March 7, 2023

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

RE: Responses to Written Questions from the Special 301 Subcommittee of the Trade Policy Staff Committee (USTR-2022-0016)

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

The App Association is a global policy trade association for the small business technology developer community. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. App developers like our members also play a critical role in developing entertainment products such as streaming video platforms, video games, and other content portals that rely on intellectual property protections. The value of the ecosystem the App Association represents—which we call the app ecosystem—is approximately $1.7 trillion and is responsible for 5.9 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[2]

In response to written questions received from the Special 301 Subcommittee of the Trade Policy Staff Committee, the App Association provides the following:

1. **Regarding India and the World Intellectual Property Organization (WIPO) Internet Treaties, please elaborate further on the specific aspects that India has not implemented and your concerns about those aspects.**

India's accession to the WIPO Internet Treaties and the Nice Agreement are commendable steps. However, the legislature has not yet amended the Copyright Act in the way that aligns India's legislation with these international best practices. Small businesses that rely on copyright protections require India to update and modernize its copyright framework to better align with its international obligations and to create a pro-innovation environment.

[1] 87 Fed. Reg. 76660.

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

For example, the government of India's existing provisions and remedies on technological protection measures (TPMs) fall short of treaty requirements. Currently, the Copyright Act and the Criminal Procedure Codes of India do not appropriately define TPMs; ensure sanctions apply to both acts of circumvention and trafficking in devices, software, components, and services that circumvent; or provide civil and criminal penalties.

TPMs like encryption are necessary to bolster trust with consumers and enterprise customers. Small business software and internet of things (IoT) device developers experience significant loss of revenue and threats to the ability to innovate, invest, and hire each year from piracy. To combat piracy, small business developers utilize a variety of TPMs such as digital rights management (DRM) tools and encryption. Including DRM in an app ensures that only users who purchased the app can install it on the authorized device. Encryption is widely used to embed digital content in apps to make it harder for the software code to be extracted. Moreover, App Association members rely on TPMs to protect their intellectual property. If consumers or bad actors can exploit workarounds to access content for which small business developers intend to charge, such a market for those workarounds would upend the business model. Such a market would also force developers to take more expensive and structurally less permissive measures to protect their content—further driving up prices for mobile software and related services.

2. **With respect to China's use of the "essential facilities" doctrine, as noted in your submission, have there been any new developments in the application of this doctrine? Are you aware of specific instances of this application outside of the *Hitachi Metals* case?**

The App Association is not aware of any new instances where the "essential facilities" doctrine has been applied outside the *Ningbo Ketian Magnet Co., Ltd. v. Hitachi Metals*[3] case. However, we do stress the important implications of its application. The App Association does not support the notion that competitors should have access to "essential" patents outside of the standardization context, as we discuss in our comments. Such a provision undermines the exclusive rights of patent holders that engage with the Chinese economy, including U.S. innovators. This is amplified by the fact that the State Administration for Industry and Commerce (SAIC) uses a significantly subjective evaluation of necessary factors in order to determine if a compulsory license should be issued. Patents that are not essential to a technical standard should not be regulated in the same way as standard-essential patents (SEPs) because they do not produce the same lock-in effect to future innovators who develop products on a technical standard. China's attempt to control the IPR and business operations of companies in the Chinese economy severely impedes U.S. innovators and their engagement with the global economy.

We also point out that another implication of the *Hitachi Metals* case is that it enabled China's use of informal forced technology transfer (FTT) practices as part of their governmental regime. FTT practices require foreign entities to transfer technology as a condition of market access or investment.[4] Since China often denies their FTT practice[5] and claims that foreign entities

[3] *Ningbo Ketian Magnet Co., Ltd. v. Hitachi Metals* (Sept. 7, 2021).
[4] Jyh-an Lee, Forced Technology Transfer In The Case Of China (Aug. 22, 2020), pg. 328, https://www.bu.edu/jostl/files/2020/08/3-Lee.pdf.
[5] *See Id*. at 327 ("Such indications are supported by surveys conducted by the U.S.–China Business Council, the American Chamber of Commerce in China, the American Chamber of Commerce in Shanghai, and the European Chamber of Commerce in China.").

voluntarily transfer their technology, the purpose of these practices remains unclear.[6] It is well-defined that the transfer of source code is, in part, justified by the intent to prevent cybersecurity threats.[7] The App Association believes that this practice is likely a violation of China's World Trade Organization (WTO) commitment regarding the technology transfer accession protocol.[8] Further, the lack of formal law or rules in China for its FTT policy creates a difficulty in determining what specific entities require disclosures for any one industry;[9] though joint venture requirements are used to mandate partnership with Chinese companies that can then access and own a percentage[10] of proprietary information from foreign companies seeking access to China's market.

Through Chinese administrative approval procedures, foreign investors can be compelled to share trade secrets and other proprietary information on their technology with government entities to different sectors of the Chinese government based on type of investments, type of products or services, and national security reviews.[11] Per China's 2022 Negative List, information transmission, software, and information technology services are restricted markets that must gain administrative approval for market access. Included in this category are "Application and Internet of Things (IoT)" software. Even with source code disclosure requirements removed from China's previous draft cybersecurity laws, data localization and technology "backdoor" encryption requirements provide loose and vague language that often implies the disclosure of source code.

3. You cite India's Intellectual Property (IP) Appellate Board as a sign of progress. What is your reaction to the closure of the IP Appellate Board and the creation of an IP Division of the Delhi High Court?

The App Association is discouraged by the decision of the IP Division of the Delhi High Court to replace the IP Appellate Board (IPAB) but remains hopeful that an appropriate appellate mechanism will be put into place. The IPAB was initially created pursuant to article 41 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement to provide for a judicial system to enforce IP rights separate from law enforcement. The creation of such a tribunal was also established to alleviate other adjudicating bodies from handling IP-intensive cases from the Indian Patent Office (IPO) and the Trade Marks Registry (TMR) that could be thoroughly reviewed by technical and judicial experts within the IPAB. The IP Division of the Delhi High Court seems to be an effective replacement for the IPAB, but we continue to gather experiences and data to make a more comprehensive assessment.

The IPAB provided for an individual tribunal with jurisdiction independent of general courts and was successful despite challenges to fully staff the tribunal. Significantly, out of 3,793 cases disposed by the IPAB, only about 3 percent were appealed, and less than 1 percent was

---

[6] *Id*.
[7] Michael Brown and Pavneet Singh, China's Technology Transfer Strategy (January 2018), p. 18 n. 62., https://nationalsecurity.gmu.edu/wp-content/uploads/2020/02/DIUX-China-Tech-Transfer-Study-Selected-Readings.pdf.
[8] Jyh-an Lee, note 1 at 345-6.
[9] Jyh-an Lee, note 1 at 329.
[10] Nathan Bush, Framing patents as essential facilities in Chinese antitrust: *Ningbo Ketian Magnet Co., Ltd. v. Hitachi Metals* (Sept. 7, 2021), https://www.dlapiper.com/fr/france/insights/publications/2021/09/antitrust-matters-september-2021/framing-patents-as-essential-facilities-in-chinese-antitrust/.
[11] Jyh-an Lee, note 1 at 333.

reversed on such appeals.[12] In addition, most judgements of the IPAB were upheld by the Supreme Court of India.[13] While the IPAB may have needed reform, its individual jurisdiction on IP disputes provided the Indian economy with a strengthened position in intellectual property enforcement and protection.

4. **You say India is decriminalizing minor offenses under the Patent Act and the Copyright Act, citing an article from 2020. Please provide more information, including how this action affected your members.**

Because India remains one of the world's most challenging major economies with respect to protection and enforcement of IPR, the decriminalizing of minor offense under IP law invites IP abuse from national and foreign entities and disables good faith innovation by small businesses, including App Association members. While such legislation has not yet passed and become law in India, they remain proposals that are being considered by the legislature. The Indian government's willingness to adequately protect IPR has presented small and medium-sized tech and software development businesses with an immense opportunity for innovation in the Indian economy. Specifically, the Cell for IPR Promotion and Management (CIPAM) and Federation of Indian Chambers of Commerce & Industry (FICCI) development of an IPR Enforcement Toolkit for Police, as stated in our broader comments to the Special 301 review. Despite this positive move forward, App Association members continue to experience IPR infringement (copyright, patent, trademark, and trade secret), and India's progress in protection and enforcement is lacking, reducing incentives for small business innovators to enter the market and compete.

The ability for foreign entities to steal IP unscathed is disproportionately harmful to small U.S. innovators that engage with the Indian economy. Further, this system poses external risk to the U.S. IP system. The Indian economy presents numerous hurdles to market access, either in place today or proposed, that 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. Therefore, App Association members must be provided strong IP enforcement regulations by the Indian government that criminalize all IP-related offenses in order to rely on the Indian innovation ecosystem.

5. **Your submission cites the Australian government interjecting itself into the digital economy as the grounds for Australia to be listed on USTR's Priority Watch List. Please explain how the Australian government's actions raises specific concerns with respect to IP protection, enforcement, or market access for U.S. persons relying on IP.**

The App Association has significant concerns with proposals developed by the Australian Competition and Consumer Commission (ACCC) which would undercut the ability of platforms to address IP infringement (and other cybersecurity and privacy issues). The proposals are currently being consulted on by the Australian Treasury. The App Association has engaged, and continues to engage, in this policy development process. However, Australian policymakers continue to indicate their willingness to advance mandates that would inhibit software platforms' ability to address IP infringement, meriting inclusion on the Priority Watch List.

[12] *See* https://updates.anandandanand.com/abolishing-ipab-an-own-goal/.
[13] *Id*.

As background, before platforms, software developers struggled to safeguard their IP against piracy and theft. Software companies faced serious challenges in protecting their products in retail stores because the licensing codes remained active and easy to steal. Once developers overcame the significant barriers to bring their products to market, they were faced with the threat of piracy and theft which limited their volume of business and hurt their bottom line.

Before software developers could leverage dispute resolution mechanisms provided by platforms, developers were left with the significant burden of IP infringement litigation in court, which could leave the legitimate IP owner with several thousand dollars per month in legal fees and months or years diverted from company matters. When the infringement originated abroad, software developers were at the mercy of foreign judicial systems, some even lacking rule of law and impartiality. Software developers and copyright holders continue to benefit from platforms' cost-effective avenues, such as their dispute resolution mechanisms referenced above, to distribute and protect the integrity of their products.

Today, IP dispute resolution mechanisms on platforms are key means of differentiation and competition (for platforms), and critical features relied on by countless small business developers in the digital economy. Australian proposals, including those that would mandate sideloading on software distribution platforms, would undercut the ability of platforms to protect IP, an aspect that countless small businesses rely on to grow and create jobs. The Australian government's proposed approaches to competition-themed policy changes for digital platforms stand poised to undercut the ability of platforms to provide this vital function.

6. **Your submission cites Korea's Telecommunications Business Act and a concern about "appropriate and timely removal of fraudsters and copyright thieves, and rigorous vetting of any new software." Please clarify the relationship between the two.**

Rigorous vetting of software applications is a vital means of preventing and addressing frausters and copyright thieves. The vetting and dispute resolution processes employed by leading platforms are essential components that protect software developers from malicious software that seeks to cause consumer confusion through trademark infringement. For example, 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. Small business software developers cannot risk delayed or slow removals of fraudsters from a platform because such abuse its costly. Consumers, too, rely on a platform's rigorous vetting process in order to trust and ultimately download an app. This process is especially important for small businesses that can authenticate their app to a consumer when they have not gained public name recognition. App Association members that develop mobile apps and provide those apps on software distribution platforms already go through a rigorous vetting and review process before their app is ever widely available for download for consumers. Therefore, these businesses rely on digital platforms and regulations around these platforms in order to protect their intellectual property, ensure platform-level privacy and security measures, and gain consumer trust. As we state in our comments, the Telecommunications Business Act (TBA) stands to benefit a small number of global brands while also freezing out U.S. small business app developers operating in the Republic of Korea and around the world that can't pivot so quickly.

The App Association appreciates the opportunity to provide responses to the TPSC's follow up questions and welcomes the opportunity to assist further moving forward.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Policy Associate

Priya Nair
Intellectual Property Policy Counsel

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