March 4, 2024

Written Follow-up to Questions Posed during February 21, 2024, Testimony

Public Hearing Regarding the 2024 Special 301 Review (Docket Number USTR-2023-0014)

Brian Scarpelli
Senior Global Policy Counsel
ACT | The App Association

Thank you for this opportunity to testify before the Office of the United States Trade Representative (USTR) on February 4, 2024. ACT | The App Association is pleased to contribute further views as the USTR on its Special 301 review 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 intellectual property protection.

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 economy—is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.

In response to various questions posed to me during my testimony:

Mexico: During my testimony, I was asked to provide insights into challenges to Mexico's implementation of the WIPO Internet Treaties (WIPO Copyright Treaty [WCT] and the WIPO Performances and Phonograms Treaty [WPPT]) and what provisions of the Mexican Constitution are being invoked in these challenges. We are aware of three constitutional challenges against provisions of Mexico's Copyright Act reform (2020) that seek to remove provisions addressing technical protection measure (TPM) protections and notice and stay down procedures. The National Commission of Human Rights challenged both provisions, while a group of 30 members of the Mexican senate, across different parties, challenged current notice and stay down procedures. The Mexican Supreme Court is reviewing a third constitutional challenge to notice and stay down provisions of the Federal Copyright Act from SLS Rule of Law Impact Lab and Article 19-Mexico. These challenges argue that the 2020 amendments to the Federal Copyright Act violate free expression provisions, such as those outlined in Article 13 of the American Convention on Human Rights and Article 19 of the International Covenant on Civil and Political Rights.

As noted in the App Association's initial comments to USTR's 2024 Special 301 Review, amendments to the Federal Copyright Law are a direct result of Mexico's accession to the U.S.–Mexico–Canada Agreement (USMCA) and the WIPO Internet Treaties. This change has significantly improved intellectual property laws in Mexico that have historically fell behind the rest

of the world. Similar to the provisions in the United States' Digital Millennium Copyright Act (DMCA), protections for TPMs and notice and take-down procedures provide necessary security for copyright holders that align with public interest and constitutional rights to free expression.

Similar to the Digital Millennium Copyright Act's notice and take-down procedures, Mexico's notice and stay down approach to intellectual property (IP) enforcement is an effective step to ensure that internet services providers (ISPs) take reasonable steps to prevent piracy on their platforms. This process prevents infringers from engaging in illicit acts. Notice and stay down procedures strengthen copyright protection and enforcement while preventing ISPs to benefit from otherwise undetected but potentially infringing digital works.

For small businesses, like App Association members, mandates to allow open access to otherwise protected software involves legalizing a "market for exceptions" that can lead to increased cyberattacks. This type of security risk is especially prominent when the software in question deals with encryption or other vital security tools, including TPMs. Prohibitions against circumventing TPMs and exemptions have proven to be effective and flexible tools that enable continued innovation in the tech sector and promote consumer choice in other jurisdictions.

TPMs protect layers of licensed software in devices. Licensed software is part of most products with digital content embedded in them. The system of licensed software is a crucial component to the investment and distribution in existing products and future innovations. The benefits to consumers across a wide variety of products and services at every price point cannot be overstated. Exemptions that allow the offering of third-party assistance or tools to circumvent TPMs protecting embedded device software compromise the protections afforded to other licensed software, putting consumers and their personal information at risk when products malfunction. It also allows software competitors access to product codes, which is a disincentive to innovation. Fortunately, there are alternative options to address many of the concerns expressed regarding access to software. Notices to consumers about restrictions and allowable uses along with offering certified third-party repair services can protect consumers and software developers. App Association members and those of other content and tech industries rely on licensed software to continue to offer low-cost, consumer-friendly products across a growing range of business models.

Innovative app developers rely on firmware TPMs like authentication and encryption to allow legitimate uses of works and mitigate serious threats to user privacy. The use of digital rights management (DRM) or TPMs is not only critical to protection against unauthorized access to a copyrighted work but also against attempts to steal personal information. In fact, digital products and services developed for every industry must comply with federal, state, and international privacy laws to protect consumer privacy. By law, the vast amount of personal information accessed through mobile apps on smart devices and appliances must be protected. The use of TPMs is necessary to maintain the integrity of software, protect end-user data collected by consumer products with embedded software from nefarious actors, and uphold the obligation to protect consumers' privacy rights. Therefore, the Mexican government should reject weak constitutional challenges to the Federal Copyright Act.

India: During my testimony, I was asked to elaborate on India's lack of compliance with the WIPO Internet Treaties. While India acceded to the WIPO Internet Treaties in 2018, the country has yet to adapt key provisions to the Copyright Act of 1957, amended in 2012 (the "Act"), and the Copyright Rules (2013). The Act does not provide for a legal mechanism for ISPs to

approach and remove infringing works from their platforms. The Act should devise a mechanism similar to successful jurisdictional approaches, such as those outlined in the United States DMCA and European Union Copyright Directive (EUCD). In parallel with this requirement, Section 52(1)(c) should require ISPs to act expeditiously to remove or disable access to the copyright infringing work or performance in the event that (i) the copyright holder notice of alleged infringement and requests that the ISP removes or disables such infringement; (ii) the work or performance has been previously removed or access was disabled from the ISPs site; and (iii) the copyright holder, in a complaint to a court, provides that the infringing work or performance has been previously removed or access was disabled from the ISP's site. In order for ISPs to better comply with these requirements, Copyright Rule 75(3), (Chapter XIV) should modify the 36-hour period for intermediaries to take down infringing content to align with more practical procedures outlined in the DMCA.

The Act does not fully comply with Article 11 of the WCT (and parallel language in Article 18 of the WPPT) requiring "adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." Section 1201 of the DMCA provides an effective mechanism to prevent the circumvention of technological measures used to shield unauthorized uses of a copyrighted work. The Act should consider Section 1201 as a model for implementing these requirements under the WIPO Internet Treaties. The Act should ensure that critical phrases are narrowly defined, including "effective technological measure," which should cover commonly-implemented DRMs and TPMs and other access and copy controls. Similarly, the provision should provide prohibitions for the manufacturing, importing, trafficking, and dealing in circumvention devices and software, or making and offering devices for such circumvention. Acts of circumvention under this provision should be subject to civil and criminal penalties.

The Act provides for broad exceptions to prohibiting the circumvention of effective technological measures that would render the provision ineffective. The DMCA permanent exemptions to Section 1201 provide a sounder approach that balances copyright protection with public needs. The DMCA exempts security testing, encryption research, and reverse engineering activities from the prohibition on circumvention within certain parameters. These activities are important and necessary parts of developing software products and services that entertain and meet the needs of consumers. For example, there is a considerable record of published results from security testing on automotive security, medical devices, voting systems, and consumer devices. Likewise, reverse engineering allows developers to create new interoperable and competing products and services. And encryption research is critical to improving technology to protect most internet traffic—everything from commercial transactions to social interactions. Our members like to say, "Just tell us the rules so we can build our business." The exemptions in the DMCA provide clear guidelines for app developers as they create and bring their products to market. This is why the DMCA intentionally sets a high bar for further exemptions to Section 1201 prohibitions that allow access to copyrighted works. The rulemaking process is specifically designed to give the law flexibility to address actual harms to the lawful uses of copyrighted works based on evidence presented by users. In addition to following the DMCA's model, the Act should narrow or remove any language that it ambiguous in nature, including in Section 65(2)(a), which states that such prohibition does not apply when "doing anything referred to therein for a purpose not expressly prohibited by this Act."

The Act, as a whole, should review multiple areas where overbroad language could conflict with international treaties, including the WIPO Internet Treaties. Such areas also include where the Act provides considerations for "exceptions and limitations" to copyright based on a "fair dealings" regime under Section 52(1)(a).

China: During my testimony, I was asked to provide examples of where the "essential facilities" doctrine is either proposed to apply, or is being applied, to patents in China outside of the context we provided in our initial comments to the 2024 Special 301 Review. For context, our initial comments raised that our small business technology developer community is concerned with the Chinese government's application of the essential facilities doctrine to IPR in the State Administration for Industry and Commerce's (SAIC)[1] Rules on Prohibition of Abusing Intellectual Property Rights to Eliminate or Restrict Competition (IP Abuse Rules), which took effect on August 1, 2015. The App Association does not support the notion that competitors should have access to "essential" patents (outside of the standardization context) because such provision seriously undermines the fundamental right to exclude others from using one's intellectual property, which is internationally respected. We are aware of at least one case where the "essential facilities" doctrine has been applied to non-standard-essential patents (SEPs), such as in 2021 when China's Ningbo Intermediate People's Court ruled that Hitachi Metals abused its dominance when it refused to license patents necessary for the production of sintered neodymium-iron-boron, though this decision was apparently later reversed based on a flawed market definition.[2]

The App Association is not aware of any new instances where the "essential facilities" doctrine has been applied outside *Hitachi Metals* case. However, despite the reversal of the Ningbo Intermediate People's Court decision on market definition grounds, we do stress the important implications of its application. 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.[3] Since China often denies their FTT practice[4] and claims that foreign entities voluntarily transfer their technology, the purpose of these practices remains unclear.[5] It is well-defined that the transfer of source code is, in part, justified by the intent to prevent cybersecurity threats.[6] 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.[7] Further, the lack of formal law or rules in China for its FTT policy

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

[2] https://www.proterial.com/e/press/2024/pdf/20240123en.pdf.

[3] 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.

[4] *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.").

[5] *Id*.

[6] 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.

[7] Jyh-an Lee, note 1 at 345-6.

creates a difficulty in determining what specific entities require disclosures for any one industry;[8] though joint venture requirements are used to mandate partnership with Chinese companies that can then access and own a percentage[9] 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.[10] 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.

South Africa: We would like to point to a fourth issue that has recently come to our attention in South Africa's copyright landscape, which the App Association raised in its written testimony. In applying the international copyright and copyright-related treaties, including the Berne Convention, WIPO Internet Treaties, and the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights, the country's provisions for limitations and exceptions do not fully align with the international three-step test. This is particularly true for new proposed statutory exceptions to the Copyright Amendment Bill (CAB) that enable access to copyrighted works to persons with visual or print disabilities. While this provision comes from a 2021 decision from the high court that declares current South African copyright law unconstitutional, such broad language is subject to abuse. Therefore, Section 19D of the CAB should be narrowly defined to be fit for the purpose of enabling access to persons that would otherwise be significantly harmed compared to other stakeholders from the lack of access to a copyrighted work.

[8] Jyh-an Lee, note 1 at 329.
[9] 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/.
[10] Jyh-an Lee, note 1 at 333.

I appreciate the opportunity to submit further comments to USTR and welcome the opportunity to assist the Administration further.

Thank you.

Brian Scarpelli
Senior Global Policy Counsel
ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005