October 28, 2022

*Submitted via Electronic Mail to www.regulations.gov*

Trade Representative Policy Staff Committee
Office of the U.S. Trade Representative
600 17th Street, N.W.
Washington, District of Columbia 20036

**RE: Comments of ACT | The App Association on Significant Foreign Trade Barriers for the 2023 National Trade Estimate Report**

In response to the Federal Register notice issued on September 15, 2022,[1] ACT | The App Association hereby submits comments to the United States Trade Representative (USTR) in response to its request for public input on the 2023 National Trade Estimate (NTE) Report on Foreign Trade Barriers report.

The App Association represents thousands of small business innovators and startups in the software development and high tech space located across the United States.[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, which today represents an economy worth more than $1.7 trillion annually and that provides over 5.9 million American jobs.[3]

While the global digital economy holds great promise for App Association member companies, our members face a diverse array of challenges when entering new markets. These challenges, commonly referred to as "trade barriers," reflect in the laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of particular domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights. These barriers take many forms but have the same net effect: impeding U.S. exports and investment.

---

[1] Office of the United States Trade Representative, *Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report*, 86 FR 51436 (September 15, 2021), *available at* https://www.federalregister.gov/documents/2021/09/15/2021-19934/request-for-comments-on-significant-foreign-trade-barriers-for-the-national-trade-estimate-report.

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

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

We applaud USTR's efforts to understand and examine the most important foreign barriers affecting U.S. exports of goods and services, foreign direct investment, and intellectual property rights. We commit to working with USTR and other stakeholders to reduce or eliminate these barriers. With respect to digital trade, 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. Innovative app development companies 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 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:*** 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. Strong but fair protection of intellectual property for copyrights, patents, trademarks, and trade secrets is essential to the success of our members.

- ***Misapplication of Competition Laws to Software Distribution Platforms:*** 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.

We also wish to draw attention to activities in certain international fora that are responsible for the creation of potential digital trade barriers or seek to legitimize policies that inhibit digital trade. For example, the App Association is a leading advocate against efforts within the United Nations' International Telecommunications Union (ITU) to develop pro-regulatory approaches to "over-the-top" (OTT) services – any service accessible over the internet or utilizing telecommunications network operators' networks.[4] In the ITU, the App Association worked to highlight the benefits of OTT to economies of all sizes across sectors. We continue to work to educate the public and other governments on how a new layer of regulation over OTT services will stifle growth, and we continue to oppose pro-regulatory OTT service proposals. The App Association has called on the ITU to seek consensus across stakeholder groups to reduce barriers to the digital economy, which will benefit of the billions of internet users around the globe. We recommend that the Trade Policy Staff Committee include the concerning proposals from international fora like the ITU that would inhibit the free flow of data and digital commerce in the NTE.

Below, we highlight numerous country-specific trade barriers that our members face, and we urge their inclusion in the Trade Policy Staff Committee's (TPSC) 2023 NTE report. The practices highlighted below include both implemented and proposed policies, both of which should be considered by USTR.

---

[4] *Comments of ACT | The App Association to the ITU Council Working Group on International Internet-Related Public Policy Issues Regarding its Open Consultation, Public Policy Considerations for OTTs*, ITU, August 18, 2017, *available at* https://www.itu.int/en/Lists/consultationJune2017/Attachments/31//App%20Assn%20Comments%20re%20ITU%20OTT%20Consultation%20081817.pdf.

**AUSTRALIA**

Issue: Improper Application of Competition/Antitrust Laws to Software Distribution Platforms

In 2020, the Australian Competition and Consumer Commission (ACCC) launched its Digital Platform Services Inquiry at the behest of the Australian government.[5] ACCC provided the Australian government's Treasurer with an interim report on the inquiry on September 30,[6] and is required to provide further interim reports every 6 months until the inquiry concludes with a final report, to be provided to the Treasurer by 31 March 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,[7] and has participated in a stakeholder hearing that took place in June 2022. The App Association has significant concerns with ACCC's apparent positioning 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.

**BRAZIL**

Issue: Brazilian General Data Protection Law

The National Congress of Brazil passed the Lei Geral de Proteção de Dados Pessoais (LGPD)[8] in August of 2018. The LGPD was enacted on August 27, 2020, and came into force, allowing for penalties and sanctions to be imposed, on August 1, 2021.[9] Various provisions of the LGPD, much like the European Union's General Data Protection Regulation (GDPR) mentioned below, impose additional requirements on non-Brazilian firms due to its extraterritorial reach that increase the cost and risk associated with handling data pertaining to Brazilian citizens. Furthermore, Article 33-36 does not permit cross-border data transfers based on the controller's legitimate interest. The countries

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

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

[7]

[8] Chris Brook, *Breaking Down LGPD, Brazil's New Data Protection Law*, DATAINSIDER, June 10, 2019, available at https://digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law#targetText=What%20is%20the%20LGPD%3F,scheduled%20date%20of%20February%202020.

[9] Robert Healy, *The Brazil LGPD: How Organizations Can Ensure Compliance*, LEXOLOGY, Oct. 7, 2021, available at https://www.lexology.com/library/detail.aspx?g=465b3d85-2f7d-40a2-aa19-b200cb819f8a.

with which cross-border data transfers will be allowed has not been determined yet, and the App Association urges USTR to advocate for the United States' inclusion on the list of permitted countries.[10] The feasibility of the LGPD hinges on its implementation, which could present insurmountable hurdle to our small business members seeking to enter the Brazilian market. We urge U.S. government to work with the Brazilian government to ensure that LGPD's implementation proceeds down a reasonable pathway to mitigate barriers to trade and market entry.

Issue: Patent Prosecution

The Brazilian government implemented a Patent Prosecution Highway program to address its patent examination backlog.[11] This program was extended through December 24, 2024, increasing the allowed frequency of applications to the program and explicitly denying the ability to appeal rejections.[12] It is important for Brazil to enter into compliance with the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement because the current standards of patentability are not compatible with international requirements. The App Association encourages USTR to make efforts to ensure that Brazil continues these efforts and meets its international obligations.

Issue: Taxation/Customs Duties on Digital Commerce

Brazil continues to propose adopting new taxes on digital services and commerce that occurs over the internet. Such proposals are immensely concerning to the App Association's community, and contradict global norms (e.g., the WTO's e-Commerce moratorium on customs duties, the OECD's consensus approach to digital economy taxation, etc.).

Issue: Discriminatory Localization Policies

Brazil has made changes to its tax laws with respect to information and communications technology (ICT) and digital goods in response to findings that the laws were in violation of World Trade Organization (WTO) rules, but Brazil's Basic Production Process law continues to inappropriately favor "local content" production of these categories.

[10] Renata Neeser, *Is the Brazilian Data Protection Law (LGPD) Really Taking Off?*, LITTLER, June 7, 2021, available at https://www.littler.com/publication-press/publication/brazilian-data-protection-law-lgpd-really-taking.

[11] Ricardo D. Nunes and Rafael S. Romano, *Brazil's Backlog Days Are Numbered*, MANAGING IP, September 23, 2019, available at https://www.managingip.com/article/b1kbm141jmzzwm/brazils-patent-backlog-days-are-numbered.

[12] Dr. Pegah Karimi, *Brazil's Phase II of the Patent Prosecution Highway Program*, JDSUPRA (Jan. 27, 2021), https://www.jdsupra.com/legalnews/brazil-s-phase-ii-of-the-patent-1256066/ (last visited October 19, 2021).

Issue: Artificial Intelligence

Brazilian federal officials have introduced several bills on artificial intelligence (AI) in the Congress as they continue to revise their national AI strategy. This new strategy introduces standards that are inconsistent with international norms, adopting a broad definition of AI with a stringent framework.[13] The Brazilian legislature has since taken further steps to advance an AI regulatory structure, including the formation of an advisory council and hold a public hearing. We support the adoption of an adaptable regulatory approach that is informed by strong public-private collaboration and the responsible development and deployment of AI, consistent with the App Association's AI policy principles.[14]

## CANADA

Issue: Digital Services Taxation

The Canadian government has reiterated its commitment to, and continued to iterate on proposal for, a digital services tax in Canada, and has committed to impose such a tax (retroactively applied to January 1, 2022) should a multilateral convention addressing digital service taxation not fall into place. We urge the U.S. government to work with Canada to ensure that it adheres to its commitment not to impose a digital services tax.

## CHINA

Issue: China's Encryption Law

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.[15] 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.

On 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

[13] "Recommendations to the Brazilian Congress on the Development of Artificial Intelligence Regulation" (June 10, 2022), https://www.itic.org/news-events/news-releases/iti-offers-recommendations-to-the-brazilian-congress-on-the-development-of-artificial-intelligence-regulation.

[14] https://actonline.org/wp-content/uploads/ACT-The-App-Association-Policy-Principles-for-AI-1.pdf.

[15] 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/.

commercial encryption products, leaving unanswered questions. 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 impede American businesses' ability to succeed in China's large consumer market.

Issue: China's Cybersecurity Law

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 new 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.[16] Important clarifications are needed to allow for American businesses to succeed in the Chinese market, including how to balance new requirements for data encryption to protect Chinese consumers' privacy while allowing on demand access to the Chinese government.[17]

The App Association continues to advocate on behalf of innovative American app developers who actively seek 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.

---

[16] 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/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/

[17] Lorand Laskai & Adam Segal, *The Encryption Debate in China: 2021 Update*, CARNEGIE ENDOWMENT INT'L PEACE, Mar. 31, 2021, available at https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218.

Our comments also addressed concerns related to the vague definition of "network operator," as the "owner of the network, network managers and service providers." This definition can be interpreted to include app developers, even though most small business innovators operate on larger platforms or networks they do not manage. Including small app developers and software companies within this broad definition forces them to abide by cybersecurity responsibilities that do not apply to them. We separately contributed comments[18] on the Cybersecurity Administration of China's (CAC's) implementation of the Cybersecurity Law's restrictive policies on data transfers outside of Chinese borders.

While we believe our advocacy has helped delay the implementation of some of the Cybersecurity Law's more onerous provisions and has limited its scope, our members seeking to reach new customers in China inevitably must assess the viability of entering the Chinese market.

Issue: Personal Information Protection Law

The Personal Information Protection Law (PIPL) took effect on November 1, 2021.[19] The law applies to all companies processing personal information of Chinese individuals inside or outside China, exposing violators to fines up to 5 percent of annual revenue from the previous year. PIPL also sets out data transfer restrictions and localization requirements for those who exceed the amount of personal information allowed by the Cyberspace Administration of China (CAC). The CAC sets the threshold amount of personal data an organization may handle without restriction and decides what companies are excepted from the law's requirements. Article 24 of PIPA also sets out restrictions on the use of automated decision-making, including systems used to deliver targeted advertisements, potentially harming the ability of American companies to derive revenue from their products through advertising. The broad extraterritorial reach of this law, and the heavy penalties associated with non-compliance, pose a significant burden to App Association members and reduces their ability to do business in China. We therefore request the inclusion of the PIPL in the NTE report.

Issue: Virtual Private Network Restrictions

A virtual private network (VPN) creates a safe and encrypted connection to the internet. Applications running on a VPN benefit from the functionality, security, and management of the private network.[20] China regulates and restricts the use of VPNs, leaving consumers in China out of the digital marketplace, while creating massive barriers to entry, and we request this policy's inclusion in the NTE report. China's "extensive blocking of legitimate websites" also threatens to impose significant costs on providers and users

[18] *See* http://actonline.org/wp-content/uploads/ACT-Comments-re-China-Data-Transfer-Proposed-Law-051117-EN-1.pdf.

[19] Hui Xu et al., China Introduces First Comprehensive Legislation on Personal Information Protection, Latham & Watkins, Sept. 8, 2021, available at https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection.

[20] Mason, Andrew G. (2002). *Cisco Secure Virtual Private Network.* Cisco Press. P. 7.

of services and products.[21] The App Association has a keen interest in this policy because it creates a serious disincentive for our members when considering whether to enter the Chinese market or pursue different business ventures.

Issue: Cyberspace Administration of China Mobile App Regulation

In June of 2016, the Cyberspace Administration of China (CAC) released, without seeking public input, a regulation regarding mobile app providers and stores, titled "Administrative Provisions on Information Services of Mobile Internet Application Programs."[22] This regulation contains numerous provisions intended to protect national security that require the monitoring of online content, the reporting of violations to government authorities, and that new app users register with their real identities. The regulation also requires the monitoring and reporting of users who publish "banned content" to Chinese government authorities. This regulation went into effect on August 1, 2016. Citing the dangerous nature of illegal information, security risks, and user rights violations, the CAC requires all mobile app stores in the country to register with the government. This regulation poses further problems because of the combined burden imposed by various regulations now affecting app developers, including the June 2017 Cyber Security Law and the 2021 Personal Information Protection Law outlined above.[23] This establishes serious trade barriers when our members have fewer opportunities to reach Chinese consumers because of the tight restrictions placed on certain app stores.

Issue: Various Data Localization Requirements and Restrictions on Cross-Border Data Flows (Proposed and Final)

China implemented or proposed numerous restrictions on the flow of data across its borders. These regulations limit or prohibit the transfer of data outside of China in areas like banking and financial credit, cybersecurity, counterterrorism, commercial information systems, healthcare, and insurance. Each represents a significant barrier to market entry and is a non-starter for small business innovators. When compared to large corporations, small businesses are often unable to overcome this barrier and will be ultimately left out of the market. Restrictions have emerged through China's implementation of its Cybersecurity Law, Data Security Law, and PIPL, all of which contain numerous ambiguities that enable subjective and selective enforcement, further shaking the App Association community's confidence in rule of law in China. In 2022 the Cybersecurity Administration of China (CAC) has issued security assessment guidelines for the transfer of data across China's borders, putting further restrictions on transfers inconsistent with international norms and creating further risks for small businesses looking to do business in China (e.g., review regimes for compliance that may even mandate disclosure of

[21] Pham, Sherisse, *China says VPN crackdown aimed at 'cleaning' the internet,* (July 25, 2017), *available at* http://money.cnn.com/2017/07/25/technology/china-vpn-censorship/index.html.

[22] Cyberspace Administration of China, *Provisions on the Management of Mobile Internet Applications' Information Services*, (June 28, 2016)*, available at* http://www.cac.gov.cn/2016-06/28/c_1119123114.htm.

[23] Richard Bird, *Where are we now with data protection law in China?*, Sept. 10, 2019, LEXOLOGY, available at https://www.lexology.com/library/detail.aspx?g=6f52a281-b5b7-4f9f-940d-1951a905c4e1.

confidential information). Even more recently, the CAC issued new measures on data exit security assessments.

Issue: New Tariffs on Information and Communication Technology (ICT)

Over the course of 2018, China also imposed a wide range of tariffs on ICT imports from the United States. Despite the phase one agreement between the United States and China these tariffs remain in place while Chinese tariffs on imports from most other countries have been reduced, harming American businesses' ability to compete.[24] The App Association's members not only provide the apps that allow for interface with the internet via smartphones and tablets, but they also increasingly provide the same for internet of things (IoT) products and services. Many of these products are affected by the new China tariffs, which have created barriers to market entry and should therefore be included in the NTE.

Issue: Intellectual Property Rights and Enforcement

Theft and infringement of IP has grown exponentially in recent years, and often originates in China. IP theft and infringement puts the App Association's members businesses and the jobs they create at serious risk, where a single occurrence can represent an "end-of-life" scenario. Both criminals and government-backed hackers, sometimes based in China, are a demonstrated and well-known risk to our members in the app developer ecosystem. USTR's 2022 National Trade Estimate Barriers (NTE) report asserts that "actors affiliated with the Chinese Government and the Chinese military have infiltrated the computer systems of U.S. companies, stealing terabytes of data, including the companies' proprietary information and IP, for the purpose of providing commercial advantages to Chinese enterprises,"[25] and China appropriately remains on USTR's Priority Watch List of countries committing the most extensive IP rights infringements.[26] We support investigations into unfair cloud computing-related and other digital trade barriers, and we urge USTR to address IP theft and infringement originating from China in violation of WTO TRIPS in the Section 421 report using precise language that reflects how copyrights, trademarks, patents, and trade secrets each represent distinct IP rights.

With respect to patents, we address both (1) intellectual property licensing generally and then (2) the unique case of standard-essential patent licensing. The App Association condemns government policies that seek to diminish IP rights to hinder market entry, and, to the extent these policies are used by the Chinese government, we

[24] Chad P. Brown, *US-China Trade War Tariffs: An Up-to-Date Chart*, Mar. 16, 2021, PETERSON INST. FOR INT'L ECON., available at https://www.piie.com/research/piie-charts/us-china-trade-war-tariffs-date-chart.

[25] USTR, "2022 National Trade Estimate [NTE] Report on Foreign Trade Barriers," 97.

[26] USTR, "2022 Special 301 Report" (USTR, May 2022), 5, https://ustr.gov/sites/default/files/IssueAreas/IP/2022%20Special%20301%20Report.pdf

urge USTR to investigate and document them. One of the most problematic Chinese policies is the application of the controversial "essential facilities" doctrine to IP in the State Administration for Industry and Commerce's (SAIC)[27] Rules on Prohibition of Abusing Intellectual Property Rights to Eliminate or Restrict Competition (IP Abuse Rules), which took effect on August 1, 2015, and were later incorporated wholesale into China's State Administration for Market Regulation (SAMR) Provisions Prohibiting the Abuse of IPR to Eliminate or Restrict Competition released 2020.[28] Article 7 of SAMR's rules states:

> No business operator that holds a dominant market position may preclude or restrict competition without justifiable reasons by refusing to license others to use, under reasonable terms, its intellectual property which is an essential facility in production and operation.
>
> The following factors shall also be considered in determining acts referred to in the immediate foregoing paragraph:
>
> (1) The intellectual property in question cannot be reasonably substituted in the relevant markets and is an essential facility for other business operators participating in competition in the relevant markets;
>
> (2) The refusal of licensing such intellectual property will adversely affect competition or innovation in the relevant markets, damaging the interests of consumers or social public; and
>
> (3) The license of such intellectual property will not result in any unreasonable damage to such business operator.

The App Association opposes the notion that competitors should have access to "essential" patents simply because they 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. Application of this provision would seriously undermine the fundamental right to exclude others from using one's intellectual property, and thus, impact incentives to innovate in the long term. Under this provision, U.S. innovators, particularly those with operations in China, are vulnerable given the significant discretion vested in SAMR to balance the necessary factors to determine the issuance of a compulsory license. The App Association encourages USTR to include such practices in its Section 421 report in the context of the WTO TRIPS.

This stated, 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, with

[27] We note that SAIC has since been merged into the State Administration for Market Regulation.

[28] gkml.samr.gov.cn/nsjg/fgs/202011/t20201103_322857.html.

companies often collaborating to develop standards by contributing their patented technologies. These technological standards bring immense value to consumers by promoting interoperability while enabling healthy competition between innovators. 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 potential with the need to access the patents that underlie the standard, standards setting organizations (SSOs) require patent holders on 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 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 SSO, SEP holders can obtain reasonable royalties from manufacturers producing products compliant with the standard, who 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 advocates for the following consensus principles to prevent patent "hold-up" and anti-competitive conduct, which we urge USTR to advance:

- **Fair and Reasonable to All** — A holder of a SEP subject to a FRAND commitment must license such SEPs on FRAND terms to all companies, organizations, and individuals who wish to use the standard.

- **Injunctions Available Only in Limited Circumstances —** Injunctions and other exclusionary remedies should not be sought by SEP holders, except in limited circumstances. Anyone wishing to use the standard is always entitled to assert claims and defenses.

- **FRAND Promise Extends if Transferred —** If a FRAND-encumbered SEP is transferred, the FRAND commitments follow the SEP in that and all subsequent transfers.

- **No Forced Licensing —** While some licensees may wish to get broader licenses, the patent holder should not require anyone wishing to use the standard to take or grant licenses to a FRAND-encumbered SEP that is invalid, unenforceable, or not infringed, or a patent that is not essential to the standard.

- **FRAND Royalties —** A reasonable rate for a valid, infringed, and enforceable FRAND-encumbered SEP should be based on several factors, including the value of the actual patented invention apart from its inclusion in the standard. The rate cannot be assessed in a vacuum that ignores the portion in which the SEP is substantially practiced or royalty rates from other SEPs required to use the standard.

Specific to China and SEPs, the App Association acknowledges that SAMR has also provided the following in its Guidelines:

> In exercise of intellectual property rights, no business operator may preclude or restrict competition by formulation or implementation of any standard (including mandatory requirements of national technical specification, the same below).
>
> In exercise of intellectual property rights, no business operator that holds a dominant market position may engage in the following activities to preclude or restrict competition without justifiable reasons during formulation or implementation of any standard:
>
> (2) In participating in formulation of a standard, the business operator intentionally avoids disclosing the information in respect of its right(s) to the standard formulating organization or explicitly waives its right(s), but claims for its patent right(s) against the implementer(s) of such standard after finding out that such standard involves its patent(s).
>
> (2) After its patent becomes a standard-essential patent, the business operator precludes or restricts competition by refusing to license, tie-in sale, or attaching other unreasonable conditions upon any transaction, in violation of the principles of fairness, reasonableness, and non-discrimination.
>
> For the purpose hereof, a "standard-essential patent" refers to a patent that is essential to the implementation of such standard.

In the past, SAMR (and its predecessors) have attempted to set policies that would have instructed Chinese-backed standardization bodies to lower or undermine royalty payments of patents without differentiating between FRAND-encumbered SEPs and other patents; however, with assistance from the international community, such efforts have been thwarted. Today, SAMR seems to 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." Even more recently-issued guidance for the automotive sector issued by the Chinese government since appears to be consistent with this approach.[29] The App Association therefore does not believe that SAMR's rules addressing SEP licensing constitute a WTO violation (in contrast to the SAMR's rules discussed above that require a patent holder to give competitors access to the former's "essential" patents. We 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 standard-essential patents.

[29] For example, the China Academy of Information and Communications Technology (CAICT) has published guidelines on SEP licensing related to the automotive industry. *See* https://mp.weixin.qq.com/s/gGFxKZfXxl6MP9XO_sWmZg.

China's Use of Antitrust Laws

China's use of antitrust law as a means to target foreign firms should raise concerns for USTR, which USTR has already documented and addressed previously.[30] China's activities justified under its antimonopoly laws appear to run counter to China's commitments to the WTO, including TRIPS Article 40 Section 8 with respect to IP, as well as due process under Article 40 ("making decisions on the merits," "without undue delay," "based only on evidence," "with an opportunity for review," "with the right to written notice," and "the right to be represented by independent legal counsel").[31] We urge for further monitoring of China's selective wielding of its antitrust laws against U.S. firms.

## COLOMBIA

Issue: Lack of Transparency and Fairness in Intellectual Property Rights Enforcement by Courts

Recently, a Colombian court decision sought to block defendant's access to legal remedies and procedural rights in other jurisdictions following an *ex parte* injunction (sales ban, Ericsson v Apple).[32] In this case, the defendant did not receive prior notice and had no opportunity to defend itself in court before a country-wide injunction was issued. U.S. law, consistent with international norms, requires SEP holders to notify SEP users of their SEPs and provide them with a FRAND license offer prior to enforcing their rights, making this decision contradictory with those norms and a barrier to trade for U.S. companies. The U.S. government is encouraged to condemn such lack of transparency and judicial attempts of blocking enforcement rights, and include this development in the NTE as a significant barrier to trade for further attention from the U.S. government.

Issue: Digital Economy Taxation

The App Association has significant concerns with Colombia's recent tax bill No. 118 of 2022, which contains new requirements for U.S. companies that invest in and export to Colombia. The proposed bill would negatively impact U.S. goods and services exports and contravene the letter and spirit of the United States-Colombia Trade Promotion Agreement in several ways.[33] The bill passed in the Third Commission of both Chambers

[30] USTR, "2020 Report to Congress on China's WTO Compliance," 38.

[31] Mark Cohen, "RCEP And Phase 1: Strange Bedfellows in IP," *China IPR*, December 3, 2020, https://chinaipr.com/2020/12/03/rcep-and-phase-1-strange-bedfellows-in-ip/; World Trade Organization, "Agreement on Trade-related Aspects of Intellectual Property Rights," https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

[32] https://www.reuters.com/legal/litigation/apple-says-ericsson-filed-secret-colombian-patent-lawsuits-sideline-texas-court-2022-07-11/.

[33] https://www.uschamber.com/assets/documents/Multi-Association-Letter-on-Colombia-Tax-Bill-Provisions-Oct-21-Final-1453-10212022.pdf.

of Congress on October 6, 2022, and a new draft will likely be presented for the last two debates in plenaries of both chambers in late October, with the objective of final passage in early November. We urge for its inclusion in the NTE, and for the U.S. government to engage with Colombian counterparts to ensure the final measure is not passed in its current form.

## EUROPEAN UNION

Issue: The EU's Digital Single Market (DSM)

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 (and should be included in the NTE), 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.[34]
- Regulation of online platforms, via the Digital Markets Act,[35] intending to address contractual clauses and trading practices in relationships between platforms and businesses, poses significant risks to U.S. small business engagement in the global digital economy.[36] The DMA proposal will only level the playing field for gatekeepers but not for small companies. App Association members will suffer from the ripple effects this legislation will have on the whole ecosystem, making it more difficult to reach consumers and compete against big brands. Among the recommendations in the DMA that could negatively impact App Association members are:
    - The combination of ex–ante rules and the market investigation tool could duplicate existing EU competition law provisions. The app economy is thriving and helping thousands of EU companies find success, even during a pandemic. The Commission's commitment to preserving competition is

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

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

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

commendable but responding to potential problems without evidence of actual harm is the wrong approach

  - The creation of a list of prohibited practices (blacklist) and obligations (whitelist) for large online platforms is concerning. The white–, gray–, and blacklists only address a snapshot of the current economy. They will be outdated a few months from now. For example, forcing multiple app stores on devices would only fragment the market and increase costs, especially for smaller app makers with limited resources. We prefer a model like the core principles in the E-Commerce Directive, defining what's truly important and what should guide competition policy moving forward.
  - Rather than taking an ex–ante approach that tries to anticipate problems, the App Association believes the best way to safeguard competition is to continuously look for evidence of actual harm and put mechanisms in place that can address it with swift remedies.

- 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.[37] 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 NTE.
- New proposals to enact sweeping regulations on the use of artificial intelligence (AI),[38] which raise concerns for the App Association about regulation pre-empting new and innovative uses of AI.

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

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

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 European Commission to begin its consideration of an adequacy determination as expeditiously as possible in order to restore transatlantic data flows and ease the burden on our small business members seeking to compete in the global economy.

## FRANCE

Issue: Digital Services Tax

On March 6, 2019, the government of France released a proposal for a 3 percent levy on revenues that certain companies generate from providing certain digital services to, or aimed at, French users. USTR has since undertaken a Special 301 investigation, releasing its report in December of 2019.[39] While the French government had initially delayed collecting the tax, since December 2020 it appears to have resumed collection.[40]

France's digital services tax (DST) is contrary to the long-standing agreement by World Trade Organization (WTO) members not to apply customs duties to cross-border electronic transmissions and prejudices ongoing discussions at the WTO and the Organization for Economic Cooperation and Development (OECD). This action will harm U.S. goods and services exporters of all sizes in nearly every sector and threaten American jobs, creating a damaging precedent for a fragmented digital economy that will suppress American small business innovation and job growth.

We recognize that some countries have made a commitment to withdraw digital service taxes once the Organization for Economic Cooperation and Development (OECD) agreement is realized. However, until they are rescinded, we urge for the inclusion of digital service taxes in the NTE.

[39] https://ustr.gov/sites/default/files/Report_On_France%27s_Digital_Services_Tax.pdf.

[40] https://www.wsj.com/articles/global-digital-tax-detente-ends-as-u-s-and-france-exchange-blows-11609333200.

## GERMANY

Issue: Unbalanced German Patent Law as a Trade Barrier

Germany is a key market in the European Union and abroad due to its global influence. The App Association is a long-time advocate of strong intellectual property protections and works hard to include our members' voices in the relevant policy development processes taking place across the EU. Small tech businesses thrive in environments where they can enjoy legal certainty, and which reflect widely accepted fairness principles. However, tech small and medium enterprises (SMEs) have long faced difficulty in Germany. Under the current legal framework, courts issue injunctions against those accused of patent infringement without fully determining if infringement has occurred. The courts also do not consider whether the remedy they order is proportionate to the impact on the public interest. Fortunately, the German government just took an important step towards creating a more competitive and innovation-enabling environment in Germany by modernizing its Patent Act.

Throughout the last year, the App Association participated in every step of the legislative process. We submitted feedback to each draft released by the Federal Ministry of Justice and Consumer Protection, met with Members of the Bundestag and participated in stakeholder roundtables. We urged the German government to:

- Introduce a proportionality test into §139 of the Patent Act concerning injunctions and the inclusion of third-party interests.
- Align German patent law with the Intellectual Property Rights Enforcement Directive (IPRED) of the European Parliament and the Council and eliminate quasi-automatic injunctive relief that is possible in the German system. The IPRED's Article 11 states that "[t]he competent courts can issue an order against the infringing party upon finding an infringement of an intellectual property right, which prohibits the infringer from further infringing the right in question."
- Reduce the timespan between an injunction and a validity test (injunction gap) to avoid situations in which an injunction is granted for a patent that is later declared invalid or should not have been granted in the first place.

Amongst other things, the modernized Patent Act provides for a change to §139, which regulates injunctive relief for the patent holder in cases of patent infringement. The new revision now allows for the limitation of injunctions for proportionality reasons. This means an injunction can be restricted if claiming it would result in disproportionate hardship for the infringer or third parties due to the extraordinary circumstances of the individual case and the good faith requirement. Appropriately, the patent holder is not disadvantaged because they would then receive additional monetary compensation. A proportionality test is now codified into the law, providing courts with an express basis for temporary or permanent suspension of an injunction against fair compensation, in addition to potential damages, for past infringements. This proportionality test will help address cases related to aggressive patent trolls, or instances where a discrepancy exists between invention value and economic loss of the defendant or detriment to "paramount interests" of third

parties. It remains to be seen over the next several years which cases will trigger these restrictions of injunctive relief and how the modernized Patent Act will impact the way courts grant injunctions in patent litigation.

Additionally, the revised Patent Act provides for a rule under which the federal patent court (the Bundespatentgericht, which provides validity decisions) "shall" provide to the litigants a first indicative assessment/interim decision of the case within six months after a nullity action has been filed. This rule aims to accelerate patent nullity proceedings as well as improve the synchronization of infringement proceedings before civil courts and the nullity proceedings before the federal patent court. At the moment, infringement proceedings are often decided before a decision on the validity of a patent has been reached, and the often-mismatched timelines of both proceedings can be frustrating for those accused of infringement as they can't point to an invalidated patent during infringement proceedings. While this new approach is meant to reduce unnecessary delays and inform both litigants and the infringement court before a decision is reached, the modernized Patent Act does not increase funding and staffing for the federal patent court so it remains unclear how significant the impact of this change will be. Funding and staffing of the federal patent court, however, is a separate and currently ongoing discussion.

Because an injunction can be devastating for SMEs whose business models and growth often depend entirely on one product line or offering, it's so important that courts confirm an injunction is in the public interest. For this reason, considering the proportionality of a remedy before granting an injunction is essential to ensure continued small business competitiveness and a level playing field for all actors. We believe this modernized Patent Act addresses some of the current power imbalances in German patent law and aligns Germany meaningfully with many other leading markets, but we encourage USTR to monitor this development and determine the impact of its implementation.

## INDIA

Issue: Various Proposed and Final Restrictive Data Localization Laws

India has both proposed and implemented policies that restrict the flow of data across its borders and create significant issues for small business innovators seeking to expand into the Indian market, including:

- India's National Data Sharing and Accessibility Policy which requires that all data collected using public funds to be stored within the borders of India.[41]
- The 2015 National Telecom M2M ("machine to machine") Roadmap,[42] which has

[41] Government of India Ministry of Science & Technology, *India's National Data Sharing and Accessibility Policy*, (2012), a*vailable at* https://dst.gov.in/national-data-sharing-and-accessibility-policy-0.

[42] Government of India Ministry of Communications & Information Technology Department of Telecommunications, *National Telecom M2M Roadmap, available at*

not been implemented, states that all M2M gateways and application servers serving customers in India need to be located within India.

- India's 2018 Draft Cloud Computing Policy[43] would require data generated within India to be stored within the confines of the country. As a result of this proposed regulation, cloud companies will either be forced out of the India market or be required to build local data centers to comply with India's policy. Therefore, this policy will deter or create a barrier to entry in the Indian marketplace for small and large companies alike.
- In 2021 the Indian Department of Telecommunications (IDoT) proposed replacing outdated provisions of the Indian Telegraph Act and Wireless Telegraphy Act. In consultation with the National Law University in Delhi, the IDoT is looking to update the laws with provisions controlling the use of M2M communications and the communications between IoT devices. This update has the potential to significantly affect American IoT device and application makers, as the Indian government looks to increase domestic production of telecommunications devices and related services.[44]

Issue: Intellectual Property Rights Enforcement

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 World Intellectual Property Organization (WIPO) Copyright Treaty and WIPO Performances and Phonograms Treaty; further, Indian patent law is inconsistent with the TRIPS Agreement. Moreover, the 2020 Department of Industrial Policy and Promotion's proposal to decriminalize copyright infringement offenses as listed in the Copyright Act of 1957 would diminish copyright protections and discourage investment across industries.[45]

Issue: Continuing Threats and Uncertainty Regarding the Ability to Use Strong Encryption

Currently, Indian internet providers must attain government approval from the Telecom Regulation Authority of India (TRAI) to employ encryption stronger than 40-bit encryption. Laws like this provide fewer touchpoints for our members' apps to reach consumers. The Indian government abandoned its proposed National Encryption Policy after widespread

http://www.gsma.com/connectedliving/wp-content/uploads/2015/05/150513-DoT-National-Telecom-M2M-Roadmap.pdf.

[43] *India Corporate Update –Data Localisation*, SQUIRE PATTON BOGGS, (2018), *available at* https://www.squirepattonboggs.com/~/media/files/insights/publications/2018/10/india-corporate-update-data-localisation/india-corporate-update--data-localisation-client-alert.pdf

[44] Ishita Guha, *Govt to Refresh Laws Before 5G Rollout*, MINT, Mar. 8, 2021, *available at* https://www.livemint.com/industry/telecom/govt-to-refresh-laws-before-5g-rollout-11615141845898.html.

[45]

pushback and recognition that encryption is a key building block for trust in digital infrastructure. Nevertheless, after a petition from the Indian Supreme Court, the government is considering diluting end-to-end encryption in a variety of use cases.[46] This is an ongoing issue of serious concern to small business innovators; therefore, we recommend it be included in the NTE to ensure continued prioritization for the U.S. government and other stakeholders.

Issue: Sweeping Privacy Regulation in India

On December 11, 2019, the Personal Data Protection Bill was introduced in India's parliament.[47] The bill includes rules for how personal data should be proposed and stored as well as lists the rights of people regarding their personal information. The bill proposes the creation of the Data Protection Authority (DPA), which would be a regulatory authority that carries out the new law by giving 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. Second, India's bill allows the government to order firms to share the nonpersonal data they collect. Third, India's bill restricts the transfer of sensitive personal data outside of India unless it meets certain requirements, similar to those of the GDPR. The information can only be processed and cannot be stored outside of India. If passed, the Personal Data Protection Bill has the potential 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. We urge USTR to include the Indian Personal Data Protection Bill in its NTE.

Issue: OTT Regulation

In 2022, the Government of India's Ministry of Communications within the Department of Telecommunications sought public comments on the draft Indian Telecommunication Act, 2022. The bill would expose OTTs (network edge residents who are not telecommunications service providers) to extensive regulatory and licensing obligations, creating significant trade barriers. We urge for USTR to include this development in the NTE and work with the Government of India to prevent the passage of the draft bill in its current form.

[46] Trisha Ray, *The Encryption Debate in India: 2021 Update*, Carnegie Endowment Int'l Peace, Mar. 31, 2021, *available at* https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-84215.

[47] Anirudh Burman and Suyash Rai, *What Is in India's Sweeping Personal Data Bill?*, CARNEGIE INDIA, March 09, 2020, *available at* https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985.

Issue: Digital Services Tax

USTR has already launched an investigation of India's DST,[48] and we agree that this DST is discriminatory, inconsistent with international tax principles, and restricts U.S. commerce. India's digital services tax is also contrary to the long-standing agreement by WTO members not to apply customs duties to cross-border electronic transmissions and prejudices ongoing discussions at the WTO and the OECD. India's DST will harm U.S. goods and services exporters of all sizes in nearly every sector and threaten American jobs, creating a damaging precedent for a fragmented digital economy that will suppress American small business innovation and job growth.

We recognize that some countries have made a commitment to withdraw digital service taxes once the OECD agreement is realized. However, until they are rescinded, we urge for the inclusion of digital service taxes in the NTE.

## INDONESIA

Issue: Data Localization Requirements on Electronic System Providers of Public Services

Indonesia's Ministry of Communications and Information Technology (MCIT) has enacted regulations that require electronic system providers for public services to locate a data center and disaster recovery center within Indonesia.[49] In October 2019, Indonesia passed Regulation No. 71 of 2019 which revoked Regulation No. 82 of 2012.[50] It also relaxed the data localization rules for "public bodies." The 2019 regulation requires private Electronic System Operators (ESOs) to register with MCIT prior to their electronic systems being made accessible to users while existing ESOs must register with MCIT within a period of one year. Currently, the MCIT's online system only accommodates Indonesian individuals and entities, which prohibits outside small businesses to complete registration. The 2019 Indonesian regulation permits private ESOs to locate electronic systems and data outside of the territory of Indonesia so long as "the location does not diminish the effectiveness of the supervision conducted by a relevant state ministry or institution and law enforcement agencies; and access to the electronic system and electronic data must be provided for the purpose of supervision and law enforcement, in accordance with law." The 2019 regulation incorporates the "right to be forgotten" and requires ESOs to delete electronic information that is within their control and is no longer

---

[48] https://ustr.gov/sites/default/files/enforcement/301Investigations/Report%20on%20India%E2%80%99s%20Digital%20Services%20Tax.pdf.

[49] *See* Mary R. Silaban, *Unleashing Indonesia's Digital Innovation*, American Chamber of Commerce in Indonesia (June 10, 2014), *available at* http://www.amcham.or.id/fe/4614-unleashing-indonesia-s-digital-innovation.

[50] *Indonesia Issues Important New Regulation on Electronic (Network and Information) Systems*, ABNR LAW, October 30, 2019, *available at* https://www.abnrlaw.com/news_detail.php?send_news_id=366&year=2019.

relevant. While the new Indonesian regulation is based on the GDPR, the App Association hopes that the implementation will properly reflect the structure of the GDPR.

Issue: New Indonesian Tariff Codes for "Intangible Goods" (Software and Other Digital Products) and Digital Services Tax

In February 2018, the Indonesian government issued Ministry of Finance Regulation No. 17/PMK.010/2018 on the Second Amendment of Regulation No. 6/PMK.010/2017 on Stipulation of Goods Classification System and Import Duty on Imported Goods (Regulation 17), which went into effect as of March 1, 2018. Regulation 17 provides Chapter 99 as a new addition to the Indonesian tariff system, covering intangible goods ("Software and Other Digital Goods"). While the import duty is currently at 0 percent, the App Association is alarmed at the unprecedented addition of digital goods to a tariff system and fears the precedent Indonesia may create. Further, its tariff would directly contravene the WTO Moratorium on Customs Duties for Electronic Transmissions.

The Indonesian government implemented a digital services tax on July 1, 2020. All digital services providers are required to collect a 10 percent tax no matter where they are located. Foreign operators are required to remit the withheld taxes to the Indonesian government. A digital services tax applied extraterritorially affects American service providers, and the 10 percent rate applied by Indonesia is far above the tax rate set out in various European countries.[51] We recognize that some countries have made a commitment to withdraw digital service taxes once the OECD agreement is realized. However, until they are rescinded, we urge for the inclusion of digital service taxes in the NTE.

We request that both Indonesia's software and other digital products tariff as well as its digital services tax be included in the NTE.

## JAPAN

Issue: Improper Application of Antitrust Law to Digital Platforms

In 2022, Japan's Headquarters for Digital Market Competition (DMCH) issued its "Interim Report on Competitive Evaluation on Mobile Ecosystem" and "Interim Report on Competitive Evaluation on New Customer Contact (Voice Assistant and Wearable)."[52] The App Association has provided detailed views on digital platforms and competition, as well as reactions and feedback on DMCH's specific proposals.[53] The App Association has significant concerns with DMCH's apparent positioning of the Japanese government to

[51] A sample of European digital services tax rates can be found at https://taxfoundation.org/digital-tax-europe-2020/.

[52] https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=060220427&Mode=0.

[53] https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi_wg/dai38/siryou1.pdf.

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 DMCH'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 Japan to mitigate the risks such an intervention would pose while supporting U.S. small business digital economy trade and leadership.

## REPUBLIC OF KOREA

Issue: Telecommunications Business Act Amendments/ Improper Application of Antitrust Law to Digital Platforms

On May 20, 2020, the National Assembly passed amendments of the Telecommunications Business Act (TBA).[54] The amendments to the TBA impose scope of service quality maintenance requirements on value added telecom service providers (VSPs) that meet certain thresholds. The VSPs that fall within the thresholds and do not have a local presence will have to appoint a local representative to receive user complaints and answer regulatory requests for information. Without knowing what the thresholds are, content providers may unfairly face requirements that do not apply to Korean competitors. The App Association asks the USTR to track the thresholds as they are defined and to advocate on behalf of U.S. businesses to avoid VSP disruptions.

Further amendments were made to the TBA in August 2021. These amendments regulate app store pricing and payment processing. These changes to the TBA will only benefit global brands like Spotify, Epic Games, and Tile while also potentially freezing out small business app developers in South Korea and around the world that can't pivot so quickly to new payment processing methods. App Association members demand platform level privacy and security measures, removal of fraudsters and copyright thieves, and rigorous vetting of any new software. These are essential to maintain an ecosystem consumers trust enough to download apps from companies without name recognition. The TBA would prohibit core platform functions that benefit our members and consumers.

Notably, the TBA prohibits "the use of a particular payment method or imposing any unreasonable or discriminatory terms or restrictions when intermediating transactions involving mobile contents and the like as an app market operator." Such a change would unduly confine app market business operators' in-app purchase practices and ultimately devalue the software platforms we rely on. Further, enactment of the proposed revisions to Telecommunications Business Act would give rise to conflicts with the ROK's commitments under the General Agreement on Trade in Services (GATS).

[54] Ben Gu, et al., *Korea Technology Sector Legal Developments,* LEXOLOGY, (May 26, 2020)*, available at* https://www.lexology.com/library/detail.aspx?g=e6451c62-2f11-461d-b699-5b365532bda6.

Issue: Regulation of "Pre-Installed Apps"

Since 2014, South Korea has implemented regulations that force telecommunication devices with smart capabilities to allow users to delete pre-installed applications on a device. In 2014, almost 60 apps installed by the country's three largest providers were put at risk, including more than half by Samsung and LG.[55] By allowing end-users to remove these apps, including those used for basic device functionality, the government is allowing changes to the operating system software. This negatively impacts the integrity of both the manufacturer and internet service provider platforms, as well as the larger app ecosystem. These regulations also impose unnecessary app developer registration requirements that add new barriers to entering a platform's market.

## KENYA

Issue: Digital Economy Taxation

Since 2021, Kenya has had a digital service tax in place that only applies to non-Kenyan entities. We have significant concerns with this tax, which contravenes WTO moratorium on ecommerce customs duties and undermines the OECD's consensus solution for digital economy taxation. We urge USTR to include this development in its NTE and to work with the Kenyan government to mitigate its damage and influence in the region.

## MEXICO

Issue: OTT Regulation

In 2020, legislation was proposed that would impose local content requirements for OTTs operating in Mexico, contravening Mexico's commitments in the USMCA. While the proposal continues to be worked on, it is not finalized or in effect yet. We urge USTR to include this development in the NTE and to work with Mexican counterparts to prevent such proposals that would undermine U.S.-Mexico digital trade.

## NIGERIA

Issue: Digital Economy Taxation

Since 2020, Nigeria has been assessing taxes on non-resident companies based on their commerce over the internet/on digital platforms. We have significant concerns with this tax, which contravenes WTO moratorium on ecommerce customs duties and undermines the OECD's consensus solution for digital economy taxation. We urge USTR to include

[55] Matt Brian, *South Korea rules smartphone users can delete Android bloatware*, ENGADGET, (January 24, 2014) *available at* https://www.engadget.com/2014/01/24/south-korea-delete-preinstalled-android-apps/.

this development in its NTE and to work with the Nigerian government to mitigate its damage and influence in the region.

## RUSSIA

Issue: Data Localization Law

Federal Law No. 242-FZ, signed by President Vladimir Putin in July of 2014, requires companies that store and process the personal data of Russian citizens to maintain servers on Russian soil and to notify the federal media regulator, Roskomnadzor, of all server locations.[56] It empowers Roskomnadzor to block websites and to maintain a registry of data violators. Additionally, in August 2015, Russia passed a non-binding clarification suggesting that localization might apply to websites that include a built-in Russian-language options, transact in Russian rubles, or use a Russian top-level domain such as ".r."[57]

In July 2016, a package of amendments was released imposing extensive data storage requirements on telecommunications providers and companies classified as internet telecommunications services.[58] Per these changes, telecom operators will have to store metadata for three years and internet telecoms for one year, while both will have to retain the content for up to six months. Companies had until July 1, 2018, to begin implementing these requirements. Moreover, if the stored messages and files are encrypted, companies are required to provide Russian state security services with decryption keys upon request. In August 2016, Russia's Federal Security Service (FSB) announced that it has the capability to obtain information necessary for decoding the electronic messaging received, "sent, delivered, and (or) processed by users of the internet."[59]

Further, on February 7, 2017, President Putin signed amendments to the Russian Code on Administrative Offences that increases fines for those violating Russian data protection laws. Effective on July 1, 2017, fines were raised substantially from RUB 10,000 to 75,000 or from approximately $170 to $1,260.[60] By raising the penalties for not abiding by this

---

[56] Russian Federation, *Federal Law No. 242-FZ*, (July 21, 2014), *available at* https://pd.rkn.gov.ru/authority/p146/p191/.

[57] Russian Federation's Ministry of Communications and Mass Media, *Clarifying Federal Law No. 242-FZ*, (Aug. 3, 2015), *available at* http://www.bna.com/russia-clarifies-looming-n17179934521/.

[58] Russian Federation, "*Yarovaya Package" Federal Law No 374-FZ*, (July 6, 2016), *available at* http://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

[59] Federal Security Service of the Russian Federation, *Encryption Keys*, (August 1, 2016), *available at* http://www.fsb.ru/fsb/science/single.htm!id=10437866@fsbResearchart.html.

[60] Hogan Lovells, *Chronicle of Data Protection,* "Russia Increases Fines for Violations of Data Protection Laws", (February 9, 2017), *available at* http://www.hldataprotection.com/2017/02/articles/international-eu-privacy/russia-increases-fines-for-violations-of-data-protection-laws/.

regulation, it is making it even harder to take a risk and creates additional barriers to digital trade and market entry.

Issue: Prohibitions on the Use of Strong Encryption

Under Russia's current System of Operative-Investigative Measures (SORM), Russian internet service providers (ISPs) must install a special device on their servers to allow the FSB to track all credit card transactions, e-mail messages, and web use. In 2014, SORM usage was extended to monitoring of social networks, chats, and forums, requiring their operators to install SORM probes in their networks. Advances of the SORM force online communications providers to provide the authorities with a means to decrypt users' messages, a technically infeasible result when end-to-end encryption methods are used. This law presents serious issues for small business innovators seeking to enter the Russian marketplace.

Russia also requires companies to provide the FSB with encryption keys for applications. Telegram, a popular messaging app, was fined 800,000 rubles for not providing FSB with one of these encryption keys.[61]

Issue: Various Virtual Private Network Restrictions

On November 1, 2017, Russia enacted regulations that prohibit consumers' ability to use VPNs to access websites as an anonymous browser. The Russian government cites this regulation as an effort to keep people from accessing dangerous and illegal content. This regulation says that any internet providers that allow these to exist, or function without being blocked, will lose their market access. This is an obvious trade barrier and real threat to the free market.

Additionally, there are now regulations regarding the anonymity of citizens while using chat apps such as WhatsApp or Facebook Messenger. Regulations that went into effect on January 1, 2018, require these apps to provide the users' phone numbers to the government to limit or prohibit access to those attempting to spread illegal content. Therefore, there is no ability to remain anonymous when using these applications. Although this is done under the veil of safety for citizens, it restricts the free flow of information and provides an extremely tough trade barrier to infiltrate.

[61] "Russia Fines Telegram App Over Encryption-Key Demand", *RadioFreeEurope RadioLiberty* (October 16, 2017), *available at* *https://www.rferl.org/a/russia-fines-telegram-app-encryption-key/28797424.html?mkt_tok=eyJpIjoiTW1OaU5EUTBPVFZtTVdObCIsInQiOiIwbVRcL1RkdDJjeXlsMFB6RkFQWStxMjBIaGV3cHFQRDZQK3BkRE1pVnE0TEtlQlZUVnFOeisyVkp6S3FlSUJpUnJZT1EzT211d1FiYWIwRis4MHhxVWZPREdGV2xPUlo2cklseE4xOEp3Mkx3aG1rc3FOTUs1RXFtWnRISDNXUHAifQ%3D%3D.*

## SOUTH AFRICA

Issue: Improper Application of Antitrust Law to Digital Platforms

In 2021, the Competition Commission of South Africa (CCSA) launched a online intermediary platforms market inquiry.[62] The App Association has provided detailed views on digital platforms and competition, as well as reactions and feedback on CCSA's specific proposals.[63] The App Association has significant concerns with the potential of the South African government interjecting 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 CCSA's inquiry into online intermediary platforms, 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 South Africa to mitigate the risks such an intervention would pose while supporting U.S. small business digital economy trade and leadership.

## TURKEY

Issue: Data Localization Requirement on Companies that Process Payments

Turkey's E-Payment Law requires the processing of e-payments occur within Turkey.[64] In mid-2016, Turkey's Banking Regulation and Supervising Industry (BDDK) initiated a policy that mandates companies locate their ICT systems in the country.[65] For instance, PayPal was forced to halt their operations after the Turkish government revoked their license. The Turkish government asserts that this action will affect "tens of thousands of businesses and hundreds of thousands of consumers."[66] These data localization requirements have largely chilled our members' plans to enter this important market should their app include e-payment capabilities.

Issue: Digital Economy Taxation

---

[62] https://www.compcom.co.za/online-intermediation-platforms-market-inquiry/.

[63] E.g., https://www.compcom.co.za/wp-content/uploads/2021/07/App-Association-Comments-on-OIPMI-Statement-of-Issues-18-Jun-2021.pdf.

[64] U.S. Dep't of State Bureau of Economic and Business Affairs, *2016 Investment Climate Statement – Turkey* (July 5, 2016), *available at* http://www.state.gov/e/eb/rls/othr/ics/2016/eur/254425.htm.

[65] Turkey's Banking Regulation and Supervising Industry (BDDK), *Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions numbered 6493*, Official Gazette numbered 28690, (published June 27, 2013), *available at* https://www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing.pdf.

[66] Lunden, Ingrid, "PayPal to halt operations in Turkey after losing license, impacts 'hundreds of thousands'" *Tech Crunch,* (May 31, 2016), *available at https://techcrunch.com/2016/05/31/paypal-to-halt-operations-in-turkey-after-losing-license-impacts-hundreds-of-thousands/.*

Since 2020, Turkey has imposed a digital services tax on any company conducting business in Turkey via the internet. We have significant concerns with this tax, which contravenes WTO moratorium on ecommerce customs duties and undermines the OECD's consensus solution for digital economy taxation. We urge USTR to include this development in its NTE and to work with the Turkish government to mitigate its damage and influence in the region.

**UNITED KINGDOM**

Issue: Digital Economy Taxation

Since 2020, the United Kingdom (UK) has imposed a digital services tax. While the thresholds for scope are high, we have significant concerns with this tax, which undermines the OECD's consensus solution for digital economy taxation. We urge USTR to include this development in its NTE and to work with the UK government to mitigate its damage and influence in the region.

Issue: UK Law with Respect to Standard-Essential Patents

In the case *Unwired Planet v Huawei*,[67] 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 into a patent license for Unwired Planet's worldwide portfolio of standard-essential patents (SEPs), even though the party was willing to enter into a license for United Kingdom (UK) SEPs. The ruling also states that the plaintiff did not violate European Union (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 fair, reasonable, and non-discriminatory (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 into a worldwide license, SEP owners will be highly incentivized 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 pre-empt U.S. law in mandating worldwide FRAND licensing, presenting a major barrier to trade for American small businesses in 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 NTE, within the ongoing U.S.-UK Free Trade Agreement negotiation, and through other avenues.

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

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.

## VIETNAM

Issue: National Cybersecurity Law

Originally proposed in June 2017, Vietnam's Ministry of Public Security has now enacted its cybersecurity law. This law's intent is based in public interest yet is too broadly scoped; in addition, the law proposed to apply to onshore and offshore companies/individuals directly involved or related to the management, provision or use of cyberspace; imposes forced localization (specifically, administrators of critical systems must store personal data and critical data within Vietnam); imposes discriminatory licensing requirements; and conflicts with Vietnam's pro-innovation and investment positions at the Asian-Pacific Economic Cooperation. Vietnam's Ministry of Public Security continues to tighten censorship and restrictions on social media and online freedom. [68]

Issue: Data Localization Law

Vietnam has expanded its use of required localization measures. For example, the *Ministry of Information and Communication's (MIC) Decree on Information Technology Services* (Decree No.72/2013/ND-CP) makes every digital service or website locate at least one server within the borders of Vietnam.[69] The small to mid-size businesses that the App Association represents, face extreme barriers to the Vietnamese market due to this decree without it benefitting Vietnamese citizens or its economy. Moreover, Vietnam's MIC released new draft amendments to Decree 72 in 2021 that further regulate internet services by expanding its scope to include data center and cloud services.[70] These requirements target foreign companies by enforcing rules that are overly burdensome and difficult to adhere to.

---

[68] Vu Lam, *Vietnam's Public Diplomacy and the Peril of Mixed Messages,* THE DIPLOMAT, (October 6, 2020)*, available at* https://thediplomat.com/2020/10/vietnams-public-diplomacy-and-the-peril-of-mixed-messages/.

[69] https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF

[70] Yee Chung Seck and Manh Hung Tran, *Vietnam: New amendments to draft regulations on internet services, online information and online games*

(Jan 14, 2022). https://www.globalcompliancenews.com/2022/01/14/vietnam-new-amendments-to-draft-regulations-on-internet-services-online-information-and-online-games-22122021/.

Issue: National Privacy Law

Vietnam adopted personal data protection laws in 2021 that restrict cross-border data flows out of Vietnam unless a company undergoes onerous licensing procedures and audits. Vietnam's approach does not align with international norms, such as the APEC Cross-Border Privacy Rules, and presents trade barriers to App Association members operations in the market. We urge for its inclusion in the NTE.

Issue: Digital Economy Taxation

Since 2020, Vietnam has imposed a digital services tax on cross-border e-commerce. We have significant concerns with this tax, which contravenes WTO moratorium on ecommerce customs duties and undermines the OECD's consensus solution for digital economy taxation. We urge USTR to include this development in its NTE and to work with the Vietnamese government to mitigate its damage and influence in the region.

The App Association appreciates the opportunity to submit these comments to the NTE. We stand ready to work with USTR and other stakeholders to address trade barriers for all of America's businesses and innovators.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Leanna Wade
Policy Associate

Priya Nair
IP Counsel

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