

June 4, 2024

Submitted via Electronic Mail to www.regulations.gov

Victor Ban
Special Counsel
Office of the United States Trade Representative
600 17th Street NW
Washington, District of Columbia 20036

RE: Post-Hearing Written Comments of ACT | The App Association, Promoting Supply Chain Resilience (USTR-2024-0002)

In supplement to ACT | The App Association's written comments¹ and May 3, 2024 public testimony to the United States Trade Representative (USTR) regarding the agency's development of objectives and strategies that advance U.S. supply chain resilience in trade negotiations, enforcement, and other initiatives, the App Association hereby submits its post-hearing written comments.

The App Association represents thousands of small business innovators and startups in the software development and high-tech space located around the globe.² As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, that digital economy is worth more than \$1.8 trillion annually and provides over 6.1 million American jobs.³ App Association members create innovative software and hardware technology solutions that power the internet of things (IoT) across modalities and segments of the economy and are part of and rely on U.S. supply chain resilience.

App Association members are both part of and beneficiaries of information and security technology and services (ICTS) supply chains; they reside at every link in such supply chains and utilize them to cost-effectively bring new and innovative products to the marketplace. We support U.S. government efforts to strengthen domestic manufacturing and to secure supply chains through strategic arrangements with trusted and regional partners. We commit to working with USTR and other stakeholders to reduce or eliminate trade barriers that disrupt supply chains and impede small business growth and job creation.

1

² ACT | The App Association, *About*, available at <http://actonline.org/about>.

³ ACT | The App Association, *State of the U.S. App Economy: 2023*, <https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf>

Generally, the small business innovators we represent prioritize the following principles:

- ***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.
- ***Prohibiting 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.

A large number of the digital trade barriers the App Association raised in its last comment to USTR on the National Trade Estimate⁴ capture how, across the different forms they take, these barriers disrupt supply chains and reduce their resiliency. This dynamic is made worse by the fact that modern supply chains are themselves digital supply chains in many ways. Across industries, many of which use the products and services of App Association members, cloud applications and new developments in artificial intelligence (AI) are being used to make supply chains more efficient. Digital trade barriers therefore have real-world effects on physical supply chains as well. We urge USTR to recognize the overall impact that digital trade barriers have on supply chain resiliency and to act to mitigate them in trade negotiations, enforcement, and other initiatives.

We strongly encourage USTR to recognize and leverage standards of excellence for supply chain integrity and resiliency, several of which the U.S. government itself has developed, as well as the adequacy of software vetting programs employed by leading app stores today.⁵ These standards, which represent leading approaches to supply chain risk management, are based on extensive engagement with and contributions from the U.S. government as well as leading private sector interests. In the context of the Department of Commerce (DoC) supply chain security rules, the App Association has requested that parties who attest to adherence to such standards be provided with safe harbor from enforcement; in the alternative, use of such standards should provide a strong presumption of compliance with the rule. These standards for resiliency include, but are not necessarily limited to:

4

⁵ <https://developer.apple.com/app-store/review/>.

- ISO 28001 (Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance);⁶
- ISO/IEC 20243-2:2018 [ISO/IEC 20243-2:2018] (Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018);⁷
- ISO/IEC 15408 Common Criteria;⁸
- National Institute of Standards and Technology (NIST) standards addressing supply chain security including:
 - The NIST Cybersecurity Framework;⁹
 - NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations);¹⁰
 - NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations);¹¹ and
 - NIST 800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations).¹²
- Department of Defense (DoD) Defense Federal Acquisition Regulations (DFARs) Subpart 239.73 (Requirements for Information Relating to Supply Chain Risk).¹³

Further, we request that USTR recognize and address well-documented standard-essential patent (SEP) licensing abuses in its efforts to advance U.S. supply chain resilience in trade negotiations, enforcement, and other initiatives. Long-standing evidence shows that a minority of well-resourced, and opportunistic SEP holders, including non-practicing entities (NPEs), abuse their monopoly positions by discarding the voluntary fair, reasonable, and non-discriminatory (FRAND) commitments they have made in order to attain unreasonable terms and excessive royalty rates. 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 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

⁶ <https://www.iso.org/standard/45654.html>.

⁷ <https://www.iso.org/standard/74400.html>.

⁸ <https://www.commoncriteriaportal.org/>.

⁹ <https://www.nist.gov/cyberframework>.

¹⁰ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

¹¹ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf>.

¹² <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf>.

¹³ http://www.acq.osd.mil/dpap/dars/dfars/html/current/239_73.htm.

the SEP has been discouraged on a global scale.¹⁴ 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.¹⁵ SEP licensing abuses impact mature supply chains, which is evident in the automotive sector. 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.

Numerous intellectual property rights policies of 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)¹⁶ and European Union (EU),¹⁷ have distorted the meaning of the FRAND commitment, creating an imbalance that heavily favors SEP holders by, for example, routinely enabling prohibitive orders (injunctions) for FRAND-committed SEPs. 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).¹⁸ 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 jurisdictions to exercise extrajudicial authority on patents outside their purview;¹⁹ 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

¹⁴ *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.”).

¹⁵ See *Continental Automotive Systems v. Avanci, LLC*, No. 20-11032 (5th Cir. 2022).

¹⁶ See *Unwired Planet International Ltd v. Huawei Technologies Co. Ltd* (SCUK 2020).

¹⁷ 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.

¹⁸ Lemley, Mark A. and Shapiro, Carl, Patent Holdup and Royalty Stacking. 85 *Texas Law Review* 1991 (2007).

¹⁹ 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/>.

implementing standards users into unreasonable licensing terms, despite their FRAND obligation.

USTR action is needed to mitigate established and prevalent bottlenecks in FRAND 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. If U.S. stakeholders are unable to develop technologies in their home country without fear of potential and likely suits from opportunistic SEP holders, many inventors will forgo production. To illustrate the broad reach of SEP abuses and their impacts on supply chains, we urge USTR (and other policymakers) to carefully consider a new cross-sectoral letter reflecting broad consensus across key U.S. stakeholders, which we include for the record as an appendix to our post-hearing comments.²⁰

The App Association reiterates its appreciation for USTR's efforts to improve the resiliency of U.S. supply chains. By understanding how digital trade and standards issues interact with the electronic components of physical supply chains, USTR can strengthen the supply chains relied upon by American businesses. Thank you for the opportunity to provide our perspective on this important matter.

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

²⁰ This letter is included as Appendix A to this comment.