

February 8, 2018

Mr. Sung Chang  
Director, Innovation and Intellectual Property  
Office of the United States Trade Representative  
600 17th Street NW  
Washington, District of Columbia 20036

**RE: *Input of ACT | The App Association regarding the U.S. Trade Representative's Request for Comments and Notice of Public Hearing Concerning its 2018 Special 301 Review [USTR-2017-0024]***

Dear Mr. Chang:

ACT | The App Association (App Association) writes in response to the Office of the United States Trade Representative's (USTR) request to identify countries that deny adequate and effective protection of intellectual property rights (IPR) or deny fair and equitable market access to U.S. persons who rely on IPR protections, to inform USTR's 2018 Special 301 Report.<sup>1</sup> We also request permission for Brian Scarpelli, senior policy counsel for the App Association, to present oral testimony at the Special 301 public hearing on February 27, 2018.

The App Association represents thousands of small business software application development companies and technology firms located across the United States.<sup>2</sup> Alongside the rapid adoption of mobile technologies, our members have developed innovative applications and products that improve workplace productivity, accelerate academic achievement, monitor health, and support the global digital economy. Today, the app ecosystem is worth more than \$143 billion and serves as a key driver of the \$8 trillion internet of things (IoT) revolution.<sup>3</sup>

---

<sup>1</sup> 82 FR 61363.

<sup>2</sup> See <http://actonline.org/about>.

<sup>3</sup> See [http://actonline.org/wp-content/uploads/App\\_Economy\\_Report\\_2017\\_Digital.pdf](http://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf).

## I. General Comments

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

- **Limiting Cross-Border Data Flows:** Limiting cross-border data flows hurts all players in the digital economy. The seamless flow of data across economies and political borders is essential to the global economy. In particular, innovative small app development companies rely on unfettered data flows to access to new markets and customers.
- **Data Localization Policies:** Companies expanding into new overseas markets often face regulations that force them to build and/or use local data infrastructure. These data localization requirements seriously hinder imports and exports, jeopardize an economy's international competitiveness, and undermine domestic economic diversification. Small app developers often do not have the resources to build or maintain infrastructure in every country in which they do business, effectively excluding them from commerce.
- **Customs Duties on Digital Content:** American app developers and technology companies take advantage of the internet's global nature to reach the 95 percent of customers that are outside the United States. However, the "tolling" of data across political borders with the intent of collecting customs duties directly contributes to the balkanization of the internet and effectively blocks innovative products and services from entering new markets.
- **Requirements to Provide Source Code for Market Entry:** Some governments have proposed or implemented policies that make legal market entry contingent upon the transfer of proprietary source code. For app developers and tech companies, intellectual property is the lifeblood of their innovation, and the transfer of source code presents an untenable risk of theft and piracy. These requirements present serious disincentives for international trade and are a non-starter for the App Association's members.

- **Requirements for “Backdoors” in Encryption Techniques:** Global digital trade depends on technical data protection methods and strong encryption techniques to keep users safe from harms like identity theft. However, some governments and companies insist that “backdoors” be built into encryption for the purposes of government access. These policies would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a security and privacy standpoint, the viability of app developers’ products depends on the trust of end users.
- **Intellectual Property Violations:** The infringement and theft of IPR (copyrights, trademarks, patents, and trade secrets) present a major threat to our members and the billions of consumers who rely on their digital products and services. Strong but fair protection of intellectual property for copyrights, patents, trademarks, and trade secrets is essential.

Most relevant to the Special 301 Report, the infringement and theft of IPR and trade secrets jeopardize the success of App Association members and hurt the billions of consumers who rely on their app-based products and services. Each kind of IPR (copyrights, trademarks, patents, and trade secrets) represents distinct utilities upon which App Association members depend. App developers and publishers lose an estimated \$3-4 billion annually due to pirated apps,<sup>4</sup> and IPR violations lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone a potential “end-of-life” occurrence for a small app development company. Common IPR violation scenarios include:

- **Copying of an App:** Disregarding copyrights, a pirate 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:** Disregarding copyrights, a pirate 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:** Disregarding copyrights, a pirate 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.

---

<sup>4</sup> Forbes, “App Developers Losing \$3-4 Billion Annually Thanks To 14 Billion Pirated Apps” (July 24, 2017), available at <https://www.forbes.com/sites/johnkoetsier/2017/07/24/app-developers-losing-3-4-billion-annually-thanks-to-14-billion-pirated-apps/#6816312e60da>.

- *“Brand-Jacking” of an App*: Disregarding copyrights, a pirate 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 ultimately putting their sensitive information at risk.
- *Misappropriation of a Trademark to Intentionally Confuse Users*: Disregarding trademark rights, a pirate will seek to use an app’s name or trademarked brand to trick users into providing their information to the pirate for exploitation.
- *Illegal Use of Patented Technology*: A pirate 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*: A pirate 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.

Section 182 of the Trade Act requires USTR to identify countries that deny adequate and effective IPR protections.<sup>5</sup> The Trade Act also requires USTR to identify which countries, if any, are Priority Foreign Countries that demonstrate subpar IPR protections for U.S. companies and citizens.<sup>6</sup> Pursuant to the relevant provisions of the Trade Act,<sup>7</sup> the App Association is pleased to provide its recommendations to this year’s Priority Watch List and Watch List. We support efforts by the U.S. government to protect American small businesses that rely on IPR to innovate and need certainty in the protection of their IPR abroad. We commit to partnership efforts with USTR to create responsible IPR protections across the globe to help our members enter new markets and create more U.S. jobs.

---

<sup>5</sup> 19 U.S.C. § 2242.

<sup>6</sup> *See id.*

<sup>7</sup> 19 U.S.C. § 2411-2415.

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

### A. China

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

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

Undertakings with dominant market position shall not, without justification, refuse other undertakings to license under reasonable terms their IPR, which constitutes an essential facility for business operation, to eliminate or restrict competition. Determination of the aforesaid conduct shall take into account the following factors:

- (i) whether the concerned IPR can't be reasonably substituted in the relevant market, which is necessary for other undertakings to compete in the relevant market;
- (ii) whether a refusal to license the IPR will adversely affect the competition or innovation of the relevant market, to the detriment of consumers' interest or public interests;
- (iii) whether the licensing of the IPR will not cause unreasonable damage to the licensing undertaking.

The App Association does not support the notion that competitors should have access to "essential" patents 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 left vulnerable because SAIC uses significant discretion to balance the necessary factors to determine the issuance of a compulsory license.

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

When a patent holder lends its patented technology to a standard, it can result in a clear path to royalties in a market that likely would not have existed without the wide adoption of the standard. To balance this growth potential with the need to access the patents that support the standard, many standard development organizations (SDOs) require patent holders of standardized technologies to license their patents on fair, reasonable, and non-discriminatory (FRAND) terms. FRAND commitments prevent the owners of SEPs, the patents needed to implement a standard, from exploiting the market power that results from the broad adoption of a standard. Once patented technologies are incorporated into a standard, manufacturers are compelled to use them to maintain product compatibility. In exchange for making a voluntary FRAND commitment with an SDO, SEP holders can obtain reasonable royalties from manufacturers that produce products compliant with the standard, who may not have existed absent the standard. Without a FRAND commitment, SEP holders would have the same power as a monopolist that faces no competition. In line with our members' core interests in this area, the App Association has established an initiative known as "All Things FRAND"<sup>8</sup> to assist policymakers including USTR in understanding SEP FRAND issues and developments; the App Association has further adopted and advocates for several key consensus principles to prevent patent "hold up" and anti-competitive conduct available on the All Things FRAND website.<sup>9</sup>

Specific to China and SEPs, the App Association acknowledges that certain entities like the Standardization Administration of China have attempted to publish policies that would have instructed Chinese-backed standardization bodies to lower or undermine royalty payments for patents, without differentiating between FRAND-encumbered SEPs and other patents. With assistance from the international community, such efforts have been thwarted. Today, SAIC's IPR Rules appropriately recognize that it may be an abuse of dominance for SEP holders to eliminate or restrict competition, "such as by refusing to license, tying or imposing other unreasonable trading terms, in violation of fair, reasonable, and non-discriminatory principle" (SAIC IP Abuse Rules, Art. 13). In contrast to its policies on patents generally, SAIC's treatment of FRAND-encumbered SEPs is consistent with an emerging consensus on how to deal with serious breaches of FRAND commitments. We strongly urge USTR to ensure that it does not conflate

---

<sup>8</sup> See <http://allthingsfrand.com> (international resource and repository for information and developments involving SEPs, including competition law issues and actions).

<sup>9</sup> See *Principles for Standard Essential Patents*, ABOUT ALLTHINGSFRAND.COM (last accessed June 8, 2017), at <https://allthingsfrand.com/about/>.

general patent licensing issues with the unique set of issues and global competition law consensus specific to SEPs.<sup>10</sup>

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

The App Association acknowledges that the Chinese judicial system has made some positive steps that lend to increased certainty in IPR protection (e.g., the establishment of specialized IPR courts). However, due to the high amount of infringement originating from China, as well as numerous policies and laws that enable IPR infringement or are selectively enforced, we strongly recommend China remain on the Priority Watch List.

## **B. Indonesia**

Indonesia continues to provide inadequate IPR protections and enforcement mechanisms, which serve as an extraordinary barrier to entry for U.S. small business innovators in the Indonesian market. We acknowledge that the Indonesian government has attempted to improve IPR enforcement. 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. These steps will also help prepare Indonesia to join the Madrid Protocol.

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 2017 review. For example, Indonesia has 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, nor have they removed counterfeit and pirated material from Indonesian markets.

As USTR noted in its 2017 review, 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, force American companies to products in Indonesia to protect their rights.

---

<sup>10</sup> To illustrate the scope of this consensus, the App Association has developed a non-exhaustive list of developments from across key economies, which can be viewed in recent comments filed by the App Association before the Japan Patent Office. See pgs. 5-12 of <http://actonline.org/wp-content/uploads/ACT-Comments-re-JPO-SEP-Licensing-Guidelines-final-111017.pdf>.

Based on the persistence of IPR protection and enforcement issues in Indonesia, the App Association recommends Indonesia remain on USTR's Priority Watch List.

### **C. Thailand**

Thailand continues to facilitate an environment where counterfeit and pirated software markets thrive because of limited legal enforcement mechanisms and a lack of rule of law. The App Association is encouraged by reports of the Thai government's attempts to employ strong commitment to address this growing concern,<sup>11</sup> but our members continue to face challenges.

The Thai government should also remain committed to address its extraordinary backlog of patent applications. In November 2017, the Thai government announced that it intended to provide more resources to combat this concern.<sup>12</sup>

Based on these issues, the App Association encourages USTR to keep Thailand on its Priority Watch List.

### **D. India**

India represents an immense opportunity for American small business tech and software development companies. However, App Association members continue to experience a wide range of IPR infringement and lack of legal redress.

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.<sup>13</sup> Moreover, as of May 20, 2016, the Indian government established additional commercial courts, advancing the 2015 Commercial Courts Act,<sup>14</sup> which the App Association perceives as further evidence of India's commitment to enhance its IP procedures.

The Indian government 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

---

<sup>11</sup> <http://thaiembdc.org/2017/06/26/thailand-focus-3/>.

<sup>12</sup> <http://www.tilleke.com/resources/thailand-now-clearing-its-backlog-patent-applications>.

<sup>13</sup> <https://spicyip.com/wp-content/uploads/2018/01/IPR-Regime-In-India-Government-Initiatives.pdf>

<sup>14</sup> <https://timesofindia.indiatimes.com/city/delhi/Commercial-courts-begin-functioning-in-Delhi-Mumbai/articleshow/52488068.cms>



(FICCI) have made an IPR Enforcement Toolkit for Police, and there have been 26 programs dedicated to training police officers on IP enforcement.

Despite this positive movement, the App Association believes it is necessary that India remain on the Priority Watch list because the country still needs to create an adequate IPR system and implement strong enforcement to provide needed certainty to our members seeking to enter the Indian market.

### **E. Russia**

The Russian market continues to present a massive challenge to App Association members. Since the USTR issued its 2017 301 report, Russia has continued to foster an environment driven by extensive software piracy. The Russian government does not appear to be committed to making any systemic changes to protect IPR.

Some positive indications can be seen, however. For example, the Russian government has attempted to reduce burdensome procedural requirements for copyright holders to bring civil actions by enacting a law on October 1, 2017, that allows pirated websites to be blocked without launching a lawsuit.<sup>15</sup> However, we hope strong and fair enforcement will accompany the development of this copyright policy.

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

### **F. Algeria**

Although it has enacted key statutes to prevent piracy, the Algerian government has yet to make any meaningful attempts to enforce these statutes. Failure to enact these statutes has allowed for widespread use of unlicensed software and has created a hurdle for U.S. small business app developers to enter the Algerian market. The Algerian government has also failed to provide adequate judicial remedies for patent infringement claims for multinational companies.

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

---

<sup>15</sup> <http://newsletter.us/articles/putin-has-14306>

## **G. Kuwait**

In 2016, Kuwait passed the landmark Copyright and Related Rights Law, which represented a positive step forward. In addition, Kuwait has demonstrated its commitment to uphold its law,<sup>16</sup> but, given the short lifespan of this legislation, USTR should continue to monitor developments in Kuwait until its system matures.

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

## **H. Ukraine**

Ukraine continues to have opaque administrative practices concerning the collection and distribution of IPR royalties. In addition, the Ukrainian government continues to unabashedly use unlicensed software with its agencies and has not enacted legislation concerning online copyright infringement.

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

## **I. Argentina**

Argentina continues to fail in providing meaningful legislation that will address rampant counterfeiting and piracy of IP protected materials. Moreover, there appears to be no effort among Argentinian law enforcement to enforce the current laws against such actions. This leaves many of our members open to having their respective IP stolen and are, thus, less likely to engage in the Argentinian market. Recently, the Argentinian government passed legislation that created a dispute resolution mechanism to enforce IPR. Although this is a positive step, USTR should continue to monitor these developments.<sup>17</sup>

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

---

<sup>16</sup> E.g., <https://www.rapidtvnews.com/2017092849008/kuwait-raids-lead-to-arrests-for-content-piracy.html#axzz56QtYauy2/>

<sup>17</sup> <http://www.wipo.int/wipolex/en/details.jsp?id=17282>.

### III. Conclusion

The App Association appreciates the opportunity to submit these comments to USTR, and we commit to work with all stakeholders to address the above concerns to create a prosperous U.S. economy.

Sincerely,



Brian Scarpelli  
Senior Policy Counsel

Joel Thayer  
Policy Counsel

McKenzie Schnell  
Associate

ACT | The App Association  
1401 K St NW (Ste 500)  
Washington, DC 20005