate scope.

The small business innovators we represent prioritize the following general principles for policies affecting the international digital economy:

- **Enabling Cross-Border Data Flows:** The seamless flow of data between economies and across political borders is essential to the functioning of the global economy. Small business technology developers must be able to rely on unfettered data flows as they seek access to new markets.
- **Avoiding Data Localization Policies:** American companies looking to expand into new markets often face regulations that force them and other foreign providers to build and/or use local infrastructure in the country. Data localization requirements seriously hinder imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification. Our members do not have the resources to build or maintain unique infrastructure in every country in which they do business, and these requirements effectively exclude them from commerce.
- **Prohibiting Customs Duties and Digital Service Taxes on Digital Content:** American app developers and technology companies must take advantage of the internet's global nature to reach the 95 percent of customers who live outside of the United States. However, the tolling of data crossing political borders with the purpose of collecting customs duties directly contributes to the balkanization of the internet. These practices jeopardize the efficiency of the internet and effectively block innovative products and services from market entry.
- **Ensuring Market Entry is Not Contingent on Source Code Transfer or Inspection:** Some governments have proposed policies that require companies to transfer, or provide access to, proprietary source code as a requirement for legal market entry. Intellectual property is the lifeblood of app developers' and tech companies' innovation; the transfer of source code presents an untenable risk of theft and piracy. Government policies that pose these requirements are serious disincentives to international trade and a non-starter for the App Association's members.
- **Preserving the Ability to Utilize Strong Encryption Techniques to Protect End User Security and Privacy:** Global digital trade depends on the use of strong encryption techniques to keep users safe from harms like identity theft. However, some governments continue to demand that backdoors be built into encryption keys for the purpose of government access. These policies jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a privacy and security standpoint, the viability of an app company's product depends on the trust of its end users.
- **Securing Intellectual Property Protections:** The infringement and theft of intellectual property and trade secrets threatens the success of the App Association's members and hurts the billions of consumers who rely on these app-based digital products and services. These intellectual property violations can lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone a potential

“end-of-life” occurrence for a small app development company. The adequate and effective protection and enforcement of intellectual property rights is critical to the digital economy innovation and growth.

- ***Avoiding the Misapplication of Competition Laws to New and Emerging Technology Markets:*** Various regulators, including key trading partners, are currently considering or implementing policies that jeopardize the functionality of mobile operating systems and software distribution platforms that have enabled countless American small businesses to grow. Since its inception, the app economy has successfully operated under an agency-sale relationship that has yielded lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections for app developers with little-to-no government influence. Foreign governments regulating digital platforms inconsistent with U.S. law will upend this harmonious relationship enjoyed by small-business app developers and mobile platforms, undermine consumer privacy, and ultimately serve as significant trade barriers.

### **III. BIS ICTS Rules Should Adopt Clear and Targeted Definitions**

The App Association encourages BIS to resolve vague definitions for connected vehicles, which would, if advanced as drafted include all segments of the automotive industry. We urge BIS to clearly and specifically define vehicle classes/supply chains that it seeks to apply ICTS rules to in order to provide clarity to the industry about impacted products, providing key use cases as guidance/to advance understanding.

### **IV. BIS ICTS Rules Should Avoid Data Localization Requirements**

As discussed above, data and processing localization requirements ignore the efficiencies and security of distributed cloud computing and do not translate to assurances of data security, instead creating unnecessary barriers to trade and innovation. The App Association strongly urges BIS to avoid local data storage or processing mandates in its rules. Such a requirement would be inconsistent with connected vehicle industry leading standards for data collection and processing, which are deferred to by the U.S. Department of Transportation.<sup>3</sup>

### **V. BIS ICTS Rules Should Preserve the Ability to Secure Data and Supply Chains Using Encryption**

Whether as a contractor or as a business partner, App Association members are required to share sensitive information with OEMs of CVs in the normal course of business using cloud computing services. They rely on risk management best practices and technical protection mechanisms to securely accomplish these vital interactions, which may include remote access and/or providing firmware or software updates. As it advances rules for ICTS connected vehicles, BIS should maintain the ability to leverage these technical protection mechanisms such as encryption, without which the secure data flows that underpin secure supply chains could not exist.

---

<sup>3</sup> <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf>.

## **VI. BIS ICTS Connected Vehicle Rules Should Align with Leading Risk Management Practices**

The App Association also urges BIS to align with leading federal guidance from the National Institute of Standards and Technology (NIST) on cybersecurity and supply chain risk management<sup>4</sup> as well as sector-specific guidance from the National Highway Traffic Safety Administration (NHTSA),<sup>5</sup> when crafting its regulations, which enable the scaling of risk mitigation practices to the harms presented. Such an alignment will ensure that BIS rules enable the industry to most efficiently identify, assess, and mitigate the risks associated with the distributed and interconnected nature of ICTS connected vehicle supply chains across the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction).

## **VII. Technology Standardization Has a Crucial Role In Supporting Secure and Strong ICTS Supply Chains For Connected Vehicles**

### **A. Historical Abuses in Standard-Essential Patent Licensing Have Reached Connected Vehicles**

Technology standards provide the foundation for many ICTS-based inventions that make vehicles “smart.” Technical standards provide an efficient and interoperable base for technology developers to create new inventions that increase the quality, safety, and reliability of vehicles for the independent consumer, businesses, and public transportation alike. These standards are subject to a larger standard-setting process housed by standard-setting organizations (SSOs) that facilitate the open and consensus-based development of a standard and guide the equitable and reasonable implementation of the standard. When a patent holder contributes their technology to a technical standard, they provide SSOs with a commitment that they will license their so-called standard-essential patents (SEPs) on fair, reasonable, and non-discriminatory (FRAND) terms in exchange for access to a wider pool of licensees. Therefore, by contributing to the standardization process, a SEP holder consents not to unduly exclude competitors from a standard past requiring a FRAND SEP license.

Unfortunately, there are well-documented SEP licensing abuses that disrupt mature and crucial supply chains, including for connected vehicles. Longstanding evidence shows that a minority of well-resourced and opportunistic SEP holders, including non-practicing entities (NPEs), abuse their monopoly positions by discarding the FRAND commitments they have made to attain unreasonable terms and excessive royalty rates. Since SSOs facilitate access to technical standards that touch various industries, these opportunistic SEP holders plague many verticals, always looking for the next market to extract additional and unrelated value for their SEP. The anticompetitive harms experienced in the SEP licensing ecosystem disrupt fair access to technical standards that support efficient innovation.

These SEP holders routinely refuse to license to certain upstream entities in the supply chain, while instead licensing to downstream entities, such as end product manufacturers, from whom

---

<sup>4</sup> E.g., <https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management>.

<sup>5</sup> <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>.

they can extract additional value for a SEP holder's patented technology from unrelated features of the implementing product. The practice by SEP holders to extract value from components of the implementing technology that do not function based on the SEP has been discouraged on a global scale.<sup>6</sup> This evidence is at odds with the position held by certain patent pools that claim they are not beholden to the FRAND commitment attached to the SEPs they license, which causes significant uncertainty in supply chains.<sup>7</sup>

The automotive sector's established supply chains have been subject to SEP licensing abuses. Opportunistic SEP holders that have patents covering wireless communication standards often choose what manufacturer in the automotive supply chain to license their SEP to, causing uncertainties about indemnification for other manufacturers. The same SEP holders seek licensing fees that extract value out of the end product (the vehicle) beyond the components that function from the SEP. This process slows down innovation in connected vehicles that are geared toward achieving important safety and sustainability goals.

## **B. Foreign Jurisdictions That Support Standard-Essential Patent Licensing Abuses Amplify Harm to U.S. Innovation**

Numerous intellectual property rights (IPR) policies of SSOs and foreign jurisdictions threaten both U.S. leadership and participation in international standard setting, and the growth of U.S. innovators that rely on the ability to readily license SEPs. A trend of court decisions abroad, starting in the United Kingdom (UK)<sup>8</sup> and European Union (EU),<sup>9</sup> have distorted the meaning of the FRAND commitment, creating an imbalance that heavily favors SEP holders by routinely enabling prohibitive orders (injunctions) for FRAND-committed SEPs. For example, Germany's approach to SEP injunctions has caused immense disruptions to supply chains across several industries and has resulted in various companies ceasing operation in the country because of the inability to reliably use standards (due to an imbalanced approach to SEP injunctions), fraying the international norm for limited injunctions on FRAND-committed SEPs and undermining international standards.

These decisions have enabled (and emboldened) SEP holders to systematically abuse their dominant market position as a gatekeeper to the use of the standard to attain supra-FRAND terms (a practice known as hold-up).<sup>10</sup> Some foreign courts have concluded that they can force a standards user to agree to a global SEP portfolio on FRAND terms set by the court or SEP holder on pain of a national injunction if the standards user does not agree to the license. In such decisions, the global SEP licenses at issue often include patents issued outside the court's jurisdiction for which validity and essentiality have not been assessed. The precedent set by such decisions has done two things to the landscape of international standards: (1) allowed

---

<sup>6</sup> *Interdigital Technology Co. v. Lenovo Group Ltd.* [2023] EWHC 126, 539 (Pat). Para 247 ("When a mobile phone, tablet or computer uses 3G, 4G or 5G technology covered by SEPs, the royalties payable should not depend on the price of the phone (or tablet or computer), which reflects many other features (e.g. screen size, processor power and other features) which are unrelated to the licensed technology even if dependent on it, as well as the status of the brand of phone or tablet.").

<sup>7</sup> See *Continental Automotive Systems v. Avanci, LLC*, No. 20-11032 (5th Cir. 2022).

<sup>8</sup> See *Unwired Planet International Ltd v. Huawei Technologies Co. Ltd* (SCUK 2020).

<sup>9</sup> See *Sisvel v Haier*, Federal Court of Justice, judgment dated 5 May 2020, Case No. KZR 36/17; see *Koninklijke Philips N.V. v. Wiko SAS*, Court of Appeal of The Hague, judgement dated 2 July 2019, Case No. C/09/511922/HA ZA 16-623.

<sup>10</sup> Lemley, Mark A. and Shapiro, Carl, Patent Holdup and Royalty Stacking. 85 *Texas Law Review* 1991 (2007).

jurisdictions to exercise extrajudicial authority on patents outside their purview;<sup>11</sup> and (2) encouraged certain SEP holders to forum shop to a more favorable jurisdiction to handle the outcome of their disputes when they are unable to force implementing standards users into unreasonable licensing terms, despite their FRAND obligation.

### **C. BIS Should Address Standard-Essential Patent Licensing Issues That Disrupt Supply Chains in Connected Vehicles**

The App Association urges BIS to ensure that its ICTS transaction rules support U.S. connected vehicle supply chain security and resiliency. In addressing ICTS transactions for connected vehicles, BIS should recognize and prevent bottlenecks in SEP licensing that are barriers to trade and which threaten the resilience of U.S. supply chains, namely those SEP licensor hold-up practices that have been well demonstrated with empirical evidence.<sup>12</sup> If U.S. manufacturers are unable to reliably develop critical components that affect consumer safety and privacy and the quality of U.S.-made connected vehicles without fear of potential and likely lawsuits from opportunistic SEP holders, many inventors will forgo production. The DOC can address these issues by increasing transparency in the FRAND SEP licensing process through a public database for base level SEP information, a government-led SEP Policy Statement, and support in U.S. participation in international standards.

BIS should, in coordination with others including the United States Patent and Trademark Office (USPTO), to secure connected vehicle supply chains. As one example, BIS ICTS transaction requirements should contribute to providing a base level of information that a SEP licensor should provide to licensees outside an overly restrictive non-disclosure agreement (NDA) that hides comparable licensing rates and terms. BIS' efforts to provide more transparency in FRAND licensing disputes through public databases would assist in facilitating fair negotiations between two licensing parties without significant intervention. We consider the following information to be "base level:"

- Information (e.g., patent list) to enable a licensee and entities within its supply chain to understand the SEPs being enforced;
- Detailed specification (e.g., claim charts) on the nature of the patent's alleged infringement by the licensee's technology, and ancillary information necessary for the licensee to assess claims of infringement, validity, and essentiality;
- FRAND licensing terms;
- Aspects of prior licensing history and any other information are needed to evaluate to offered and potential FRAND terms.

BIS should equally promote a balance between a SEP holder's patent rights and reasonable access to technical standards for those needing licenses in order to use standards and secure their supply chains by supporting broadly-accepted principles reflecting the meaning of the FRAND commitment. A balanced and pro-innovation multi-agency policy statement that

---

<sup>11</sup> Bonadio, Enrico, Mohnot, Rishabh, Standard Essential Patents, Global Licensing Approach and the Principle of Territoriality (September 6, 2022), <https://patentblog.kluweriplaw.com/2022/09/06/standard-essential-patents-global-licensing-approach-and-the-principle-of-territoriality/>.

<sup>12</sup> See Love, Brian J. and Lefouili, Yassine and Helmers, Christian, Do Standard-Essential Patent Owners Behave Opportunistically? Evidence from U.S. District Court Dockets (November 8, 2020). Available at SSRN: <https://ssrn.com/abstract=3727085>.

presents a whole of government approach to mitigating harmful SEP licensing abuses is key to amicable resolutions to FRAND licensing disputes. Policy solutions that facilitate more transparency in the licensing process can provide licensing parties with reasonable information to conclude a FRAND SEP license. These procedures are more crucial for entities that lack the professional and financial resources as their larger competitors, like small and medium-sized businesses. These policy solutions also provide courts and tribunals with evidence compiled through an expert opinion. These opinions should not prevent the court or tribunal from making an independent determination.

An important component of securing and strengthening supply chains is supporting U.S stakeholder participation in international technology standards development around ICTS innovations. The IP-based incentives in the standardization process differ from non-essential IP incentives. Patents are contributed to the standardization process to enable more inventors to use that standard. In this process, SEP holders are owed reasonable royalties for the use of their patented invention. The United States Government National Standards Strategy on Critical and Emerging Technology (USG NSSCET) is clear that the success of the voluntary, consensus-based, open-participation technology standards system is vital for U.S. competitiveness and national security. The success of this system to standards development is that industry participants are providing competing patent contributions and approaches. This system enables the market to determine a company's success and incents standardized technology development. This system ensures that internationally adopted standards are high quality, incorporate U.S. stakeholder input, and benefit all standards users. The consensus-based, open-participation technology standards system must be preserved in order to protect competitive standards that include U.S. leadership and involvement. Therefore, BIS should work with NIST to support U.S. participation and leadership in international technical standards.

## **VIII. Conclusion**

The App Association appreciates the opportunity to provide comments to BIS on securing the ICTS connected vehicle supply chains.

Sincerely,



Brian Scarpelli  
Senior Global Policy Counsel

Chapin Gregor  
Policy Counsel

Priya Nair  
Senior IP Policy Counsel

**ACT | The App Association**  
1401 K St NW (Ste 501)  
Washington, DC 20005