January 30, 2023

Mr. Daniel Lee
Assistant U.S. Trade Representative for Innovation and Intellectual Property
Office of the United States Trade Representative
600 17th Street NW
Washington, District of Columbia 20036

RE: ***Input of ACT | The App Association regarding the U.S. Trade Representative's Request for Comments and Notice of Public Hearing Regarding the 2023 Special 301 Review [USTR-2022-0016]***

Dear Mr. Lee:

ACT | The App Association (App Association) writes in response to the Office of the United States Trade Representative's (USTR) request to identify countries that deny adequate and effective protection of intellectual property rights (IPR) or deny fair and equitable market access to U.S. persons who rely on IPR protections, to inform USTR's 2023 Special 301 Report.[1]

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 entertainment products such as streaming video platforms, video games, and other content portals that rely on intellectual property protections. The value of the ecosystem the App Association represents—which we call the app ecosystem—is approximately $1.7 trillion and is responsible for 5.9 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[2]

[1] 87 Fed. Reg. 76660.

[2] The App Association, State of the U.S. App Economy 2020, 7th Ed.,https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf.

I. General Comments

The global digital economy holds great promise for small app development companies, but our members face a diverse array of trade barriers when entering new markets. These barriers may take the form of laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of domestic goods and services, or fail to provide adequate and effective protection of IPR. While these barriers have different forms, they all have the same net effect: impeding U.S. exports and investment at the expense of American workers. Such trade barriers include:

- ***Intellectual Property Violations***: The infringement and theft of IPR (copyrights, trademarks, patents, and trade secrets) present a major threat to our members and the billions of consumers who rely on their digital products and services. Strong but fair protection of intellectual property for copyrights, patents, trademarks, and trade secrets is essential to their businesses.
- ***Limiting Cross-Border Data Flows***: Limiting cross-border data flows hurts all players in the digital economy. The seamless flow of data across economies and political borders is essential to the global economy. In particular, innovative small app development companies rely on unfettered data flows to access new markets and customers.
- ***Data Localization Policies***: Companies expanding into new overseas markets often face regulations that force them to build and/or use local data infrastructure. These data localization requirements seriously hinder imports and exports, as well as jeopardize an economy's international competitiveness and undermine domestic economic diversification. Small app developers often do not have the resources to build or maintain infrastructure in every country in which they do business, which effectively excludes them from global commerce.
- ***Customs Duties on Digital Content***: American app developers and technology companies take advantage of the internet's global nature to reach the 95 percent of customers who are outside the United States. However, the "tolling" of data across political borders with the intent of collecting customs duties directly contributes to the balkanization of the internet and prevents small business digital economy innovators from entering new markets.
- ***Requirements to Provide Source Code for Market Entry:*** Some governments have proposed or implemented policies that make legal market entry contingent upon the transfer of proprietary source code. For app developers and tech companies, intellectual property is the lifeblood of their business, and the transfer of source code presents an untenable risk of theft and piracy. These requirements present serious disincentives for international trade and are non-starters for the App Association's members.
- ***Requirements for "Backdoors" in Encryption Techniques:*** Global digital trade depends on technical data protection methods and strong encryption techniques to keep users safe from harms like identity theft. However, some governments and companies insist that "backdoors" be built into encryption for the purposes of government access. These policies would degrade 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 security and privacy standpoint, the viability of app developers' products depends on the trust of end users.

- ***Ill-Advised Regulatory Interventions into Digital Platform Functions and Utilities:*** 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 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 will upend this harmonious relationship enjoyed by small-business app developers and mobile platforms, inhibit proven measures for the enforcement of IP, undermine consumer privacy, and ultimately serve as significant trade barriers.

The infringement and theft of IP online threatens consumer welfare by undermining the ability of creators of digital content to innovate, invest, and hire. App developers that drive the global economy are subject to an estimated loss of $3-4 billion in revenue annually due to pirated apps[3] and IPR violations. Between 2013 and 2018, App developers and publishers lost an estimated $17.5 billion to pirated apps.[4] Loss of revenue presents a major threat to the success of the App Association's members, their consumers, and the workforce that supports the creation and growth of digital products and services. Each kind of IPR (copyrights, trademarks, patents, and trade secrets) represents distinct utilities upon which App Association members depend. IPR violations lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone is a potential "end-of-life" occurrence for a small app development company. Common IPR violation scenarios include:

- ***Copying of an App***: An infringer will completely replicate an app but remove the digital rights management (DRM) component, enabling them to publish a copy of an app on illegitimate websites or legitimate app stores.
- ***Extracting and Illegally Reusing App Content****:* An infringer will steal content from an app—sounds, animations, characters, video, and the like—and repurpose it elsewhere or within their own app.
- ***Disabling an App's Locks or Advertising Keys****:* An infringer will change advertising keys to redirect ad revenue from a legitimate business to theirs. In other instances, they will remove locked functions like in-app purchases and security checks meant to prevent apps from running on devices with removed software restrictions (jailbroken devices).
- ***"Brand-Jacking" of an App****:* An infringer will inject malicious code into an app that collects users' private information and republishes a copy of the app. The republished app looks and functions like the original—often using the same name, logo, or graphics–ultimately luring customers who trust the brand into downloading the counterfeit app and

[3]*See generally*, Forbes, "The Mobile Economy Has a $17.5B Leak: App Piracy" (February 2, 2018), *available at* https://www.forbes.com/sites/johnkoetsier/2018/02/02/app-publishers-lost-17-5b-to-piracy-inthe-last-5-years-says-tapcore/#740b2fdf7413.

[4] Forbes, *The Mobile Economy Has a $17.5B Leak: App Piracy,* February 2, 2018,https://www.forbes.com/sites/johnkoetsier/2018/02/02/app-publishers-lost-17-5b-to-piracy-in-the-last-5-years-says-tapcore/#18a906f87413

putting their sensitive information at risk. A survey of App Association members indicates that one-third of sampled members with trademarks have experienced brand-jacking.[5]

- ***Sideloading of an App***: Piracy has rapidly adapted to new technologies in the app ecosystem and, in some instances, has artificially capped customer beneficial use of digital platforms - with 80 percent of piracy attributable to illegal video streaming through devices and apps.[6] Apps themselves have become the conduit through which all other content is pirated. The reality is that apps providing access to pirated movies, music, and television are available on all platforms, although less so on mobile platforms thanks in large part to app store prohibitions on content piracy and measures to prevent sideloading (downloading software onto a smart device from outside the main app store). A report by the Digital Citizens Alliance on ad-supported piracy highlighted several examples of apps being used to provide free access to content. Apps like MyMuzik and YTSMovies are just two of hundreds of results from a simple search for "free streaming apps." Some piracy apps, such as Cine Vision V5 and MegaFlix have outperformed legitimate applications by stealing their streaming content.[7] Piracy, like illegal streaming, is costing content owners billions each year.
- ***Misappropriation of a Trademark to Intentionally Confuse Users****:* Disregarding trademark rights, an infringer will seek to use an app's name or trademarked brand to trick users into providing their information to the infringer for exploitation.
- ***Illegal Use of Patented Technology***: An infringer will utilize patented technology in violation of the patent owner's rights. Our members commonly experience such infringement in both utility patents and design patents (e.g., graphical user interfaces).
- ***Government Mandated Transfer of IPR To Gain Market Entry****:* A market regulator will impose joint venture requirements, foreign equity limitations, ambiguous regulations and/or regulatory approval processes, and other creative means (such as source code "escrowing") that force U.S. companies to transfer IPR to others in order to access their market.
- ***Government Failure to Protect Trade Secrets****:* An infringer will intentionally steal a trade secret, and subsequently benefit from particular countries' lack of legal protections and/or rule of law. The victim of the theft will be unable to protect their rights through the legal system.

In addition, the App Association notes our growing concern with third-party litigation funding (TPLF) used as a mechanism to abuse patent process in the United States and internationally against U.S. companies. While this issue is faced globally, we focus on its impact to the U.S. market. Non-practicing entities (NPEs) initiate a majority of the abusive and frivolous patent

[5] Survey Says: IP is Essential to Innovation (June 21, 2022), https://actonline.org/2022/06/21/survey-says-ip-is-essential-to-innovation/.

[6] David Blackburn, PH.D. et. al., Impacts of Digital Video Piracy On The U.S. Economy (June 2019), https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf.

[7] Ernesto Van der Sar, 'Pirate' Streaming Apps Beat Netflix and Disney in Brazil's Play Store (June 16, 2022), https://torrentfreak.com/pirate-streaming-apps-beat-netflix-and-disney-in-brazils-play-store-220616/.

infringement suits in the United States[8] and it has recently been revealed that many NPE suits are financially backed by unnamed investors hidden through shell corporations or wealth funds that may have a real interest in the outcome of litigation.[9] TPLF has affected critical U.S. technology industries, including telecommunication, automotives, and semiconductors. Funders may be individual entities seeking economic gain or competing countries strategically undermining essential U.S. industries and U.S. national security. The serious harms to the U.S. market evidenced by TPLF will undermine equity for U.S. businesses, workers, and consumers. We urge the USTR to consider all potential motivations of TPLF and how to address its abusive presence in the U.S. IP system and in IP systems around the world that are utilized by U.S. companies. The availability of anonymous investment sources enables bad actors to flood adjudicating bodies with potentially illegitimate claims. The inception of the Unified Patent Court (UPC) in Europe will likely escalate this issue by allowing abusers to engage in multi-jurisdictional litigation and collect significant damages from European and U.S. companies that allegedly infringe on European patents. USTR should lead the U.S. government (USG) in examining the motivations of individual entities and competing economies to use TPLF and adopting strong disclosure requirements in all relevant U.S. venues, including the U.S. International Trade Commission (USITC), the U.S. Patent and Trademark Office (USPTO), and the U.S. federal courts. The USTR should similarly encourage affected foreign jurisdictions to adopt the same or similar requirements to ensure full transparency in global IP litigation proceedings.

Section 182 of the Trade Act requires USTR to identify countries that deny adequate and effective IPR protections.[10] The Trade Act also requires USTR to identify which countries, if any, are Priority Foreign Countries that demonstrate subpar IPR protections for U.S. companies and citizens.[11] Pursuant to the relevant provisions of the Trade Act,[12] the App Association is pleased to provide its recommendations to this year's Priority Watch List and Watch List. We support efforts by the U.S. government to protect American small businesses that rely on IPR to innovate and need certainty in the protection of their IPR abroad. We commit to partnership efforts with USTR to create responsible IPR protections across the globe to help our members enter new markets and create more U.S. jobs.

[8] 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), 17, https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2020/wp_tse_1160.pdf/.

[9] *See In re Nimitz Technologies LLC*, No. 23-103 (Fed. Cir. 2022).

[10] 19 U.S.C. § 2242.

[11] *See id.*

[12] 19 U.S.C. § 2411-2415.

II. Countries that Should Be on, or Remain on, USTR's Priority Watch List

A. Australia

In 2020, the Australian Competition and Consumer Commission (ACCC) launched its Digital Platform Services Inquiry at the behest of the Australian government.[13] ACCC provided the Australian government's Treasurer with an interim report on the inquiry on September 30, 2020,[14] and is required to provide further interim reports every six months until the inquiry concludes with a final report, to be provided to the Treasurer by March 31, 2025. The App Association has provided detailed views on digital platforms and competition, as well as reactions and feedback on specific conclusions raised by ACCC in its September 2022 interim report[15] and has participated in a stakeholder hearing that took place in June 2022. The App Association has significant concerns with ACCC's apparent positioning of Australian government to interject itself into the digital economy without an evidence base to support such an intervention, which would jeopardize the functionality of mobile operating systems and software distribution platforms that have enabled countless American small businesses to grow. We therefore request that the ACCC's inquiry into digital platform services, and the risks it poses to American small business innovators that rely on software distribution platforms, be captured in the 2023 NTE report, and that the U.S. government work with Australia to mitigate the risks such an intervention would pose while supporting U.S. small business digital economy trade and leadership.

B. China

Theft and infringement, which increasingly originates in China, puts our members' businesses and the jobs they create at serious risk. In many cases, a single IPR violation can represent an "end-of-life" scenario for small businesses and innovators. Numerous Chinese government laws and policies have a negative impact on our members, who have experienced IPR infringement in the Chinese market in each of the common scenarios described above. Overall, our members view the business environment in China as a continued challenge, largely driven by a lack of confidence in IPR protections.

[13] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25.

[14] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25/september-2020-interim-report.

[15] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25/september-2022-interim-report

Notable examples include the Chinese government's application of the controversial "essential facilities" doctrine to IPR in the State Administration for Industry and Commerce's (SAIC)[16] Rules on Prohibition of Abusing Intellectual Property Rights to Eliminate or Restrict Competition (IP Abuse Rules), which took effect on August 1, 2015. Article 7 of SAIC's IP Abuse Rules states:

> Undertakings with dominant market position shall not, without justification, refuse other undertakings to license under reasonable terms their IPR, which constitutes an essential facility for business operation, to eliminate or restrict competition. Determination of the aforesaid conduct shall consider the following factors:
>
> (i) whether the concerned IPR can't be reasonably substituted in the relevant market, which is necessary for other undertakings to compete in the relevant market;
>
> (ii) whether a refusal to license the IPR will adversely affect the competition or innovation of the relevant market, to the detriment of consumers' interest or public interests;
>
> (iii) whether the licensing of the IPR will not cause unreasonable damage to the licensing undertaking.

The App Association does not support the notion that competitors should have access to "essential" patents (outside of the standardization context, as discussed below) because they allegedly cannot compete without such access, even in the rare cases where there is little damage to the IP holder, or consumer interests are allegedly harmed by lack of competition. This provision seriously undermines the fundamental right to exclude others from using one's intellectual property, and thus affects incentives to innovate in the long term. Under this provision, U.S. innovators, particularly those with operations in China, are left vulnerable because SAIC uses significant discretion to balance the necessary factors to determine the issuance of a compulsory license.

The App Association notes the critical differences between regular patents and standard-essential patents (SEPs), which must be considered separately. Generally, seamless interconnectivity is made possible by technological standards, such as Wi-Fi, LTE, and Bluetooth. Companies often collaborate to develop these standards by contributing their patented technologies. These technological standards, which are built through an open and consensus-based process, bring immense value to consumers by promoting interoperability while enabling healthy competition between innovators.

[16] While its functions (along with a number of further Chinese agencies) have since been consolidated under the State Administration for Market Regulation, the SAIC rules have not yet been replaced by SAMR.

When a patent holder lends its patented technology to a standard, it can result in a clear path to royalties in a market that likely would not have existed without the wide adoption of the standard. To balance this growth potential with the need to access the patents that support the standard, many standard development organizations (SDOs) require patent holders of standardized technologies to license their patents on fair, reasonable, and non-discriminatory (FRAND) terms. FRAND commitments prevent the owners of SEPs, the patents needed to implement a standard, from exploiting the market power that results from the broad adoption of a standard. Once patented technologies are incorporated into a standard, manufacturers are compelled to use them to maintain product compatibility. In exchange for making a voluntary FRAND commitment with an SDO, SEP holders can obtain reasonable royalties from manufacturers that produce products compliant with the standard, which may not have existed absent the standard. Without a FRAND commitment, SEP holders would have the same power as a monopolist that faces no competition. In line with our members' core interests in this area, the App Association has established an initiative known as "All Things FRAND"[17] to assist policymakers, including USTR, in understanding SEP FRAND issues and developments; the App Association has further adopted and advocates for several key consensus principles to prevent patent "hold-up" and anti-competitive conduct which are available on the All Things FRAND website.[18]

Specific to China and SEPs, the App Association acknowledges that certain entities like the Standardization Administration of China have attempted to publish policies that would have instructed Chinese-backed standardization bodies to lower or undermine royalty payments for patents, without differentiating between FRAND-encumbered SEPs and other patents. With assistance from the international community, such efforts have been thwarted. Today, SAIC's IPR Rules appropriately recognize that it may be an abuse of dominance for SEP holders to eliminate or restrict competition, "such as by refusing to license, tying or imposing other unreasonable trading terms, in violation of fair, reasonable, and non-discriminatory principle." In contrast to its policies on patents generally, SAIC's treatment of FRAND-encumbered SEPs is consistent with an emerging consensus on how to deal with serious breaches of FRAND commitments. We strongly urge USTR to ensure that it does not conflate general patent licensing issues with the unique set of issues and global competition law consensus specific to SEPs.[19] In 2020, China's State Administration for Market Regulation (SAMR) released four new Guidelines as part of a book of Chinese antitrust regulations and guidelines and related legal and regulatory documents, one of which is *Guidelines on Anti-monopoly in the Field of Intellectual Property* (国务院反垄断委员会关于知识产权领域的反垄断指南). Notably Article 27 addresses "Special Issues in SEPs," and though no official English translation is available, this Article appears to align with the global norms for SEP law and policy that the App Association identifies elsewhere in this comment.

The USTR should consider its position on anti-suit injunctions (ASIs), particularly as it relates to the European Union's (EU's) recently filed request for dispute settlement at the World Trade Organization (WTO) against the People's Republic of China (China). A blanket condemnation of

[17] *See* http://allthingsfrand.com (international resource and repository for information and developments involving SEPs, including completion law issues and actions).

[18] *See Principles for Standard Essential Patents*, ABOUT ALLTHINGSFRAND.COM (last accessed January 28, 2021), *at* https://allthingsfrand.com/about/.

[19] To illustrate the scope of this consensus, the App Association has developed a non-exhaustive list of developments from across key economies, which can be viewed in comments filed by the App Association before the Japan Patent Office. *See* pgs. 5-12 of http://actonline.org/wp-content/uploads/ACT-Comments-re-JPO-SEP-Licensing-Guidelines-final-111017.pdf.

ASIs would be detrimental to U.S. companies, U.S. consumers, and ultimately U.S. interests more broadly. ASIs are properly exercised as an essential instrument to preserve jurisdiction by prohibiting a party in litigation from pursuing foreign parallel proceedings on the same dispute. The use of ASIs in litigation has been a long-standing practice of U.S. courts in many areas of the law, including in cases involving SEPs.[20] U.S. case law demonstrates that ASIs are appropriate on a case-by-case basis and under a carefully balanced legal test.[21] For example, in *Microsoft v. Motorola*, a federal district court issued an ASI to prevent Motorola from pursuing injunctive relief against Microsoft in Germany after Microsoft filed a breach of contract claim case against Motorola in the United States and agreed to pay a FRAND royalty determined by the court for Motorola's portfolio.[22] Therefore, the issuance of an ASI by the court of any one country is not evidence of the country's unwillingness to provide adequate and effective protection of intellectual property rights.

While the global community has expressed a strong concern about Chinese courts' use of ASIs to obstruct transparent and fair judicial process,[23] we strongly encourage USTR to distinguish this procedural posture as a country-specific possibility separate from the determination to issue ASIs *per se*. The recent issuance of ASIs by Chinese courts can be explained as a symptom of courts in the EU and the UK that attempt to assert jurisdiction over disputes involving Chinese patents. In fact, many countries have begun to use ASIs in the SEP context in order to prevent courts from asserting jurisdiction outside their purview – in many cases without any assessment whether the requested rates and terms are FRAND or whether the jurisdiction to assess the essentiality, validity, or value of foreign patents exists.[24] U.S. courts have similarly granted ASIs to enjoin SEP-holders from enforcing their patent rights in member states of the European Union.[25] A prime example of this overreaching jurisprudence is *Unwired Planet International Ltd v. Huawei Technologies Co. Ltd* (SCUK 2020), where the U.K. Supreme Court approved the issuance of injunctions barring defendants from participating in the U.K. market unless they agreed to court-determined *global* portfolio SEP licenses, which included foreign patents outside the jurisdiction of the U.K. courts.[26] German courts, too, have issued injunctions against defendants in disputes involving global portfolio SEP licenses;[27] they have also issued "anti-anti-

[20] Peter K. Yu, George L. Contreras, and Yu Yang, *Transplanting Anti-suit Injunctions*, 71 AM. U.L. REV. 1537, 21 n. 121 (2022), https://aulawreview.org/blog/transplanting-anti-suit-injunctions/.

[21] *See Microsoft v. Motorola*, 696 F.3d 872 (9th Cir. 2012).

[22] *Id*.

[23] OFF. OF THE U.S. TRADE REPRESENTATIVE 2021 SPECIAL 301 REPORT 47 (2021) ("[r]ight holders have...expressed strong concerns about the emerging practice in Chinese courts of issuing [ASIs] in [SEP] disputes, reportedly without notice or opportunity to participate in the injunction proceedings for all parties.")

[24] *See e.g.*, the dispute between Sharp, a Japanese patent-holder, and Oppo, a Chinese handset manufacturer towhich the EU's complaint refers.

[25] *Microsoft Corp v Motorola Inc*, 871 F. Supp. 2d 1089 (W.D. Washington 2012); *Huawei Technologies Co Ltdv Samsung Elecs Co Ltd*, Case No 3:16-cv-02787 (N.D. California 2018); *TCL Comm Tech Holdings Ltd v Telefonaktiebolaget LM Ericsso*n, Case No 8:14-cv-00341 (C.D. California 2017).

[26] *Unwired Planet International Ltd v. Huawei Technologies Co. Ltd* (SCUK 2020).

[27] *See Huawei Technologies Co. v. ZTE Deutschland GmbH* (CJEU 2015); *see Sisvel International S.A. v. Haier Deutschland GmbH* (FCJ 2020).

suit" injunctions prohibiting litigants from petitioning U.S. courts for ASIs.[28] The increase in ASIs in China and elsewhere is a direct response to these developments.

Chinese courts have issued ASIs in a small number of licensing disputes between handset manufacturers and SEP holders. These disputes all concerned the licensing of SEPs for cellular standards, such as 3G and 4G standards in which the negotiating parties could not agree upon the terms of a license. In all of these cases, the handset manufacturer was of the opinion that the respective SEP holder had refused a license on FRAND[29] terms and had thus breached its contractual FRAND undertaking. Similar to the U.S. case of *Motorola v. Microsoft*, the respective handset manufacturer thus initiated national court proceedings to have the court adjudicate (F)RAND terms of such license (in the following "rate-setting proceedings"). In all of the five cases listed in the EU's complaint at the WTO, the ASI granted by a Chinese court sought to allow the pending rate-setting proceedings before the respective Chinese court to be conducted without external impairment by foreign patent infringement proceedings. Thus, the foreign patent infringement proceedings had to be halted for the Chinese court to conclude the pending rate-setting proceedings. Here, the issuance of an ASI by a Chinese court is also comparable to the case of *Motorola v. Microsoft*, where the court found that "a judicially-determined FRAND license encompassing all of Motorola's H.264 essential patents would necessarily dispose of Motorola's request for an injunction in Germany" as the "issues before it in this litigation were dispositive" of the German patent infringement action, and enjoined Motorola from enforcing the injunction.[30] Chinese courts have modeled their practice of granting ASIs after the well-established U.S. practice and legal framework for ASIs. Chinese courts have therefore ultimately picked up and adopted this "response" that U.S. courts had already developed previously,[31] and that even a court in the European Union itself found to be legitimate in certain, narrow circumstances.[32]

In addition, small app businesses depend on customer trust to grow and create more jobs, an endeavor that can only be maintained using the strongest technical protection mechanisms (TPM) available, including encryption. In cross-sector and sector-specific contexts, the Chinese government continues to threaten the ability to utilize TPMs, primarily encryption. Not only do these requirements jeopardize our members' ability to protect their IPR, but they also threaten the integrity and security of the digital economy.

More broadly, numerous policies in place today or proposed in China create significant market access issues for App Association members who all rely on IPR. Such measures include

---

[28] See Munich H. Regional Ct., Continental Automotive Systems, Inc. v. Avanci LLC, Case Nos. 21 O 9333/19.

[29] Policies of some SSOs require an undertaking to grant licenses on fair, reasonable and non-discriminatory terms, and some policies omit the criteria of "fair". For the purpose of this paper, the terms "FRAND" and "RAND" are used interchangeably.

[30] *Microsoft v. Motorola*, 854 F.Supp.2d 993 (United States District Court for the Western District of Washington, February 27, 2012), affirmed by *Microsoft v. Motorola*, 696 F.3d 872 (United States Court of Appeals for the Ninth Circuit 2012).

[31] *Yu/Contreras/Yu*, Transplanting Anti-suit Injunctions (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3937716).

[32] *Ericsson v. Apple*, KG ZA 21-914, ¶¶ 4.44 (District Court of The Hague, December 16, 2021) with regard to so-called "performance ASIs" for cases in which a party has already a priori restricted its fundamental right toenforce its patent in court, e.g. under a covenant not to sue.

restrictions on cross-border data flows and data localization requirements effected through China's Cybersecurity Law (CSL); vague restrictions and requirements placed on "network providers" with further issues created through standards and measures developed by the Cybersecurity Administration of China pursuant to the CSL; source code disclosure mandates; and foreign direct investment restrictions.

China's encryption rules and cybersecurity laws should be monitored by the USTR and included in the report. On May 11, 2020, China issued the Commercial Encryption Product Certification Catalogue and the Commercial Encryption Certification Measures. Manufacturers of products listed on the catalogue will not be subject to mandatory approval requirements before launching products into the market. The certification is voluntary, but its goal is to serve as an assurance to customers that the commercial encryption products conform to Chinse standards.[33] If effective, App Association members may be able to successfully get their products to customers in China. The certifications remain valid for a five-year period but are subject to further review if the product or entity producing the product undergoes any changes.

Additionally, October 26, 2019, China enacted an Encryption Law, which took effect on January 1, 2020. The new encryption law greatly impacts the regulatory landscape for foreign-made commercial encryption products and leaves unanswered questions surrounding "commercial encryption." For example, the import licensing and export control framework provides an exemption for "commercial encryption" used in "products for consumption by the general population." However, because the law does not sufficiently define either of these terms, businesses are left to speculate on how to apply the law. As a result, app developers will experience legal uncertainty, and App Association members will suffer due to their inability to maintain customers' trust regarding the security of their information. Furthermore, the lack of clear regulations will also prevent American businesses' ability to succeed in China's large consumer market.

China's Cybersecurity Law imposes tough regulations, introduces serious uncertainties, and unreasonably prevents market access for American companies seeking to do business in China. This law is particularly difficult for App Association small business members seeking access to digital markets and consumers in China. The law includes onerous data localization requirements and uses overly vague language when outlining important provisions (such as when Chinese law enforcement bodies can access a business's data or servers or how frequently a business must perform demanding safety assessments). Legal certainty is vital to app developers' operations and their ability to maintain their customers' trust in the protection of their data. In addition to creating obligations that are often infeasible for our members, the Cybersecurity Law's vague language leaves businesses without clear guidelines about how the law will be applied and jeopardizes American businesses' potential to succeed in China's important market. The law requires Critical Information Infrastructure operators to predict the potential national security risks that are associated with their products and services. It includes restrictive review requirements and will most likely cause supply disruptions.[34]

---

[33] Yan Luo and Zhijing Yu, *China Issued the Commercial Encryption Product Certification Catalogue and Certification*, INSIDE PRIVACY, May 15, 2020, available at https://www.insideprivacy.com/data-security/china-issued-the-commercial-encryption-product-certification-catalogue-and-certification/.

[34] Yan Luo and Zhijing Yu, *China Issued the Commercial Encryption Product Certification Catalogue and Certification*, INSIDE PRIVACY, May 15, 2020, https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/

The App Association continues to advocate on behalf of innovative American app developers who actively, or look to, conduct business in China. We have opposed data localization requirements in written comments and have identified numerous areas where China's law uses overly prescriptive and technically and/or economically infeasible mandates to address public safety goals.

The App Association acknowledges that the Chinese judicial system has made some positive steps that lend to increased certainty in IPR protection (e.g., the establishment of specialized IPR courts in Beijing, Guangzhou, and Shanghai; and the standing up of various IP tribunals). The National People's Congress (NPC) made changes to the China Patent Law in 2020 which became effective June 1, 2021.[35] USTR should continue to monitor the impact of these changes, including significant changes to damages calculations in IPR litigation.[36] Additionally, existing agreements between the United States and Chinese governments include commitments to improve IPR enforcement in China.[37] However, across patent, copyright, trademark, and trade secrets, enforcement is often poor and usually unreliable. Due to the continued high amount of infringement originating from China, as well as numerous policies and laws that enable IPR infringement or are selectively enforced, we strongly recommend China remain on the Priority Watch List.

C. European Union

The App Association supports the EU's Digital Single Market (DSM) strategy's goals of opening digital opportunities for businesses and enhancing Europe's position in the digital economy. While the DSM benefits European businesses by facilitating business across the EU through e-commerce, it should also bring Europe into the global digital market. The App Association has advocated for the success of the DSM through measures such as requirements to store data locally or mandates to diminish the use of strong encryption.

We encourage USTR to remain engaged on this sweeping strategy. The European Commission has already carried forward numerous regulations, directives, consultations, and proposals under the DSM that raise significant concerns for the App Association, including:

- A range of competition-themed activities and policies focused on the EU's "digital sovereignty" that stand to cause damage to the digital economy and American small businesses' ability to operate in the EU.[38]
- Regulation of online platforms, via the Digital Markets Act (DMA),[39] intending to address contractual clauses and trading practices in relationships between platforms and

[35] Aaron Wininger, *China's National People's Congress Releases Translation of the Amended Patent Law*, NAT'L L. R. (Sept. 17, 2021), https://www.natlawreview.com/article/china-s-national-people-s-congress-releases-translation-amended-patent-law.

[36] Aaron Wininger, *Top 5 Changes in China's Newly Amended Patent Law*, CHINA IP L. UPDATE (Oct. 19, 2020), https://www.chinaiplawupdate.com/2020/10/top-5-changes-in-chinas-newly-amended-patent-law/.

[37] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/december/united-states-and-china-reach

[38] European Commission, *The Digital Services Act package*, *available at* https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

[39] European Commission, *Online Platforms, available at* https://ec.europa.eu/digital-single-market/en/policies/online-platforms.

businesses, poses significant risks to U.S. small business engagement in the global digital economy.[40] Although they may not qualify as gatekeepers, small app developers will suffer significant consequences from the new obligations introduced in the DMA. SMEs are particularly vulnerable if those obligations threaten the tangible advantages currently provided to them by digital platforms. Specifically, the DMA, through mandating sideloading, will prevent digital platforms from taking measures to protect IPR in the digital economy. With the DMA now in place, its impact on IP enforcement in the digital economy represents a significant trade barrier in the context of the 301 Special Report, and should be included in the Special 301 Report to Congress as such.

- Attempts to regulate the free flow of information online through measures such as the EU's Digital Services Act which centers around tackling illegal hate speech with the goal, moving forward, of removing illegal content from the internet.
- Various provisions of the GDPR, which impose additional requirements on non-European firms (due to its extraterritorial reach) that increase the cost and risk associated with handling data pertaining to EU citizens. For example, Article 27 of the law requires firms to physically place a representative in the EU.[41] Such provisions can be an insurmountable hurdle to our small business members seeking to enter the EU market. Anything that can be done throughout the GDPR implementation process to ease the burden for small and medium-sized companies could have tremendously positive economic implications.
- The EU's proposed ePrivacy Regulation, framed as a complement to the GDPR by addressing the rights of EU citizens using any electronic communication services, including IoT devices and OTT communications services, presents further difficulties and complications to small business innovators seeking to reach new EU markets. App Association members do not take lightly the extension of the proposed Regulation's scope to include non-EU companies that process the electronic communications data of EU individuals. While this Regulation is currently in development, we urge that it be included in the Special 301 Report.
- New proposals to enact sweeping regulations on the use of artificial intelligence (AI),[42] which raise concerns for the App Association about regulation pre-empting new and innovative uses of AI.

Each of these concerns contains regulatory proposals for nascent economic segments and services that are solutions in search of a problem and should not move forward. Data-demonstrated public needs should form the basis for activities under the DSM, rather than hypotheticals and edge use cases.

The App Association notes its support for the Administration and the European Commission negotiating a new transatlantic data transfer mechanism, and the Administration's release of an Executive Order supporting the construct. Going forward, we urge the USTR to begin its consideration of an adequacy determination as expeditiously as possible in order to restore

---

[40] https://actonline.org/wp-content/uploads/ACT-The-App-Association-DMA-Position-Paper-March-.pdf.

[41] *See* https://www.privacy-regulation.eu/en/27.htm.

[42] Digital Single Market: Artificial Intelligence, European Commission, last updated September 27, 2021. https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

transatlantic data flows and ease the burden on our small business members seeking to compete in the global economy.

D. India

India represents an immense opportunity for American small business tech and software development companies. However, App Association members continue to experience a wide range of IPR infringement and lack of legal redress, despite ongoing (incomplete) efforts across Indian ministries and courts that appear to lend themselves to a more consistent and reliable IPR regime in the country. Ongoing problems in this key market include but are not limited to:

- A marked lack of copyright protections and enforcement;
- A failure to provide consistent protection for trade secrets across India; and
- Data storage and processing localization requirements imposed on small businesses that can require unfettered access to data (including IP), a non-starter for App Association members.

Certain steps indicate the Indian government's willingness to adequately protect IPR. For example, the Indian government undertook efforts to further its commitment to formally establish a copyright royalty board and appoint a functional IP Appellate Property Board. Under the Finance Act of 2017, the informal Copyright Board merged with the Intellectual Property Appellate Board. As a result, applications for copyrights increased by 78 percent from 2016-2017, compared to 2015-2016.[43] As of May 20, 2016, the Indian government established additional commercial courts, advancing the 2015 Commercial Courts Act,[44] which the App Association perceives as further evidence of India's commitment to enhance its IPR procedures. Furthermore, India acceded to the WIPO Internet Treaties in July 2018 (namely the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty). The Indian government also appears committed to the IPR Task Force announced by the Maharashtra government. As of January 24, 2018, Cell for IPR Promotion and Management (CIPAM) and Federation of Indian Chambers of Commerce & Industry (FICCI) have made an IPR Enforcement Toolkit for Police, and there have been 26 programs dedicated to training police officers on IP enforcement. Despite this positive movement, App Association members experience weak and ineffective enforcement in India.

Moreover, numerous hurdles to market access, either in place today or proposed, restrict market access for App Association members that rely on IPR, including but not limited to data localization requirements and in-country cybersecurity testing mandates. For example, on November 18, 2022, the Digital Personal Data Protection Bill[45] replaced the Personal Data Protection Bill, withdrawn on August 4, 2022. The new bill was proposed by the Ministry of Electronics and Information Technology to provide a legal framework for the liabilities and protections associated with the collection and processing of personal digital data. One issue of note with India's Digital Personal Data Protection Bill is that the bill give's India's central government the power to exempt any agency from the bill's requirements on grounds related to national security, national sovereignty, and public order. If passed, the Digital Personal Data Protection Bill has the potential

[43] https://spicyip.com/wp-content/uploads/2018/01/IPR-Regime-In-India-Government-Initiatives.pdf.

[44] https://timesofindia.indiatimes.com/city/delhi/Commercial-courts-begin-functioning-in-Delhi-Mumbai/articleshow/52488068.cms.

[45] https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.

to create technical issues that raise small businesses' compliance costs. For the small business innovators, the App Association represents, the imposition of this new law presents the possibility of damaging the use case for market entry.

App Association members continue to experience IP infringement originating from India, and face challenges in enforcement through the Indian system. India has not yet implemented its obligations under the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty; furthermore, Indian patent law is inconsistent with the TRIPS Agreement. Another troubling development is the Indian government's proposal decriminalizes provisions in the Patent Act and the Copyright Act.[46] This proposal threatens copyright protections that aim to protect small businesses and innovators alike.

The App Association believes it is necessary that India remain on the Priority Watch list because of its need to further develop an adequate IPR system and to demonstrate consistent enforcement.

E. Indonesia

While the Indonesian government has taken steps to improve IPR enforcement, Indonesia continues to present challenges with respect to IPR protections and enforcement mechanisms that translate into a barrier to entry for U.S. small business innovators in the Indonesian market. For example, its revision of Indonesian trademark law in November 2016 demonstrates a positive step forward to advance the rights of trademark holders through shorter examination times and better criteria for protected marks. In addition, Indonesia joined the Madrid Protocol in January 2018.

However, there are still ongoing concerns with whether the recent provisions will be adequately enforced and there has been minimal progress in integrating USTR's suggested reforms in its 2018 review. For example, Indonesia has apparently not yet created a specialized IPR unit within its National Police to enforce against Indonesian criminal syndicates that create counterfeit and pirated marks and works. Indonesia's 2016 revisions to its Patent Law continue to raise concern. Indonesia's revised Patent Law included localization rules that require foreign patentees to transfer proprietary technologies to local companies, which, in effect, forces American companies with products in Indonesia to protect their rights. Certainty in enforcement is lacking and continues to present challenges.

Furthermore, numerous hurdles to market access, either in place today or proposed, restrict market access for App Association members that rely on IPR, including but not limited to various local presence requirements; data localization requirements for public sector data; and—of highest concern to the App Association—amendments to Indonesia's Harmonized Tariff Schedule to categorize "software and other digital products transmitted electronically," setting the stage for subjecting e-commerce to customs duties. We also continue to monitor Indonesia's new E-Commerce Regulation, issued in November 2019, that may impose restrictions on the flow of data

Based on the above, the App Association recommends Indonesia remain on USTR's Priority Watch List.

[46] Surojit Gupta, *Govt Moves to Decriminalise Minor Offences to Woo Investors*, June 12, 2020, https://timesofindia.indiatimes.com/india/govt-moves-to-decriminalise-minor-offences-to-woo-investors/articleshow/76331374.cms.

F. Republic of Korea

In September of 2021, the Republic of Korea's (ROK's) legislature passed the Telecommunications Business Act, which intervenes into the operation of app stores based on undemonstrated claims of harm to app developers and mandates platforms' support of third-party payment systems to process the sale of digital products and services. The Telecommunications Business Act stands to benefit a small number of global brands including Spotify, Epic Games, and Tile, while also freezing out small business app developers in the ROK and around the world that can't pivot so quickly. App Association members demand, and realize in today's leading platforms, platform-level privacy and security measures, appropriate and timely removal of fraudsters and copyright thieves, and rigorous vetting of any new software. These characteristics are essential to maintain an ecosystem consumers trust enough to download apps from companies without name recognition. Therefore, the Telecommunications Business Act prohibits core platform functions, including those that will protect IPR in the digital economy, that benefit our members and consumers and should be of immense concern to USTR in light of its negative impact on U.S. small business digital economy innovators. We recommend that this development in the ROK be reflected in the Special 301 Report, and that it be accurately characterized as a means of denying adequate and effective protection of IPR, as well as a denial fair and equitable market access to U.S. small businesses who rely on IPR protections.

G. Russia

The Russian market continues to present massive challenges to App Association members. Unfortunately, Russia has continued to foster an environment that permits extensive software piracy. The Russian government does not appear to be committed to making any systemic changes to protect IPR and has actively encouraged the infringement of patented technologies.[47]

The App Association therefore urges USTR to keep Russia on the Priority Watch List.

H. United Kingdom

In the case *Unwired Planet v. Huawei*,[48] the United Kingdom Supreme Court recently upheld an injunction prohibiting the sale of wireless telecommunications products in Britain due to a party's failure to enter a patent license for Unwired Planet's worldwide portfolio of SEPs, even though the party was willing to enter into a license for UK SEPs. The ruling also states that the plaintiff did not violate EU competition law by seeking an injunction for infringement of its UK SEPs, even though those SEPs were subject to a commitment to license on FRAND terms. Controversially, the ruling rejects antitrust liability in concluding that a SEP holder's insistence on only agreeing to a worldwide license is consistent with its FRAND obligation. If a single patent in a single jurisdiction can be used to obtain an injunction unless the alleged infringer enters a worldwide license, SEP owners will be highly incented to engage in global forum shopping, depressing the ability for American innovators like App Association members to compete abroad.

The *Unwired Planet* decision presents grave risks to those who rely on standards to innovate and threatens U.S. sovereignty by holding that a UK court can preempt U.S. law in mandating worldwide FRAND licensing, presenting a major barrier to trade for American small businesses in

[47] https://www.economist.com/business/2022/06/02/has-russia-legalised-intellectual-property-theft.

[48] https://www.supremecourt.uk/cases/docs/uksc-2018-0214-judgment.pdf.

the digital economy and IoT that rely on standards to innovate and compete. The App Association strongly encourages the U.S. government to address this harmful development by including it in the Special 301 Report, within the ongoing U.S.-UK Free Trade Agreement negotiation, and through other avenues.

Additionally, the *Optis v. Apple* case seems to be compounding the damage caused in *Unwired Planet*. In any other business situation, a company would not agree to sign a contract without knowing what's in it, and it should be no different for SEP licensing agreements. Further, the extraterritorial application of court-determined royalty rates both harms the ability of parties to negotiate FRAND terms for licensing SEPs and discourages American businesses from operating in the UK due to the risk of having worldwide royalty rates set by the court there.

Given the impact of the above-described developments in the UK, we strongly recommend that the Special 301 Report accurately capture and characterize them as means of denying adequate and effective protection of IPR, as well as a denial fair and equitable market access to U.S. small businesses who rely on IPR protections.

I. Vietnam

Vietnam continues to present challenges to App Association members with respect to IPR policies and enforcement, where inadequate frameworks and inconsistent enforcement undermine confidence. With respect to market access, Vietnam has enacted rules that impose data localization requirements and restrictions on encryption. Even more recently, Vietnam's new Cybersecurity Law, containing many of the same requirements as China's Cybersecurity Law discussed above, went into effect, further disincentivizing market entry.

The App Association therefore encourages USTR to keep Vietnam on its Priority Watch List.

III. Conclusion

The App Association appreciates the opportunity to submit these comments to USTR, and welcomes the opportunity to assist the Administration further.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Priya Nair
Intellectual Property Policy Counsel

Leanna Wade
Public Policy Associate

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