October 30, 2025

Edward Marcus
Chair of the Trade 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, *Request for Comments on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report* [90 FR 44448]

In response to the Federal Register notice issued on September 15, 2025,[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 2026 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 globe.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, that digital economy is worth more than $1.8 trillion annually and provides over 6.1 million American jobs.[3]

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.

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:

[1] 90 FR 44448.
[2] ACT | The App Association, *About*, *available at* http://actonline.org/about.
[3] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf

- ***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, and for American small business technology developers 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.
- ***Prohibiting Customs Duties and Digital Service Taxes on Digital Content:*** American innovators must take advantage of the internet's global nature to reach customers who live outside of the United States. However, the tolling of data crossing political borders with the purpose of collecting customs duties directly contributes to the balkanization of the internet. These practices jeopardize the efficiency of the internet and effectively block innovative products and services from market entry.
- ***Ensuring Market Entry is Not Contingent on Source Code Transfer or Inspection:*** Some governments have proposed policies that require companies to transfer, or provide access to, proprietary source code as a requirement for legal market entry. Intellectual property is the lifeblood of app developers' and tech companies' innovation; the transfer of source code presents an untenable risk of theft and piracy. Government policies that pose these requirements are serious disincentives to international trade.
- ***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 a technology developer'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 American innovators and hurts the billions of consumers who rely on their 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 company. The adequate and effective protection and enforcement of intellectual property rights is critical to the digital economy innovation and growth.
- ***Avoiding the Misapplication of Consumer Protection and Competition Laws to New and Emerging Technology Markets:*** Various regulators, including key trading partners, are currently considering or implementing policies that would put mandates on nascent and developing emerging technology markets. For example, some regulators are jeopardizing small businesses' ability to compete by upending the functionality of digital platforms that lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections. Others are considering interventions into undefined and emerging technology markets, such as for artificial intelligence. Foreign governments upending technology markets through misguided regulations inconsistent with U.S. law will disadvantage American innovators and serve as significant trade barriers.

Traditionally, USTR has been a consistent supporter of pursuing the above principles in international trade discussions. However, during the previous Administration, USTR withdrew its support for several of these policies in its NTE for 2024, including enabling cross-border data flows, avoiding forced data localization mandates, protecting source code, and ensuring digital products are not unduly discriminated against. This shift widened gaps facing U.S. small technology firms that depend on predictable rules-based certainties in digital trade, overlooking the unique vulnerabilities of these firms, particularly their limited capacity to navigate divergent foreign regulatory regimes and rising compliance costs. Weakening the U.S. bargaining position on these issues is counterproductive. As explained in a multi-association stakeholder letter led by the App Association to the Biden Administration,[4] we are deeply concerned that additional trade barriers that could result from a U.S. retreat from these important policy goals would fall especially hard on small businesses, which are less able to absorb increased costs than large multinational firms. We therefore urge in the strongest terms that USTR return to the battlements on these key issues in the 2026 NTE.

Next, we would like to highlight specific trade barriers related to intellectual property (IP). 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[5] and IPR violations. Between 2013 and 2018, App Association member developers and publishers lost an estimated $17.5 billion to pirated apps.[6] Such a 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).

---

[4] *See* https://actonline.org/wp-content/uploads/Small-Business-Ltr-re-USTR-Digital-Trade-3-Nov-2023-w-cosigners-1.pdf .

[5] *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.

[6] 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.

- ***"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 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.[7]
- ***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.[8] 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.[9] 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.

Relatedly, 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-

[7] Survey Says: IP is Essential to Innovation (June 21, 2022), https://actonline.org/2022/06/21/survey- says-ip-is-essential-to-innovation/.
[8] 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.
[9] 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/.

practicing entities (NPEs) initiate a majority of the abusive and frivolous patent infringement suits in the United States[10] and 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.[11] 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.

We also draw USTR's 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.[12] 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 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 inhibit the free flow of data and digital commerce in the NTE.

---

[10] 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/.

[11] *See In re Nimitz Technologies LLC*, No. 23-103 (Fed. Cir. 2022); *see also* https://www.unifiedpatents.com/insights/2023/2/21/litigation-investment-entities-the-investors-behind-the-curtain.

[12] *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.

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) 2026 NTE report. The practices highlighted below include both implemented and proposed policies, both of which should be considered by USTR.

AUSTRIA

Issue: Digital Services Taxation

Austria has implemented a DST that imposes a 5% tax on the advertising revenues of U.S. digital companies. For reasons discussed above, the App Association is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

Issue: Prohibitions on the Use of Strong Encryption

The App Association remains concerned with Australian policymaking efforts that stand to undercut the ability to leverage end-to-end encryption and otherwise undermine privacy protection practices, notably through its failure to revise the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. The App Association continues to work with the Australian government to reform surveillance and privacy frameworks while protecting online privacy and security.

Issue: Digital Platform Regulation

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. Most recently, the Australian Treasury has officially proposed a new digital competition regulatory intervention, with comments due February 14, 2025.[15] The App Association 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[16] and participated in a stakeholder hearing that took place in June 2022.

The App Association has significant concerns with ACCC's apparent positioning of the 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, including with respect to intellectual property enforcement at the platform level. We therefore request that the ACCC's digital platform regulatory efforts, and the risks they pose to American small business innovators that rely on software distribution platforms for intellectual property rights 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://treasury.gov.au/consultation/c2024-547447.
[16] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25/september-2022-interim-report.

be captured in the investigation of harm from non-reciprocal trade agreements 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.

Issue: Artificial Intelligence Regulation

The Australian government is seeking to categorize all general-purpose AI models as high-risk under a new regulatory framework, which would impose substantial compliance burdens on U.S. companies offering AI products and services in Australia. The App Association has significant concerns with this approach, which would distort the Australian market and inhibit our members ability to compete there.

Issue: Merger Policy Reform

As of March 2025, the Australian government has made significant changes to its merger review policies and processes, creating new challenges for small businesses seeking to enter pro-competitive transactions. For App Association members, acquisition is often a critical path for future growth. While we share the goals of creating an efficient and transparent process for mergers and acquisition (M&A) review in Australia, the App Association continues to encourage the Australian Parliament to ensure that any reforms do not unfairly increase burdens on small companies or prevent pro-competitive transactions. Relatedly, in August 2024, more than 50 App Association small business technology developer members signed an open letter to global regulators advising caution when updating existing merger rules, and to emphasize the importance that M&A has in the startup ecosystem. Building on its longstanding advocacy to Australian policymakers on competition issues, the App Association will continue to work with its members to advocate for merger policy reform that supports small company innovation and growth and will work to bring the voice of small technology developers to the table as the Australian Parliament debates this legislation.

BELGUIM

Issue: Digital Services Taxation

Belgium's government has pledged to introduce a 3% DST by 2027. For reasons discussed above, the App Association is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

BRAZIL

Issue: Brazilian General Data Protection Law

The National Congress of Brazil passed the Lei Geral de Proteção de Dados Pessoais (LGPD)[17] in August of 2018. The LGPD was enacted on August 27, 2020, and came into force, allowing for

[17] 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.

penalties and sanctions to be imposed, on August 1, 2021.[18] Various provisions of the LGPD, much like the EU's General Data Protection Regulation , 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 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.[19] Such provisions can be an insurmountable hurdle to our small business members seeking to enter the Brazilian market. Anything that can be done throughout the LGPD's implementation process to ease the burden for small and medium-sized companies could have tremendously positive economic implications.

More recently, Brazil's Congress introduced Bill No. 4097/2023, which seeks to impose new "digital sovereignty" measures within the LGPD. This bill would require IT companies operating in Brazil to have a significant level of Brazilian ownership and control—such as at least 25 percent of voting shares held by Brazilian nationals, incorporation under Brazilian law, or headquarters in Brazil.

Issue: Proposed Intervention into Competitive Digital Markets

The App Association remains concerned with the introduction of PL 2768/2022 in the Brazilian House of Representatives, which would designate certain digital platforms as "essential access control power holders" and intervene into their operations, oblige the payment of an inspection fee amounting to 2 percent of their annual gross operating revenue, and empower Brazil's National Telecommunications Agency (ANATEL) to sanction platforms with a fine of up to 2 percent of the national revenue and suspend certain business activities. The App Association is also concerned about the development of a report on digital markets by Brazil's Department of Economic Studies (DEE) of the Administrative Council for Economic Defense (CADE) intended to substantiate the Brazilian government's competition-themed intervention into digital markets. Brazilian government intervention into the digital economy would jeopardize the functionality of mobile operating systems and software distribution platforms that have enabled countless American small businesses to grow.

The Brazilian government later released its Digital Platform Report. The App Association has urged that Brazilian government's next steps be taken only after carefully considering the impact of proposed interventions into nascent and evolving markets that support small business growth and job creation in Brazil. Any Brazilian government interventions into digital platform markets should be based on demonstrated risks to competition and consumers and avoid disrupting the competitive dynamics of the app economy. The App Association notes its support for the report's recommendation that CADE, the government's primary competition agency, is best suited to lead the Brazilian government's work in overseeing digital platforms using Brazil's existing laws. As the Brazilian government continues to assess digital platform competition and next steps, the App Association will work closely with local policymakers to ensure the perspective of small business technology developers are at the forefront of the decision-making process.

---

[18] 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.
[19] 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.

Most recently, Brazil's new digital platform legislation, Bill 4.675/2025, has been introduced. The bill aims to regulate large digital platforms by introducing *ex ante* rules similar to the European Digital Markets Act. The bill proposes creating a distinct Digital Markets Superintendency to enforce special obligations on companies deemed to have "systematic relevance" in digital markets, based on criteria like market power and data control. Key features include mandatory interoperability, prohibitions on self-preferencing, algorithmic transparency, and data portability, with sanctions of up to 20% of Brazilian turnover for non-compliance. These regulations will affect a select group of no more than 10 companies, targeting those already designated as "gatekeepers" under the EU's DMA framework - predominantly American technology companies. The proposal's structure will create an uneven playing field, where other foreign and domestic competitors will not need be subject to the same rules, uncertainty or potential fines.

Issue: OTT Regulatory Requirements

The App Association is concerned with the launch of a public consultation by ANATEL proposing mandates for financial contributions by OTTs (termed "value added services") for the improvement, expansion, and maintenance of the network infrastructure and a related push to establish ANATEL as a regulator for the digital economy in Brazil. The expansion of network infrastructure support fees to OTTs would imperil countless network edge technology innovators' efforts to grow and create new jobs and contradicts well-established U.S. policy on universal service contribution base expansion.

Issue: Intellectual Property Rights (IPR) and Standards

Brazil has begun presenting IPR and competition challenges for App Association members. The country is seeing an influx of SEP disputes, in which injunctions are being rapidly awarded without serious competition consideration. This trend of injunctive relief is in part because Brazilian IP law does not require previous licensing negotiations or notice prior to seeking an injunction. In adjudicating these cases, Brazilian courts do not delineate their treatment of SEP cases and cases regarding regular patents as opposed to the U.S. courts that make this distinction through a proportionality test that determines when an injunction is appropriate and within the public interest.[20] Instead, Brazilian courts apply either preliminary or final injunctions that do not adequately consider SEP holders' voluntary FRAND commitments. For example, while preliminary injunctions in Brazil are assessed based on the impact on the defendant's business and public interest as mandated by Article 300(3) of the Civil Procedure Code, final injunctions are issued almost automatically upon a finding of infringement. This places SEP holders in a unique position to control who can use a standard by virtue of their patent's necessity.

The Brazilian patent system contributes to the enabling (and emboldening) of foreign SEP holders to systematically abuse their dominant market position as a gatekeeper to the use of the standard to attain supra-FRAND terms (a practice known as hold-up[21]) from U.S. businesses. For example, Swedish company Ericsson is a well-known SEP holder that uses courts in key jurisdictions to support hold-up tactics. Most recently, Ericsson sought injunctions in Brazilian and Colombian courts after filing a suit in the United States for the same alleged infringement but before a U.S.

[20] *eBay Inc. v. MercExchange, L.L.C*, 547 U.S. 388 (2006).

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

court could determine FRAND compliance. While the lower court denied the defendant's plea for an anti-suit injunction against Ericsson to stop interference of U.S. jurisdiction over the case, the United States Court of Appeals for the Federal Circuit reversed and remanded this decision.

Therefore, the FRAND commitment can only be raised as an affirmative defense to a patent infringement suit. We expect Brazil's jurisprudence to have a significant impact on the global SEP licensing landscape. We encourage USTR to work with Brazil to improve their approach to SEPs.

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.

Further, recent amendments to Institutional Security Group (GSI) policies require the localization of certain types of government data. The GSI, led by the military, issued a Normative Instruction outlining new rules for federal cloud service contracts, mandating that data and metadata be stored exclusively within Brazil in certain cases. These requirements disadvantage foreign digital service providers that lack local data storage capabilities, setting a concerning precedent for broader data localization mandates.

Meanwhile, the Department of Innovation within the Ministry of Development, Industry, and Trade (MDIC) is exploring legislative proposals modeled after the European Union's Data Act, aimed at regulating the "data economy." While no formal proposal has been released, a public consultation is expected by the end of the year, with discussions on how Brazil should implement a similar framework. There is concern that such regulations could impose discriminatory obligations on U.S. companies, particularly through targeted thresholds.

Brazil also maintains various data localization barriers, largely in response to the limited competitiveness of its domestic tech sector. It offers tax incentives for locally produced information and communication technology (ICT) goods and equipment (under the Basic Production Process – PPB, Law 8387/91, Law 8248/91, and Ordinance 87/2013) and prioritizes local ICT hardware and software providers in government procurement (per 2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903). Additionally, Brazil does not recognize conformity assessments conducted outside the country for telecommunications equipment (per ANATEL's Resolution 323).

The GSI has also updated its cloud computing guidelines, mandating localization for certain types of government data. While these rules currently apply only to government data and remain advisory in nature, they set a troubling precedent for broader restrictions on cross-border data flows, raising serious concerns for U.S. digital service providers operating in Brazil.

Issue: Artificial Intelligence

Brazil's Congress is rapidly advancing AI regulation that diverges sharply from the U.S.-led risk-based approach and could undermine the global competitiveness of American technology firms. Bill 2338/2023, already approved by the Senate and pending House approval, has faced

widespread opposition from civil society, businesses, and academia, who warn it could harm Brazil's economy, stifle innovation, and disrupt international interoperability. The bill would impose significant restrictions on U.S. AI developers and businesses deploying AI-driven solutions, limiting their ability to export tools and services to Brazil—dealing a major setback to leading U.S. innovators competing against Chinese tech firms. Of particular concern, the bill takes a broad, indiscriminate approach to AI regulation, failing to focus on high-risk applications and instead encompassing even low-risk, routine business functions. Additionally, it lacks clear distinctions between AI system developers and deployers, creating regulatory uncertainty that could severely hinder companies of all sizes from advancing AI innovation.

Issue: Digital Services Tax

The App Association is a strong supporter of the several multilateral efforts to keep digital services taxes (DSTs) out of the international taxation system. Despite these efforts, the Brazilian Congress has introduced a number of bills seeking to create a DST that would impact any U.S. company that does business in Brazil. Seven such bills are currently under consideration, and President Lula recently expressed report for their goal of "charging taxes from U.S. digital service providers." If the policy envisioned by these bills—an additional tax exclusively on the revenue of multinational companies—becomes law, the burden will fall heavily on American companies and may force small businesses to withdraw from the country's marketplace.

CANADA

Issue: Digital Service Taxes

The Canadian government's recent positioning with respect to DSTs, including its opposition to the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting's agreement extending a moratorium on imposing DSTs, is a matter of concern. The App Association has consistently made clear that a Canadian DST would negatively impact Canada's and the United States' most innovative markets, including software development and IoT connected devices, in which App Association members lead.

On June 2025, Canada announced a planned repeal of its DST before its first collection. The DST was initially adopted in June of 2024, which would impose a three percent tax on online services, primarily targeting U.S firms and retroactively costing them an estimated US$3 billion in 2025.[22] While collection has paused, reimbursements have yet to be made for payments made by industry in anticipation of the tax, and the law has yet to be formally repealed, leaving open the possibility of its revival. App Association members remain concerned about the changes to Canadian law that may upend business planning and research and development cycles for small business innovators and are inconsistent with international tax standards, chilling the investment and innovation climate in Canada and abroad. The App Association encourages the USTR to continue its formal dispute investigation, beginning with consultations under the U.S.-Mexico-Canada Agreement's framework, to continue defending small business innovators.

[22] https://www.congress.gov/crs-product/IN12399

Issue: Data Protection and Localization Requirements

The Province of Québec's privacy legislation, Bill 64 (the Act to Modernize Legislative Provisions as Regards the Protection of Personal Information), adopted in 2021 followed by phased in enforcement, significantly restricts cross-border data transfers and introduces compliance burdens that are disproportionate for small firms.[23] The U.S. International Trade Commission identified the law as a barrier to digital trade in its Year in Trade 2021 report.[24] The law's prescriptive consent and localization requirements create operational uncertainty for U.S. technology providers and threaten the integrity of the integrated U.S.–Canada digital marketplace.

At the federal level, the Canadian government has indicated plans to reintroduce comprehensive privacy legislation in 2025. This approach renews focus on "digital sovereignty" and could introduce additional restrictions on cross-border data flows and data storage. Such provisions increase compliance costs and legal uncertainty for U.S. companies, impede innovation in emerging fields such as artificial intelligence, and risk fragmenting a market long defined by interoperability.[25] The App Association urges USTR to engage proactively with the Canadian government to advocate for a privacy framework that aligns with global standards and supports a fair and open digital marketplace. The App Association remains concerned with Bill C-27, which proposes comprehensive updates to federal privacy legislation, is currently under review by the House of Commons Industry Committee. The bill seeks to align Canada's private-sector privacy laws with European data protection standards while introducing new obligations with respect to minors. Although the government has expressed a commitment to regulatory interoperability, further work is needed at the committee level to ensure consistency and predictability for businesses operating nationwide. Key areas requiring clarification include establishing a uniform definition of a minor (as provincial definitions vary), refining consent exceptions, explicitly recognizing advertising and marketing as legitimate business activities, and confirming a 2-3-year implementation timeline. Once approved by the House of Commons Committee, the bill will proceed to the Senate for further review.

Additionally, in August 2025, Shared Services Canada (SSC) issued a request for information to guide the development of a sovereign procurement regime for Infrastructure-as-a-Service and Platform-as-a-Service offerings.[26] This proposal would require that all government data be processed and stored within Canada and that providers—including parent companies—be free from any foreign legal obligations permitting external governmental access to data. Invoking a "national security exception" to justify these restrictions, the proposal would effectively exclude U.S. cloud providers based on ownership rather than objective security criteria. Such an approach risks violating Canada's trade commitments and unfairly discriminates against U.S. suppliers by limiting their ability to compete in public-sector procurement. The App Association urges USTR to treat Canada's proposed localization and procurement policies as discriminatory trade barriers warranting continued monitoring and engagement in the 2026 NTE.

[23] https://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html
[24] https://www.usitc.gov/publications/332/pub5349.pdf
[25] https://www.lexisnexis.com/blogs/en-ca/b/legal-thought-leadership/posts/canad-a-at-a-privacy-crossroads-what-legal-professionals-should-watch-for-post-bill-c27#:~:text=Bill%20C%2D27%20was%20designed,AI%20or%20modern%20data%20practices.
[26] https://canadabuys.canada.ca/sites/default/files/webform/tender_notice/71894/rfi-dr-wave-1---vague-1---sovereign-cloud-supplier-webinar---august-22-2025_0.pdf

Issue: Intellectual Property Rights Enforcement

The App Association remains concerned with the Canada's approach to Intellectual Property Rights Enforcement. The Canadian government's notice and notice requirement under Canada's Copyright Act is an ineffective step to ensure that internet services providers (ISPs) take reasonable steps to prevent piracy on their platforms. This process does not prevent infringers from engaging in illicit acts, such as the common IPR violations provided above that affect App Association members. Stronger enforcement mechanisms, such as a notice-and-takedown procedures provided by the U.S. Digital Millennium Copyright Act (DMCA) are more effective steps that should be encouraged to the Canadian government to protect businesses, including App Association members, that interact with their economy.

Issue: Artificial Intelligence Regulation

In June 2022, the Canadian government introduced the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27, the Digital Charter Implementation Act, 2022. AIDA grants the government broad authority to regulate "high-impact" AI systems, but its overly vague definitions risk encompassing low-risk applications, posing significant challenges for U.S. companies and the U.S.-led risk-based approach to AI governance. The bill also includes steep penalties—up to 3% of global revenue—and introduces an unprecedented criminal enforcement provision for non-compliance. This regulatory framework would impose a heavy compliance burden on leading U.S. AI researchers and developers while undermining interoperability across North America. Since its introduction, AIDA has faced significant criticism from stakeholders for its ambiguous language, lack of proper consultation, and misalignment with global AI standards.

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 in 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.[27] 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 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

[27] 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/.

either of these terms, businesses are left to speculate on how to apply the law. As a result, app developers 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 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.[28] 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.[29]

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.

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[30] on the Cybersecurity Administration

[28] 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/

[29] 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.

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

of China'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) was enacted by the Chinese National People's Congress on August 20, 2021, and took effect on November 1, 2021.[31] 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 reduce their ability to do business in China. We therefore request the inclusion of the PIPL in the NTE report.

Issue: Various Data Localization Requirements (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. Companies face large penalties for non-compliance. These events threaten to disrupt the free flow of information over the internet on a much larger scale.

Issue: China's Use of Antitrust Laws

The App Association believes USTR should, in the context of China's WTO commitments, remain concerned with China's antitrust laws being used as a means to target foreign firms which USTR has already documented and addressed. China's activities justified under antimonopoly laws often contradict China's commitments under the WTO, including in relation to IP licensing in violation of TRIPS Article 40 Section 8, and in violation of Article 40 which invokes other standards in TRIPS, such as due process ("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

[31] 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.

represented by independent legal counsel").[32] In addition, China's antimonopoly laws justify Chinese court practices, such as extra-territorial antisuit injunctions, likely in violation to China's commitment to TRIPS Articles 1.1, 28.1, 28.2, 41.1, 44.1, 63.1, and 63.3. China's antitrust and competition laws continue to raise concerns regarding their deployment against foreign firms as part of broader economic statecraft. Notably, SAMR's enforcement practice increasingly employs discretionary measures which may conflict with WTO TRIPS procedural safeguards, such as due process rights, evidentiary standards, and independent legal counsel protections. Chinese courts' use of extraterritorial antisuit injunctions and other measures targeting foreign parties may also contravene China's WTO commitments.
Recent high-profile antitrust investigations during 2024-2025 illustrate an intensification of scrutiny over foreign company operations in China, linked to claims of IP misuse and competition harm, although transparency remains limited. These instances highlight the ongoing tension between China's ambitions to protect domestic industry and the trade obligations that guard fair treatment of foreign entrants.

Issue: Harmful Digital Platform Regulation

China's new digital platform policies impose stringent requirements on digital platforms, substantially increasing compliance burdens and operational risks. Notably, frequent reporting obligations, the risk of heavy fines, and potential business suspensions create significant regulatory barriers for cross-border e-commerce and digital services, particularly for App Association members, hindering digital trade and complicating market entry and operation.

Issue: Intellectual Property in China

Theft and infringement of IP has grown exponentially in recent years and often originates in China. China's harmful practices put our members' businesses and the jobs they create at serious risk – a single occurrence can represent an "end-of-life" scenario. Both criminals and government-backed hackers based in China are a demonstrated and well-known risk to our members in the digital economy, and the Center for International and Strategic Studies has described China's behavior as "long-running state espionage programs targeting Western firms and research centers" that has carried over into cyberspace.[33] Numerous USTR National Trade Estimate (NTE) reports have detailed how 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. China appropriately remains on USTR's Priority Watch List of countries committing the most extensive IP rights infringements.[34] We support investigations into unfair cloud computing-related and other digital trade barriers, where China has intentionally disenfranchised U.S. firms.[35]

---

[32] 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.
[33] Jim Lewis, "Learning the Superior Techniques of the Barbarians," Center for International and Strategic Studies.
[34] https://ustr.gov/sites/default/files/IssueAreas/IP/2022%20Special%20301%20Report.pdf
[35] Stephen Ezell, "Hearing on U.S.-China Innovation, Technology, and Intellectual Property Concern," (April 14, 2022), 15, https://www2.itif.org/2022-us-china-innovation-tech-ip.pdf.

First, we fully support strong and enforceable IP rights for U.S. companies and condemn government policies that seek to diminish those rights to hinder market entry. To the extent these policies are used by the Chinese government, we urge USTR to investigate and document them to determine its next steps. 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)[36] 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 Provisions Prohibiting the Abuse of IPR to Eliminate or Restrict Competition, that were most recently updated in 2023.[37] These rules prohibit the preclusion or restriction of 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 App Association does not support the notion that competitors should have access to regular 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 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, like 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. 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, many standards development organizations (SDOs) 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 SDO, 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.

[36] SAIC has since been merged into the State Administration for Market Regulation.

[37] https://www.samr.gov.cn/zw/zfxxgk/fdzdgknr/fgs/art/2023/art_e155397fbe5c4c05ad3c1838c1322ad2.html.

In line with our members' core interests in this area, the App Association has advocated for the following consensus principles to prevent patent "hold-up" and anti-competitive conduct:

- **The FRAND Commitment Means All Can License** – A holder of a FRAND-committed SEP must license that SEP to all companies, organizations, and individuals who use or wish to use the standard on FRAND terms.
- **Prohibitive Orders on FRAND-Committed SEPs Should Only Be Allowed in Rare Circumstances** – Prohibitive orders (federal district court injunctions and U.S. International Trade Commission exclusion orders) should not be sought by SEP holders or allowed for FRAND-committed SEPs except in rare circumstances where monetary remedies are not available.
- **FRAND Royalties** – A reasonable rate for a valid, infringed, and enforceable FRAND-committed SEP should be based on the value of the actual patented invention itself, which is separate from purported value due to its inclusion in the standard, hypothetical uses downstream from the smallest saleable patent practicing unit, or other factors unrelated to invention's value.
- **FRAND-committed SEPs Should Respect Patent Territoriality** – Patents are creatures of domestic law, and national courts should respect the jurisdiction of foreign patent laws to avoid overreach with respect to SEP remedies. Absent agreement by both parties, no court should impose global licensing terms on pain of a national injunction.
- **The FRAND Commitment Prohibits Harmful Tying Practices** – While some licensees may wish to get broader licenses, a SEP holder that has made a FRAND commitment cannot require licensees to take or grant licenses to other patents not essential to the standard, invalid, unenforceable, and/or not infringed.
- **The FRAND Commitment Follows the Transfer of a SEP** – As many jurisdictions have recognized, if a FRAND-committed SEP is transferred, the FRAND commitments follow the SEP in that and all subsequent transfers.

In the past, SAMR (and its predecessors) have attempted to finalize 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. With assistance from the international community, such efforts have been thwarted. Today, SAMR appropriately recognizes 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." While an official translation is not available, further guidance issued by the Chinese government since appears to be consistent with this approach.[38] The App Association, therefore, does not believe that inclusion of the SAMR's rules addressing SEPs constitutes 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 additionally commend SAMR for taking positive and significant steps to investigate into patent pool practices that do not align with its Anti-Monopoly Law, including evidenced

[38] 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.

anticompetitive practices by Avanci in the automotive industry[39] and for providing updated guidance reinforcing respect for FRAND commitments without mandatory licensing beyond essential patents.

In contrast to its policies on patents generally, SAMR's treatment of FRAND-committed SEPs is consistent with an established consensus on the meaning and effect 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 standard-essential patents.

COLOMBIA

Issue: Digital Services Tax

Colombia has introduced a 3% tax on digital services provided by foreign companies starting January 2024 under its Significant Economic Presence framework. In September 2025, the government proposed raising this rate to 5% through a tax reform bill. This policy imposes additional tax burdens on U.S. digital service providers, undermining the United States-Colombia Trade Promotion Agreement (USCTPA) by treating them unfavorably.

Issue: Intellectual Property Rights

We note that Colombia's patent system is similar to that of Germany and Brazil in that the system bifurcates infringement and validity proceedings, so that an injunction may be awarded even if the validity of the patent has not been examined in complete misalignment with the U.S. approach under eBay, denying adequate protection to U.S. small businesses that rely on a fair and transparent SEP licensing ecosystem to engage in standards-driven markets. Colombia's system has led Swedish company Ericsson to use this court system to leverage their bargaining position in SEP licensing negotiations, much like German courts are abused for the same purpose. Unless addressed by the United States, we expect that Colombia will continue to be a venue for SEP licensing abuse and have a significant impact on the global SEP licensing landscape and American small businesses in particular.

Issue: Over-The-Top Regulation

Colombia's Communications Regulatory Commission (CRC) and Ministry of Information and Communications Technologies (MinTIC) launched a consultation in 2024 aimed to gather input on OTT digital services, which has fed into the prospect of introducing specific regulations or fees on OTT platforms. The App Association has engaged with CRC and MinTIC, raising concerns that such policy changes would put trade barriers into place, stifling innovation and limiting competition in Colombia's digital ecosystem, most acutely harming small companies.

[39] *See* Zhong Chun, A deep dive into China's three-letters-one-notice system as compliance challenges emerge for patent pools, GCR (Aug. 22, 2024), https://globalcompetitionreview.com/hub/sepfrand-hub/2023/article/deep-divechinas-three-letters-one-notice-system-compliance-challenges-emerge-patent-pools; *see also* Carrier, Michael A. and Scarpelli, Brian and Nair, Priya, Admissions Confirm Avanci's Rigged Game (September 03, 2024). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4945572.

CZECHIA

Issue: Digital Services Taxation

Czechian government has proposed a 7% DST. For reasons discussed above, the App Association is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

EUROPEAN UNION

Issue: Digital Platform Regulation

The App Association has concern with numerous steps taken by the EU themed in advancing European sovereignty, which often are positioned to exclude American companies from entering and competing in the EU.

As a prime example, the European Commission's (EC) imposition of regulations on digital platforms, via the Digital Markets Act (DMA)[40] continues to present a significant protectionist barrier to trade. The DMA, without justification, intervenes in the operations of competitive and well-functioning digital markets that enable countless small businesses to grow and create jobs. By creating new obligations for "gatekeeping" platforms, the DMA has had, and will have, far-reaching consequences for the companies that operate on them, including App Association members. As recent reports have demonstrated,[41] Implementing this novel piece of regulation thoughtfully will be more critical than ever to ensure it does not only level the playing field between the largest players but also truly benefits all businesses, including small app developers. If not implemented with small enterprises in mind, some of the obligations for gatekeepers will lock small app developers with fewer resources out of the market. Further, the DMA's broad-stroke obligations for online platforms has unintentionally open the gate to malicious actors and put end-users' data and safety at risk. App developers rely on the safe environment platforms provide to keep bad actors out of the app ecosystem, gain consumers' trust, and innovate. The DMA must be implemented to enable all SMEs to innovate, grow, and thrive in a fair, competitive, and safe app ecosystem, and the App Association looks forward to collaborating with policymakers to ensure SMEs continue to succeed. The DMA has already been appropriately acknowledged by USTR as a barrier to digital trade and should remain designated as such in future NTEs. As we have discussed in a recently-released paper, the impact of the DMA has been harmful and discriminatory in its first year of operation.[42]

The App Association agrees that the DMA functions as an ex ante competition regulation that is in effect targeting U.S. entities (e.g., notably identifying six U.S. companies as gatekeepers that must adhere to restrictions on data usage, obligations for data portability and access, and requirements for interoperability). Currently, the EC is imposing substantial fines on these companies in enforcement, with the harm to our community only beginning to be understood. A mandatory

[40] European Commission, *Online Platforms, available at* https://ec.europa.eu/digital-single-market/en/policies/online-platforms.
[41] https://www.politico.eu/article/iphone-apple-eu-ios-dma-big-tech-anti-competition-pornhub-users-app/.
[42] https://actonline.org/wp-content/uploads/DMA-One-Year-Later.pdf.

review of the DMA is set for May 2026, which could broaden its scope to encompass additional services, such as generative AI and cloud computing.

Further, the EC has already carried forward numerous regulations, directives, consultations, and proposals that raise significant concerns for the App Association, including 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.

Issue: Privacy Regulation

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.[43] 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.

Issue: Digital Service Taxes

Numerous EU Member States without a DST in place are looking to revive discussions on a Directive for a common system of digital services tax on revenues generated from certain digital services and potentially a corporate tax on a "significant digital presence." The App Association strongly encourages the USTR to oppose discriminatory DSTs.

Issue: Network Usage Fees

Since 2022, the European Commission has pursued ways to impose network usage fees on large digital service providers, primarily U.S. technology and content companies, requiring them to subsidize European telecom operators' infrastructure. Despite the EU's commitment in the EU-U.S. Joint Statement not to adopt such fees, the Commission is considering indirect approaches through the upcoming Digital Networks Act (DNA), expected in December 2025. This act may extend the scope of the European Electronic Communications Code (EECC), imposing new costs throughout the internet infrastructure and network edge layers, harming small developers. Italy's AGCOM has already set a precedent by ruling CDNs fall under EECC dispute mechanisms, allowing Italian telcos to press payment claims, a move that could spread across Europe if unchecked. These developments threaten to impose hidden costs on small U.S. digital firms.

Issue: Standards Regulation

In a development that could significantly influence the direction of data and AI regulations, the European Commission has initiated a project to localize standards-setting within the Union for essential sectors of the economy. The EC has stated that this effort aims to prevent the "undue influence of actors from outside the EU and EEA" in establishing standards for crucial areas. As a

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

result, this initiative could limit App Association members' capacity to contribute to the standards that will be vital for upcoming regulations.

Issue: EU Space Act Proposal

The EU Space Act proposal, introduced in June 2025, introduces uncertain and potentially novel technical requirements on service providers that diverge from international norms, particularly in areas like orbital congestion and collision avoidance. Further, under the Space Act, EU operators must rely on the EU Space Surveillance and Tracking system, while non-EU operators, including U.S. companies, face operational challenges due to exclusion from this system and must meet alternative standards not aligned with best practices. The law also discriminates in registration processes by imposing undefined timelines on non-EU operators and features governance concerns given potential conflicts of interest. Enforced from 2030, with a tight compliance window for next-generation constellations, the Act grants the Commission inspection rights over non-EU facilities, raising issues around confidentiality and conflicts with U.S. regulations. Overall, the EUSA imposes disproportionate burdens on non-EU operators, effectively limiting their competitiveness in the European space market, reducing competition in connectivity markets, with harms flowing down to small businesses that rely on a competitive market for internet connectivty.

Issue: Cloud Security Regulation

Since 2020, the EU Agency for Cybersecurity (ENISA) has been developing the European Cybersecurity Certification Scheme for Cloud Services (EUCS). In June 2022, ENISA revised the draft framework to introduce four new criteria— including immunity from foreign law—for cloud service providers (CSPs) to qualify for the highest cybersecurity certification level. If implemented, this requirement would restrict eligibility to companies with their head office and global headquarters in an EU Member State, effectively barring U.S. CSPs from servicing the public sector and regulated industries in the EU and limiting competition and choice for small businesses. While the European Commission has temporarily suspended negotiations on the EUCS, it is expected to use the forthcoming revision of the EU Cybersecurity Act (CSA) to reintroduce discriminatory requirements in future certification schemes.

Issue: Network Usage Fees

In 2022, the European Commission initiated a consultation to assess the feasibility of requiring large content and application providers to contribute financially to telecom infrastructure development in Europe. Backed by European telecom operators, this proposal would initially compel six U.S. companies to pay €20 billion annually to telecom operators for infrastructure support. Despite widespread opposition from many key stakeholders including the App Association, the Commission advanced a similar proposal in its February 2024 White Paper on the future of Europe’s digital infrastructure. The paper suggests expanding EU telecom regulations to include CSPs, introducing an arbitration mechanism that mandates interconnection fees to telecom operators, and imposing "universal service obligations" requiring digital companies to co-finance telecom infrastructure in rural and remote areas.

Although the proposal continues to face strong resistance from the App Association community, it is being pushed forward with the support of aggressive lobbying from major European telecom operators.

Issue: Artificial Intelligence Regulation

The EU's enactment of sweeping regulations on the use of artificial intelligence (AI)[44] raises concerns for the App Association about regulation pre-empting new and innovative uses of AI and related IPR issues. On August 1, 2024, the EU AI Act went into force, which include both positive and uncertain approaches to regulating AI. While we appreciate the EU's use of a risk-based approach, we are most concerned with the cost of complying with minimum requirements for transparency and safety standards for SMEs and startups.

Additionally, the AI Act will mandate that providers of general-purpose AI models disclose a "sufficiently detailed" summary of their model training data. The European Commission is currently working on a template for these disclosures. If the template requires detailed disclosure of training data, it could compromise the intellectual property and trade secrets of model developers. Furthermore, Recital 106 of the AI Act states that "any provider placing a general-purpose AI model on the Union market must comply with [the Regulation's copyright obligations], regardless of the jurisdiction in which the copyright-relevant acts related to the training of those general-purpose AI models occur." If the AI Act imposes more rigorous requirements or compliance standards, it could further complicate matters for small developers.

We also note that European standardization organizations CEN and CENELEC have established a dedicated technical committee (JTC 21) to create harmonized standards that will facilitate the implementation of the AI Act. This includes developing a framework for AI trustworthiness, as well as standards for AI risk management and quality assurance. It remains uncertain whether these standards will align with existing ISO standards, such as ISO 42001. If the standards diverge, the App Association community would face immense burdens in adjusting to EU-specific requirements.

Issue: Intellectual Property and Standards

The established Unified Patent Court (UPC) has posed significant concerns for American companies that operate within the EU economy. The UPC enables holders of IP issued in one of the 18 Member States that joined the court to seek an injunction that would be applied across all 18 jurisdictions. The court has become an attractive venue for SEP holders who use the court to leverage their dominant market position against potential licensees. In a 2024 case between Chinese company Huawei and American entity NETGEAR, the Munich Local Division refused to follow the important holding from the Court of Justice of the European Union (CJEU) in *Huawei Technologies Co. v. ZTE Deutschland GmbH,* which provided steps that SEP holders must take in order to enforce an injunction against an alleged infringer.[45] We suspect that the UPC will continue to be a venue ripe for abuse of SEP and other IP rights against American companies.

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

[45] *Huawei Technologies Co. v. ZTE Deutschland GmbH* (CJEU 2015) (The court provided steps that a SEP licensor must take to enforce an injunction against an infringer: 1) The SEP holder must notify a party of infringement before bringing an action; 2) If the party is a willing licensee, the SEP holder must provide a written licensing offer in coordination with the FRAND commitment; 3) If the licensee continues infringement

We note that while the European Commission's recent request to withdraw the EU proposed regulation on standard-essential patents (SEPs) will continue to enable bad actors to abuse the SEP licensing and standards ecosystem. A lack of soft intervention in the EU SEP landscape will impact all American businesses that build on top of technical standards and sell their products and devices in the EU. We urge the USTR to support the EU in moving forward with the proposed regulation on SEPs as an effective solution to improve judicial process that is inconsistent with established policy goals.

Each of these concerns is either effecting or proposing policy changes for nascent economic segments and services that are solutions in search of a problem and stand to enable discrimination against small digital economy innovators to compete in the EU.

FRANCE

Issue: Digital Services Tax (DST)

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 2019.[46] By September 2025, the French Constitutional Court ruled that the 3 percent DST is constitutional, dismissing the USTR's recommendations.[47]

In October 2025, the French National Assembly's finance committee voted in favor of a fivefold tax increase from 3 percent to 15 percent, specifically on U.S. tech companies.[48]France's 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 committed to withdrawing DSTs 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

Issue: Prohibitions on the Use of Strong Encryption

---

or does not provide a proper response (ex. counteroffer on FRAND terms), the SEP holder may seek an injunction).

[46] https://ustr.gov/sites/default/files/Report_On_France%27s_Digital_Services_Tax.pdf.
[47] https://kpmg.com/us/en/taxnewsflash/news/2025/09/france-dst-upheld-constitutional-court-decision.html
[48] https://waysandmeans.house.gov/2025/10/27/ways-and-means-committee-republican-leaders-slam-french-proposal-to-impose-higher-discriminatory-digital-services-tax-on-u-s-innovators/#:~:text=WASHINGTON%2C%20D.C.%20%E2%80%93%20As%20lawmakers%20in,against%20DSTs%20around%20the%20world.

The App Association is deeply concerned with efforts by the French National Assembly to pass legislation that would significantly weaken encryption (known as 'Loi Surveillance te Narcotraficotage') under the pretext of combating narcotrafficking. As we explain above, App Association members depend on the use of strong encryption techniques to keep users safe from harms like identity theft. French government efforts to require that backdoors be built into encryption keys for the purpose of government access jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit.

GERMANY

Issue: Data Sharing Mandates

The German Competition Act has been amended to incorporate extensive restrictions that disproportionately affect U.S. companies, including the mandatory sharing of proprietary data with competitors. This has already led to legal actions and findings aimed at U.S. firms.

Issue: Unbalanced German Patent Law as a Trade Barrier

Germany continues to develop damaging patent policy and enforcement frameworks. Under Germany's 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.

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 in its investigation of harm from non-reciprocal trade agreements.

In practice, German courts have historically been a favorable venue for patent holders to enforce their patents. Courts in Germany have been known to award injunctive relief to patent holders based on the court's determination of infringement before that validity of the patent has properly been assessed by the German Federal Patent Court. Germany's practice to award injunctions so readily has created international conflicts where their decisions extend to patents issues in another jurisdiction.

For example, in *Microsoft v. Motorola,*[49] a U.S. district court issued an anti-suit injunction 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 court-determined FRAND royalty for Motorola's portfolio. Motorola sought an injunction in Germany again in 2014 for Apple's alleged infringement of SEPs, but the European Commission found this action to be an abuse of the SEP holder's dominant position in the market, stating that the ability to seek injunctive relief against a willing licensee of a FRAND-encumbered SEP could limit products from the market

[49] 696 F.3d 872 (9th Cir. 2012).

and lead licensees to accept anticompetitive licensing terms that they would have not accepted absent the use or threat of an injunction.[50]

In the following years, German courts have continued their practice of awarding injunctions to SEP holders against licensees without first considering the validity of the patents, and on the basis that the licensee did not sufficiently express its willingness to take a licensee from the SEP holder.[51] The burden that German courts have imposed on licensees to show their "willingness" to accept a SEP holder's offered license on seemingly FRAND terms distorts an important holding from *Huawei Technologies Co. v. ZTE Deutschland GmbH*. German legislators have gone so far as to amend the German Patent Act to only exclude "under the special circumstances of a singular case and considering the principle of good faith, its enforcement would result in disproportionate hardship on the infringer or third parties beyond what is justified by the exclusionary right."[52] The European Commission's growing concern about German courts' interpretation of *Huawei Technologies Co. v. ZTE Deutschland GmbH* led to their amicus brief filed in the SEP dispute, *VoiceAgeEVS v. HMD*, before the Munich Higher Regional Court. The brief clarifies that CJEU decision and its importance to curb anticompetitive practices. While it remains to be seen if the Munich court will refer to the CJEU, the Commission's action underscores the ongoing concern about the practices of German courts enabling SEP licensing abuse.

Germany's approach to SEP injunctions has caused immense disruptions to supply chains across several industries and has resulted in various companies ceasing operation in the country because of the inability to reliably use standards (due to an imbalanced approach to SEP injunctions), fraying the international norm for limited inunctions on FRAND-committed SEPs and undermining international standards.

HUNGARY

Issue: Data Localization Requirement

In Hungary, data management for state and local government bodies providing essential services is regulated by Act No. 50 of 2013 on the Electronic Information Security of State and Local Government Bodies. This law mandates that data handled by these bodies must be processed and stored within Hungarian territory, unless the supervisory authority permits processing in another European Economic Area country. Additionally, any organization not registered in Hungary but dealing with such data is required to appoint a local representative in Hungary, ensuring compliance and local oversight.

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

[50] *See* https://ec.europa.eu/commission/presscorner/detail/en/IP_14_490.
[51] *See* Nokia v Daimler, District Court (Landgericht) of Mannheim, judgment dated 18 August 2020, Case-No. 2 O 34/19; *see* Sisvel v Haier, Federal Court of Justice, judgment dated 5 May 2020, Case No. KZR 36/17.
[52] Section 139 (1) of the German Patent Act.

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.[53]
- The 2015 National Telecom M2M ("machine to machine") Roadmap,[54] which has 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[55] 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.[56]

Issue: Intellectual Property Rights Enforcement

India represents an immense opportunity for American small business tech and software development companies. India's technology industry is becoming a global leader, employing over 5.4 million workers with revenues expected to rise by $245 billion at the end of 2023.[57] 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 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.

[53] 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.
[54] Government of India Ministry of Communications & Information Technology Department of Telecommunications, *National Telecom M2M Roadmap, available at* http://www.gsma.com/connectedliving/wp-content/uploads/2015/05/150513-DoT-National-Telecom-M2M-Roadmap.pdf.
[55] *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
[56] 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.
[57] See https://nasscom.in/sites/default/files/sr-2023-press-release.pdf.

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.[58] As of May 20, 2016, the Indian government established additional commercial courts, advancing the 2015 Commercial Courts Act,[59] 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 Intellectual Property Rights 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[60] 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 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.[61] This proposal threatens copyright protections that aim to protect small businesses and innovators alike.

India has become a new venue for SEP abuse, impeding over 3,000 SMEs and startups from

[58] *See* https://spicyip.com/wp-content/uploads/2018/01/IPR-Regime-In-India-Government-Initiatives.pdf.
[59] *See* https://timesofindia.indiatimes.com/city/delhi/Commercial-courts-begin-functioning-in-Delhi-Mumbai/articleshow/52488068.cms.
[60] *See* https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.
[61] 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.

bringing deep-tech solutions to critical global markets.[62] In 2023, the Delhi High Court held that SEP holders are not prohibited from seeking an injunction from the court at an interim or final stage.[63] Importantly, the court cited the UK Supreme Court 2020 decision in *Unwired Planet v. Huawei*[64] to support the notion that a SEP holder may require a license for a global portfolio of FRAND-encumbered SEPs, or alternatively receive an award of injunctive relief upon a *prima facie* showing that one patent in the portfolio is infringed.

This case was decided in parallel with an investigation by the Competition Commission of India (CCI) into multiple complaints, including by Intex, regarding Ericsson's alleged abuse of its dominant position in India in the context of SEP licensing. The Delhi High Court ultimately dismissed these proceedings on grounds that Indian patent law preempts competition law on patent-related issues, however the allegation in the CCI investigation, if proven true, would have revealed significant findings that Ericsson conducted anti-competitive SEP licensing practices that are antithetical to the FRAND commitment.[65] Complainants alleged that Ericsson engaged in discriminatory practices across similarly situated licensees, required restrictive nondisclosure agreements (NDAs), and licensing fees that reflected value unrelated to the patent technology being licensed.[66] The complainant, Micromax, stated that Ericsson demanded acceptance of licensing terms within 25 days of receiving those terms or else Micromax would have been considered unwilling to take the license and therefore infringing on Ericsson's SEPs.[67]

The Delhi High Court's decision to ignore complaints alleged in the CCI investigation and contribute bad case law formed across key jurisdictions aids opportunistic SEP holders in controlling markets by squeezing SME innovators, of their limited resources through exorbitant fees and supra-FRAND terms by threating or seeking to threaten national injunctions across the world. While we are encouraged by the court's clarification regarding the importance of adhering to FRAND principles in recent cases, we are concerned with the court's decision in *Intex v. Ericsson*, which makes it easier for SEP holders to receive preliminary injunctions.[68] In particular, the Delhi High Court made it easier for SEP holders to seek injunctive relief for global SEP portfolios by stating that there is no embargo on a SEP holder seeking an injunction from the court at an interim or final stage. The court also distorted their reliance on global precedent that reached a final determination, including cases from the United States, UK, and EU. For example, the decision allows the court to set FRAND rates and terms on global SEP portfolios based on likelihood, relying on *Unwired Planet v. Huawei*. The decision avoids important Indian precedent at the interim stage - *Nokia v. Oppo*, which laid out a four-factor test for the court to determine whether it could require royalty payments from an alleged infringer. Instead, Ericsson only had to establish a "prima facie" that it would prevail at end of case on the issues of whether the patents in suit were essential, valid, and infringed and that the royalty sought was FRAND. As a result, many cases have been decided at the preliminary stage and parties are unable to provide sufficient facts to prove their positions (ex. computation for FRAND rates).

---

[62] *Id*.
[63] Intex Technologies (India) Ltd. V. Telefonaktiebolaget L M Ericsson [2023 SCC OnLine Del 1845].
[64] Unwired Planet International Ltd v. Huawei Technologies Co. Ltd (SCUK 2020).
[65] Telefonaktiebolaget LM Ericsson (PUBL) v. Competition Commission of India & ANR., 2023 SCC OnLine Del 4078, decided on 13-07-2023.
[66] *Id*. at para 4, 7.
[67] *Id*.
[68] *See Intex Technologies (India) Ltd. V. Telefonaktiebolaget L M Ericsson [2023 SCC OnLine Del 1845]*.

Small inventors, including App Association members, rely on the FRAND construct to develop cutting-edge technology around the globe, which is defeated by the ability for some SEP holders to hold international technical standards hostage. We address this issue in detail in our piece, "A Call to Action: Guiding a Fair Standard-Essential Patent Licensing Process for a Thriving Indian Economy,"[69] a comprehensive paper recommending a pro-competitive standards and SEP framework for India that will protect and augment its Indian innovation as well as India's global leadership.

Issue: Digital Platform Regulation

The Indian government (most recently the Ministry of Corporate Affairs[70]) continues to propose competition-themed interventions into nascent and highly competitive digital markets, raising significant concerns for App Association members that pro-competitive dynamics in the Indian market will be distorted to benefit a few large developers. While the Indian government has since withdrawn the draft digital competition law in its current form and announced that it will first commission a comprehensive market study before introducing a fresh version of the legislation, there is a possibility this could be resurfaced. We urge USTR to track digital platform regulation in India and to include it in the next NTE report.

Issue: Proposed Regulation of Over-The-Top Services

India continues to explore proposed regulation of OTTs (e.g., its draft India Telecommunications bill and through TRAI consultations), including through licensing and extending universal service contribution mandates to OTTs. The App Association strongly objects to these proposals and continues to engage with India to avoid OTTs being treated the same as telecommunications services, save for OTT communications services that have the primary purpose of providing real-time person-to-person telecommunication voice services using the network infrastructure (e.g., utilizing a telephone number) of a TSP. Recent reports indicate that OTT's may be excluded from a TSP licensing regime. Consistent with the above, this development is of high concern to our community and we urge for its consideration in the investigation of harm from non-reciprocal trade agreements.

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

Currently, Indian internet providers must attain government approval from 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 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.[71] This

[69] *See* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4536835.

[70] https://www.mca.gov.in/bin/dms/getdocument?mds=gzGtvSkE3zIVhAuBe2pbow%253D%253D&type=open.

[71] 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.

is an ongoing issue of serious concern to small business innovators; therefore, we recommend it be considered in the investigation of harm from non-reciprocal trade agreements to ensure continued prioritization for the U.S. government and other stakeholders.

Issue: Sweeping Privacy Regulation in India

India's Personal Data Protection Bill includes rules for how personal data should be proposed and stored as well as lists the rights of people regarding their personal information. As the bill has evolved, the App Association believes that its provisions have improved much, though implementation of the law will be crucial in shaping App Association members' ability to operate and grow in this vital market. The App Association is participating in India's latest policy consultation to inform its development of a privacy law, and requests U.S. government support to ensure that its law and implementation do not serve as trade barriers.

Issue: Digital Services Tax

USTR has already launched an investigation of India's DST,[72] 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 investigation of harm from non-reciprocal trade agreements.

INDONESIA

Issue: Data Localization Requirements

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.[73] In October 2019, Indonesia passed Regulation No. 71 of 2019 which revoked Regulation No. 82 of 2012.[74] 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

---

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

[73] *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.

[74] *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.

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 relevant.

Issue: Intellectual Property Rights Enforcement

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.

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

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 remains very concerned at the unprecedented addition of digital goods to a tariff system and fears the precedent Indonesia may create.

We note that Ministry of Finance Regulation No. 190/PMK.04/2022 came into effect on January 13, 2023, introducing a new import declaration procedure for intangible goods. This regulation effectively establishes a customs administrative framework that allows Indonesia to begin collecting duties on intangible goods if it decides to raise the applicable duty rate from zero percent. This change could lead to significant compliance costs and administrative burdens for small businesses operating in Indonesia. Customs authorities have yet to determine the complete implementation of Regulation 190 and the application process for reporting customs data, with additional technical provisions still under development, despite the regulation currently being in effect.

We recognize Indonesia's recent commitment to remove its HTS code for digital goods, and urge for USTR to ensure this commitment is followed through on.

Issue: Digital Services Tax

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.[75] 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 U.S. government opposition to them.

Issue: Harmful Digital Platform Regulation

Indonesia's Ministry of Communication and Digital Affairs (Komdigi) continues to develop digital platform regulatory proposals, which the App Association continues to engage with them on. The App Association is concerned that Indonesia may enact EU DMA-like requirements that are barriers to digital trade.

ITALY

Issue: Digital Services Taxation

Italy currently imposes a 3% DST. For reasons discussed above, the App Association is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

JAPAN

Issue: Digital Platform Regulation

Japan has enacted a new law, the Act on Promotion of Competition Related to Specified Software Used on Smartphones (known as the SSCPA), which is currently in its initial implementation stages. The SSCPA effects ill-advised regulations for digital platforms that would unduly restrict the ability of platforms to curate apps and content, including with respect to enforcing IPR, as the law contains no exception for compliance for appropriate protection of IPR. Most recently, the Japan Fair Trade Commission has sought comment on the scoping of this law, which the App Association has provided written comments on.[76] The App Association has engaged extensively with relevant Japanese government actors for years, including the Ministry of Internal Affairs and Communications, the Headquarters for Digital Market Competition, and the Japan Fair Trade Commission to emphasize the need for protecting IPR on platforms, and has also raised concerns with the law's conflicts with obligations in both Article 16 of the General Agreement on Trade in Services and other trade agreement obligations. Because the SSCPA stands to inhibit some core

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

[76] *See* https://actonline.org/wp-content/uploads/App-Assn-Comment-re-JFTC-SSCPA-Scaling-RFI-EN.pdf.

platform functions, including those that will protect IPR in the digital economy, we urge USTR to track this development, recommend that be reflected in the USTR's investigation of harm from non-reciprocal trade agreements, unless altered, a means of denying adequate and effective protection of IPR (as the SSCPA contains no exception to compliance for protecting IPR), as well as a denial fair and equitable market access to U.S. small businesses who rely on IPR protections.

Much like the EU's DMA, Japan's regulatory approach risks undermining the very foundations of the mobile ecosystem—security, privacy, and consumer trust—that app developers rely upon and users expect. By restricting core marketplace management functions, such as app review and consumer-protection screening, the SSCPA weakens the value of COMs for SMEs while specifically targeting U.S. companies that provide these COMs. These changes distort competition between app stores and developers by limiting discoverability and driving up overhead for small businesses. Moreover, by prohibiting key features of the current marketplace framework, the SSCPA shifts costs downward, forcing smaller firms to absorb the compliance costs.

We acknowledge Japan's recent commitment not to regulate digital services in a discriminatory manner. We urge USTR to be vigilant in seeing this commitment being realized.

Issue: Artificial Intelligence Regulation

The App Assocation notes that the Japan Fair Trade Commission (JFTC) has launched an inquiry into the competitiveness of generative AI markets, raising the potential of Japanese government intervention into these nascent and rapidly-evolving segments of the economy. We have discouraged such interventions and urged Japan to study the impacts of the hasty intervention made into AI markets by the EU before moving forward. We urge USTR to oppose Japanese government regulation of AI markets at this time.

KENYA

Issue: Data Localization

The Data Protection Regulations of 2020 mandate the localization of a broad set of data, including national civil registration systems, population register and identity management, primary and secondary education, electronic payment systems, revenue administration, health data, and critical infrastructure. The Regulations require that at least a copy of the data falling under these categories be stored in a data center located in-country.

In addition, Kenya's 2025 National Cloud Policy requires sensitive categories of data to be hosted locally through local accredited providers or the government cloud. While framed as a measure to strengthen national infrastructure, the preference for local storage and local providers risks excluding or disadvantaging foreign suppliers, creating discriminatory barriers to market access that conflict with Kenya's trade commitments and undermine the competitiveness of U.S. cloud and digital service providers.

Issue: Intellectual Property Rights Protection

Recently, Kenya took steps to strengthen its IP enforcement by updating its copyright and trademark legislation. The App Association sees this as a positive step to deter IP infringement in Kenya.[77]

Issue: Digital Platform Competition

In May 2024, the Competition Authority of Kenya (CAK) issued a draft Competition (Amendment) Bill for public comment, in which the App Association participated, that would create a framework similar to the EU DMA, discussed above, in an attempt address concerns with large tech platforms. As with DMA, we believe such a move would create barriers to participation in the Kenyan digital economy and stifle innovation and growth.

MALAYSIA

Issue: Network Operation Fees

The Malaysian government intends to implement a Universal Service Provision (USP) Fund contribution for Cloud Service Providers (CSPs). This new requirement, slated to take effect in 2026, marks a significant departure from its previous policy and would affect the competitiveness of cloud services in Malaysia, impacting their availability and cost to small businesses.

Issue: Intellectual Property Rights Enforcement

Concerns persist regarding intellectual property matters, including the prevalence of pirated copyright and counterfeit trademark products, as well as the absence of suitable U.S.-style safe harbors to facilitate the efficient removal of infringing or problematic content.

Issue: Digital Platform Regulation

The Malaysia Competition Commission (MyCC) is actively engaged in advancing new regulation of digital platforms under the Competition Act 2010. Conducted from mid-2024 to late 2025, the review focuses on five strategic sectors: mobile operating and payment systems, e-commerce marketplaces, digital advertising services, online travel agencies, and data privacy as a cross-cutting issue. MyCC has released a draft final report outlining preliminary recommendations, which the App Association has advocated on extensively, emphasizing the impact of the small business technology innovator community. We continue to work with MyCC and Malaysian government to avoid the adoption of harmful *ex ante* EU DMA-like requirements being imposed on the ecosystem.

Issue: Artificial Intelligence Regulation

Malaysia's National AI Office (NAIO) has introduced a Sovereign AI Strategy featuring a tiered governance approach with strict requirements around compute infrastructure, data residency, and operational workflows, especially for sensitive government workloads. The strategy includes plans

[77] USTR, *2019 National Trade Estimate Report on Foreign Trade Barriers*, 312 (2019).

for government-owned cloud and compute capabilities for the highest tier (L3) workloads and introduces sovereignty certification requirements, even when collaborating with global companies. While NAIO expresses an "ecosystem-supportive" policy open to both foreign and local providers, the new mandates raise concerns about possible market entry barriers and favoritism toward domestic firms. The strict rules for managing sensitive government data, along with enhanced certification and audit standards, would increase compliance burdens and operational costs for small U.S. companies in Malaysia.

MEXICO

Issue: Intellectual Property Rights Enforcement

Intellectual property laws in Mexico have made significant improvements but lag behind the rest of the world on protection and enforcement. Mexico accession to the U.S.–Mexico–Canada Agreement (USMCA), the WIPO Internet Treaties (WIPO Copyright Treaty [WCT] and the WIPO Performances and Phonograms Treaty [WPPT]) has strengthened both their Federal Copyright Law and Federal Criminal Code. This significant progress was met with constitutional challenges that we were encouraged were rejected by the Mexican Supreme Court. While these reforms were upheld as constitutional, we now urge USTR to encourage the Government of Mexico to fully implement these them without further delay by issuing the corresponding implementing regulations by the Minister of Culture and the Copyright Office. If these laws are overturned, Mexico will be a jurisdiction for significant IP abuse. The App Association therefore encourages USTR to consider this issue in its investigation of harm from non-reciprocal trade agreements.

NIGERIA

Issue: Data Localization & Nigerian Workforce Requirements

The Nigerian government enacted "Guidelines for Nigerian Content Development in Information and Communications Technology,"[78] which raise a myriad of concerns for our members. The Nigerian government imposes data localization requirements on multinational companies. For instance, section 10.3 of the Nigerian government's guidelines mandates multinational companies to not only store their data in Nigeria but also requires such companies to incorporate 50 percent of local products when manufacturing ICT devices in the region. Additionally, it requires companies to hire local engineers when manufacturing such products.

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 this development in its investigation of harm from non-reciprocal trade agreements and to work with the Nigerian government to mitigate its damage and influence in the region.

[78] NITDA, *Guidelines for Nigerian Content Development in Information and Communications Technology* (2017).

Intellectual Property Rights Protection:

While Nigeria has taken steps towards improving its IP protections[79], Nigerian enforcement agencies lack the resources needed to effectively enforce IP rights.

PAKISTAN

Issue: Data Localization

The App Association notes that Pakistan has released a new draft of the "Personal Data Protection Bill." This updated version maintains the ban on the cross-border transfer of a vaguely defined category of "critical" personal data. The draft bill also proposes the establishment of a National Commission for Personal Data Protection, which would have broad authority to create new regulatory frameworks and access data.

Additionally, in 2022, Pakistan introduced a Cloud First Policy that imposes data localization requirements on various broad categories of data, including "restricted," "sensitive," and "secret." In the financial sector, the State Bank of Pakistan (SBP) prohibits financial institutions from storing and processing core workloads on offshore cloud services. These data localization requirements do not effectively enhance data protection while making it more difficult to enter the market and raising costs for App Association members.

PERU

Issue: Proposed OTT Regulation

Peru's Organismo Supervisor de la Inversion Privada en Telecommunicaciones (OSIPTEL) has initiated a consultation on the potential implications of the framework for regulating over-the-top (OTT) services and applications, posing the potential of network fees and other onerous requirements on innovative OTT services that App Association members offer. Consistent with our views above, the App Association has significant concerns with the potential of such a regime being imposed in Peru, and we have provided our detailed views to OSIPTEL. We are continuing to engage with the Peruvian government and believe this development should be included in the next NTE report.

PHILIPPINES

Issue: Data Localization Mandate

A new draft executive order in the Philippines proposes data residency and classification rules requiring certain data types to be stored in local infrastructure. Notably, it excludes U.S. cloud service providers from three of the four tiers of public sector data. Though not yet signed, the government aims to enact it soon, similar to a 2023 proposal that was shelved after stake holder

[79] *See* USTR, *2019 National Trade Estimate Report on Foreign Trade Barriers* (2019) ("In 2017, Nigeria submitted its instruments of accession and ratification of four World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty, the WIPO Performances and Phonograms Treaty, the Marrakesh Treaty, and the Beijing Treaty").

pushback. Legislative moves parallel this trend, including a last-minute addition to the Open Access in Data Transmission Act empowering the DICT to safeguard local data for national security and public interest. The App Association remains concerned with continued developments in this space, and urges for their attention in the NTE.

POLAND

Issue: Intellectual Property Rights Enforcement

Poland's treatment of enforcement against online piracy is concerning to App Association members, particularly due to the nation continuing not to implement significant provisions of EU directives, including Article 8(3) of the EU Copyright Directive (2001/29/EC) requiring Member States to ensure injunctive relief is available "against intermediaries whose services are used by a third party to infringe a copyright or related right."

REPUBLIC OF KOREA

Issue: Discriminatory Digital Platform Regulation Policies

The App Association remains deeply concerned about the Republic of Korea's escalating use of competition policy and proposed ex-ante regulation to target U.S. digital firms and distort healthy competition in the online platform economy, despite bipartisan opposition from U.S. policymakers including explicit warnings from President Trump.

Both the Korean National Assembly and the Korea Fair Trade Commission (KFTC) continue to pursue government interventions into the operation of U.S.-based digital platforms that, among other consequences, would undermine small businesses' access to competitive and secure app ecosystems. Specifically, the Korean National Assembly continues to pursue sweeping regulatory initiatives modeled on the EU's DMA, including the proposed Online Platform Monopoly Act (OPMA) and Fairness in Online Platform Brokerage Transactions Act ("Fairness Act").[80] These bills would "pre-designate" major U.S. platforms (e.g., Google, Apple, Meta, Coupang) through arbitrary market thresholds, compelling disclosure of proprietary algorithms and even source code, while exempting powerful domestic conglomerates and Chinese platforms. Coupled with the KFTC's planned "Platform Bureau,"[81] these efforts mark a sharp departure from Korea's evidence-based competition tradition and threaten to chill innovation, raise compliance costs for small developers, and reduce consumer choice. Alarmingly, these proposals focus on specific sectors and set arbitrary revenue and user-base thresholds to target successful U.S. companies while exempting most Korean conglomerates and all Chinese tech giants operating in the Korean market.

The "Fairness Act," in particular, problematically singles out online platform intermediaries for supposedly exercising a superior bargaining position over business users and using this position to implement unfair trade practices. By narrowing the scope to this single sector, it is tailor-made to disproportionately cover a substantial number of innovative U.S. companies, including Google,

[80] https://www.techpolicy.press/digital-regulation-is-no-longer-just-domestic-policy-as-korea-and-us-clash-over-new-law/

[81] https://n.news.naver.com/mnews/article/214/0001428922?sid=154

Apple, Coupang, Meta, Netflix, Uber, and potentially others, while ignoring other sectors where Korean conglomerates have a well-documented dominant position in the Korean economy.[82]

Though the legislation in theory captures a greater number of companies than the OPMA due to lower proposed financial thresholds, it would still, in practice, give Chinese competitors a free pass since the companies in scope (e.g., Temu, Shein, Alibaba) have a history of deceptive practices, including mispresenting business data and corporate revenues. Alibaba also has "self-regulatory" arrangements with the KFTC, which raises legitimate questions about whether they would be targeted to the same degree as the many American firms in scope.

Beyond specific legislation like the Fairness Act and OPMA, President Lee's newly appointed KFTC Chair nominee has promised to renew the push for online platform regulation following the conclusion of bilateral trade discussions with the U.S. As such, the App Association urges the U.S. government to ensure that Korea's competition and digital-platform policies are applied transparently and without discrimination, and to prioritize updates to Chapter 16 of KORUS or equivalent USMCA-style provisions to prohibit regulatory practices that unfairly target U.S. firms and stifle the global digital economy.

Issue: Competition Law Enforcement

The Korea Fair Trade Commission (KFTC) has increasingly relied on aggressive and unpredictable enforcement tools, such as dawn raids, threats of criminal prosecution for practices considered lawful elsewhere, and record-setting penalties, creating significant uncertainty for U.S. small technology firms. These measures, often lacking transparent due process or clear evidentiary bases, have produced unjustified investigations and constrained legitimate business operations.

Recent KFTC actions against U.S. firms over platform integration, network usage fees, and subscription-cancellation features exemplify a troubling trend toward enforcement that disadvantages foreign innovators while granting broad leeway to domestic and Chinese competitors. Such actions not only burden U.S. market entrants with disproportionate compliance costs but also risk contravening Korea's obligations under the KORUS FTA.

Notably, a new study by the Competere Foundation (October 2025)[83] finds that Korea's regulatory and antitrust policies targeting U.S. companies could cost the United States and Korea a combined $1 trillion in economic losses over the next decade ($525 billion in the U.S. alone). These findings underscore how Korea's KFTC and digital trade bills undermine U.S. innovation, exports, and small-business access to Asia, running directly counter to President Trump's agenda to eliminate non-tariff barriers, expand digital exports, and secure reciprocal market access for U.S. firms. Addressing these policies would strengthen U.S.–Korea supply-chain resilience and advance the administration's Indo-Pacific trade objectives.

U.S. industry concerns about KFTC's targeting American companies has been exacerbated by the appointment of Ju Byung-ki as KFTC Chairman in September 2025, who has articulated a worldview deeply critical of U.S. trade policy and capitalism[84]—describing U.S. trade leadership as

[82] https://www.nytimes.com/2023/12/18/business/chaebol-south-korea.html
[83] https://competere.co.uk/korea-study-landing-page/
[84] https://n.news.naver.com/mnews/article/047/0002484791?sid=101

exploitative and politically manipulative. His leadership of KFTC risks further converting the agency into an explicitly ideological body—where anti-U.S. sentiment informs investigations and targeted enforcement against U.S. companies.

The App Association therefore, encourages USTR to launch a review of KFTC enforcement under President Lee and Chairman Ju to identify discriminatory or politically motivated patterns. Moreover, USTR can leverage Section 301 and KORUS trade mechanisms to ensure that Korea's competition policy does not become an instrument of anti-U.S. economic nationalism.

Issue: Intellectual Property Rights Enforcement

Korea continues to propose ill-advised regulations for digital platforms that would unduly restrict the ability of platforms to curate apps and content, including with respect to enforcing IPR. Most recently, the ROK's legislature is considering amendments to its Monopoly Regulation and Fair Trade Act (MRFTA) which would inhibit the protection of IPR on platforms subject to Korean law. The App Association has engaged extensively with the ROK to emphasize the need for protecting IPR on platforms, and has also raised concerns with the law's conflicts with obligations in both Article 16 of the General Agreement on Trade in Services and the U.S.-Korea Free Trade Agreement in chapters addressing investment and electronic commerce.[85] Because ROK proposals for platform regulation would inhibit some core platform functions, including those that will protect IPR in the digital economy, we urge USTR to track this development, recommending that it be reflected in the USTR's its investigation of harm from non-reciprocal trade agreements, unless altered, 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.

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.[86] 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."[87]

In July 2016, a package of amendments was released imposing extensive data storage requirements on telecommunications providers and companies classified as internet

[85] *See* https://actonline.org/2025/01/24/act-the-app-associations-letter-to-the-republic-of-koreas-government-regarding-online-platform-regulation-legislation/.
[86] Russian Federation, *Federal Law No. 242-FZ*, (July 21, 2014), *available at* https://pd.rkn.gov.ru/authority/p146/p191/.
[87] 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/.

telecommunications services.[88] 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."[89]

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.[90] By raising the penalties for not abiding by this 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.[91]

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

---

[88] 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/.

[89] 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.

[90] 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/.

[91] "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.

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.

SOUTH AFRICA

Issue: Data Localization

South Africa's Data and Cloud Computing Policy, released in May 2024 by the Department of Communications and Digital Technologies (DCDT), includes provisions for data sovereignty. The policy specifies that "data related to the protection and preservation of national security and sovereignty of the Republic shall be stored exclusively in digital infrastructure within the country's borders." However, the extent of the data covered under this provision is still uncertain, presenting challenges to App Association members.

Issue: Digital Platform Regulation

In 2021, the Competition Commission of South Africa (CCSA) launched an online intermediary platforms market inquiry.[92] The App Association has provided detailed views on digital platforms and competition, as well as reactions and feedback on CCSA's specific proposals.[93] The App Association has significant concerns with the the South African government's interjecting itself into the digital economy, jeopardizing 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 next 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.

Issue: IP Rights Protection

IP laws in South Africa do not adequately address protection and enforcement of inventive and creative works in the digital age. Due to insufficient IP protections, inventive technologies and creative works are easily accessed and impact overall innovation and creation in Sub-Saharan Africa. The App Association shares concerns with proposed changes to South Africa's copyright framework, though such changes have not advanced to become final policy.

[92] https://www.compcom.co.za/online-intermediation-platforms-market-inquiry/.
[93] E.g., https://www.compcom.co.za/wp-content/uploads/2021/07/App-Association-Comments-on-OIPMI-Statement-of-Issues-18-Jun-2021.pdf.

We further urge USTR to consider the Competition Commission of South Africa's (CCSA) market inquiry into online intermediation platforms as a potential 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. CCSA mandates for digital platform operations must preserve the ability for those platforms to provide IPR-related curations that countless developers operating in South Africa rely on.

SPAIN

Issue: Digital Services Taxation

Italy currently imposes a 3% DST. For reasons discussed above, the App Association is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

THAILAND

Issue: Digital Platform Regulation

Thailand's Electronic Transactions Development Agency (EDTA) has initiated a policy development process for digital platform regulation.[94] The App Association has engaged with EDTA and others in the Thai government to emphasize the need for protecting IPR on platforms.[95] While this legislative proposal was withdrawn, we understand that further efforts to develop new digital platform regulations in Thailand are underway, including the development of new "guidance" by EDTA. Because regulatory interventions into digital platforms markets by the EDTA stand to inhibit some core platform functions, including those that will protect IPR in the digital economy, we urge USTR to oppose onerous platform regulation in Thailand.

TURKEY

Issue: Digital Service Taxes

Turkey has implemented a 7.5% DST which applies to companies that have worldwide revenues of €750 million and local revenues of 20 million Turkish Lira. For reasons discussed above, the App Association is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

Issue: Digital Platform Regulation

The Law of the Protection of Competition, No. 4054, in Turkey was amended to include a new online platforms regulatory framework that aligns with concepts outlined in the EU's DMA. The regulation, however, imposes additional requires for designated companies intended to enable the interoperability of core platforms services and/or ancillary services, but stands to inhibit the ability of curated online marketplaces to enforce IPRs, which, as explained above, is a vital function small businesses in the digital economy rely upon. Because regulatory interventions into digital platforms

[94] *See* https://www.trade.gov/market-intelligence/thailand-information-technology-digital-platforms.
[95] *See* https://actonline.org/wp-content/uploads/ACT-Positions-on-Digital-Platforms-and-Competition-for-Thailand-EDTA-EN.pdf.

markets by Turkey stand to inhibit some core platform functions, including those that will protect IPR in the digital economy, we urge USTR to assist in opposing digital platform regulation in Turkey.

Issue: Data Localization

Turkey's E-Payment Law requires the processing of e-payments occur within Turkey.[96] In mid-2016, Turkey's Banking Regulation and Supervising Industry (BDDK) initiated a policy that mandates companies locate their ICT systems in the country.[97] 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."[98] These data localization requirements have largely chilled our members' plans to enter this important market should their app include e-payment capabilities.

Issue: Social Media Law

Turkey amended the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts (Law No. 5651), with these amendments coming into force October 1, 2020. These amendments are collectively known as the Social Media Law, and affect all businesses considered social network providers.[99] The law's broad definition of social network providers – which includes any business allowing users to create, view, or share text or media for social interaction – may include many App Association members not traditionally considered social network providers, placing a heavy burden on the business and discouraging expansion into the Turkish market.

UNITED ARAB EMIRATES

Issue: Data Localization

The UAE requires CSPs serving the public sector and specific regulated industries to be exclusively governed by UAE law, exempt from foreign jurisdiction and laws, and to physically localize data centers along with engineering, security, maintenance, and support operations and personnel. For reasons discussed above, the App Association community is concerned with such requirements and requests USTR support in opposing them.

---

[96] 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.

[97] 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.

[98] 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/.*

[99] Begüm Yavuzdogan Okumus & Direnç Bada, *Turkish data localization rules in effect for social media companies*, IAPP, Oct. 20, 2020, *available at* https://iapp.org/news/a/turkish-data-localization-rules-in-effect-for-social-media-companies/.

UNITED KINGDOM

Issue: Digital Platform Regulation

The Digital Markets, Competition and Consumers Act (DMCCA), effective January 2025, establishes a new regulatory framework empowering the UK Competition and Markets Authority (CMA) to oversee digital markets by designating firms with "Strategic Market Status" (SMS) based on their market dominance and revenue thresholds. The Act shifts the CMA's role from traditional post-investigation enforcement to proactive, ongoing oversight, allowing it to impose forward-looking conduct obligations. Similar to its concerns noted above regarding the EU DMA, we believe the DMCCA represents a significant barrier to digital trade.

Issue: Prohibitions on the Use of Strong Encryption

Media reports suggest that the UK government has issued a technical capability notice (TCN) under Section 253 of the Investigatory Powers Act 2016 compelling Apple to introduce a backdoor into its end-to-end encrypted cloud services. This would embed a systemic security vulnerability into one of the world's largest mobile device providers, endangering the security and privacy of all its users—not just in the UK, but worldwide. Additional reporting indicates that Apple has now discontinued its Advanced Data Protection feature in the UK, an optional service that offers end-to-end encryption for iCloud backups, file storage, and certain other apps.

The App Association's small business members know that, in order to compete across consumer and enterprise markets, they must be able to reliably restrict data access to authorized users, ensure data remains accurate and unmodified, and guarantee information is available when needed by authorized users. End-to-end encryption is a primary tool for providing the trust and security of their customers. Attempts by governments—most recently the UK—to mandate backdoors to encryption algorithms significantly undermines these goals.

The App Association understands and appreciates the need for policymakers to protect public safety across new and emerging digital modalities. However, the TCN issued by the UK government to Apple does not accomplish this goal. Its implementation will deeply damage security and trust across the digital economy by creating flaws in algorithms that can be used to compromise data confidentiality, integrity, and access requisites.

It is impossible to reserve security backdoors for just the "good guys." If a door exists then bad actors can, and will, exploit it. It is fair to assume that other tech firms will be asked to create similar backdoors into encrypted services, further damaging security and trust. The UK's demand also sets a precedent for other countries and regimes to demand similar access to encrypted private data, further reducing citizens' privacy and safety.

The damage that would be caused by the implementation of the UK government's TCN to American small businesses innovating and competing across the global digital economy is not hypothetical. As a prime example, government mandates in the 1990s for broadband internet providers to enable law enforcement agencies access to encrypted communications on their networks has directly led recently to the China-backed hacker group Salt Typhoon gaining unprecedented unauthorized access to swaths of sensitive data. While the magnitude of this breach of U.S. telecommunications carrier networks continues to be investigated, at this time, it appears that Salt Typhoon's access

was essentially unlimited. This (ongoing) episode is the strongest evidence that mandating unfettered access via backdoors to encrypted devices or data in transit will result in that access being exploited by unintended actors. The Salt Typhoon experience demonstrates that weakening encryption will expose businesses to more frequent breaches, creating an even greater risk for those already marginalized.

The UK government's issuance of the reported TCN also stands in stark contrast the U.S. government's efforts to encourage the use of encryption for securing critical infrastructure, businesses, and personal data; promote best practices for encryption in cybersecurity; and for the U.S. government itself to use encryption to protect classified information and communications. With cyber attacks to critical infrastructure continuing to increase in both frequency and severity, the need for security that end-to-end encryption provides has never been more essential. A mandated weakening of encryption will undermine the

In a separate letter,[100] we have explained to the UK Home Office that in compelling a company to covertly compromise the security of its product, the UK undermines its own stated goal of "protect[ing] and promot[ing] its interests as a sovereign nation in a world fundamentally shaped by technology"[101] and raises serious concerns about the security of products from UK firms, leading to investors and consumers questioning whether their products contain hidden security vulnerabilities mandated by the UK government. The precedent the TCN implementation will create may force some of our members to consider withdrawing from the UK market to avoid the reputational risks associated with undermining their own product's security, representing the closing off of a key market to countless U.S. small business innovators. Any government that mandates, or attempts to mandate, backdoors to encryption damages their own standing in global security and innovation policy.

The UK Home Office has since abandoned its original TCN, and issued a new TCN limited to the UK. We note that the App Association's concerns above remain, despite this second attempt.

We strongly support efforts to combat governments' attempts to undermine encryption damage and distort security and competitiveness foundations that our small business innovator community relies on. The U.S. has the power to protect encryption standards, ensuring they remain strong enough to safeguard our digital infrastructure without creating loopholes that compromise security. We request USTR leadership in pushing back against the UK Home Office's reported TCN, and for USTR partnership in engaging the UK government (and other governments around the world) in a new policy dialogue to ensure that end-to-end encryption supports U.S. national and economic security. Our community fully commits to participating in such a process, and to more broadly support policies that enhance security and innovation as well as U.S.' global leadership.

Issue: Digital Services Taxation

The UK levies a 2% Digital Services Tax (DST) on companies that have worldwide revenues of £500 million and local revenues of £25 million. For reasons discussed above, the App Association is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

[100] https://actonline.org/wp-content/uploads/ACT-Ltr-re-UK-Encryption-TCN-24-Feb-2025.pdf.
[101] https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

Issue: Intellectual Property Rights and Standards

In the case *Unwired Planet v. Huawei*,[102] the United Kingdom Supreme Court 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 continues to present 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 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 USTR's investigation of harm from non-reciprocal trade agreements within the ongoing U.S.-UK Free Trade Agreement negotiation, and through other avenues.

In recent years, the UK courts have experienced many developments in their SEP landscape. The ongoing dispute between InterDigital and Lenovo has shed light on significant anticompetitive SEP licensing practices, where InterDigital licensed their SEPs to small entities at a supra-FRAND rate and applied volume discounts for larger entities. Since then, the dispute was appealed by Lenovo to the UK Supreme Court, challenging the Court of Appeal's decision that limitation periods do not apply in FRAND cases. The App Association submitted an amicus brief in support of this case being heard. Although the parties ultimately settled, leaving the Court of Appeal's decision as established law for now, this case remains an important reference point in UK SEP jurisprudence. This case sets harmful precedent to remove a statute of limitations period of FRAND cases.

The UK Court of Appeal also heard the dispute in *Panasonic v. Xiaomi*, where Xiaomi successfully appealed the High Court's decision not to grant an interim license to Panasonic's SEP portfolio. The Court of Appeal's judgment is noteworthy not just for its impact on the licensing dispute, but because it strongly criticized Panasonic's conduct in seeking injunctions in Germany and the UPC. The Court found that such actions were out of compliance with the ETSI IPR Policy, making this case an important reference in the ongoing debate over SEP injunctions. This decision is contrasted by *Ericsson v. Lenovo* and *Amazon v. Nokia*, where the UK High Court denied an interim license in both cases. This trend of court decisions shows a new practice by UK courts, which is likely to continue developing for SEP disputes.

The Court has also made a judgement in the SEP dispute between Tesla and patent pool Avanci, denying the ability of Tesla, as the licensee, to request the court to set a rate on a SEP holder's FRAND-encumbered license. Unfortunately, this decisions appears to support Avanci's position

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

that it does not have any liability under the FRAND commitment attached to the SEPs it licenses despite the fact that its members have voluntarily committed to licensing their SEPs on FRAND terms. The App Association, along with academic Michael Carrier, detail important admissions from Avanci that pose serious anticompetitive concerns in the piece "Avanci's Admissions Cast Doubt on Pool's Procompetitive Effects."[103]

The UK Intellectual Property Office (UK IPO) separately released their report on SEPs, which includes important objectives, including addressing SME concerns within the SEP licensing landscape. What this report expressly does not include in an inquiry into injunctions as they relate to SEPs. We find this concerning since injunctions are often improperly used in this context and have a direct impact on UK SMEs. The House of Lords has discussed their concern about the IPO's decision.

In addition, the UK's Competition and Markets Authority (CMA) continues to take steps towards competition-themed mandates for digital platforms that would inhibit some core platform functions, including those that will protect IPR in the digital economy. We therefore urge USTR to track this development, recommend that it be reflected in the the USTR's investigation of harm from non-reciprocal trade agreements as a potential means of denying adequate and effective protection of IPR, as well as a denial of fair and equitable market access to U.S. small businesses who rely on IPR protections.

Given the impact of the above-described developments in the UK, we strongly recommend that USTR's investigation of harm from non-reciprocal trade agreements accurately capture and characterize the above concern.

VIETNAM

Issue: Digital Platform Regulation

In June 2025, Vietnam adopted the Law on Digital Technology Industry (DTI Law) that goes into effect in January 2026.[104] The law, while designed to set up new legal frameworks governing new technology industries like cryptocurrencies, in-app credits, or digital goods, also aims to rein in companies benefiting from Vietnamese users. This acts similarly to the DMA as a digital tax on U.S. innovation. The USTR must remain concerned on how these obligations may disproportionately burden small U.S.-based app developers and digital-services firms operating in Vietnam (or planning to enter) by imposing new oversight, compliance, registration and reporting requirements on larger players.

More recently, Vietnam's proposed new digital platform law, the Draft Law on Digital Transformation, has been introduced. The law, much like the EU's DMA, places significant restrictions on digital platforms, introduces extensive obligations, and would impose other onerous restrictions. The law also designates certain platforms as dominant based on user base thresholds and imposes restrictions similar to the EU Digital Services Act. These measures would, if put into

[103] *See* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4945572.
[104] https://www.lexology.com/library/detail.aspx?g=13cca09d-b7b2-42f6-aee3-227fc93562b4&utm

place, represent substantial digital trade barriers that would limit operational flexibility and raising barriers to market entry for App Association members.

Issue: Artificial Intelligence Regulation

Vietnam's new proposed AI legislation also functions as a trade barrier. It would mandate strict regulation of AI development and deployment, including requirements for AI systems to disclose involvement in content creation and prohibitions on AI use for fraudulent purposes or to spread misinformation. This legislation would impose burdensome compliance and certification processes, especially for small technology firms wishing to operate in Vietnam. These broad, vague provisions threaten to restrict the participation of small AI providers through restrictive standards and transparency requirements, thereby limiting cross-border AI trade and innovation.

Issue: National Cybersecurity Law

Vietnam's broadly scoped National Cybersecurity Law applies 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. [105]

***

[105] 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/.

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 Global Policy Counsel

Chapin Gregor
Policy Counsel

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