July 29, 2019

Ms. Raquel Cohen
The Office of Intellectual Property Rights (OIPR)
International Trade Administration, U.S. Department of Commerce
1401 Constitution Ave. NW, Room 21028
Washington, District of Columbia 20230

RE: Comments of ACT | The App Association to The Report on State of Counterfeit and Pirated Goods Trafficking and Recommendations [Docket No. 190703544-9544-01]

Dear Ms. Cohen:

ACT | The App Association (App Association) writes in response to the Department of Commerce Office of Intellectual Property Rights request for comment regarding the state of counterfeit and pirated goods trafficking through online third-party marketplaces to inform the President's Memorandum on "Combating Trafficking in Counterfeit and Pirated Goods."[1]

The App Association represents over 5,000 small business software application development companies and technology firms located across the mobile economy.[2] Alongside the rapid adoption of mobile technologies, our members develop innovative applications and products that improve workplace productivity, accelerate academic achievement, monitor health, and support the global digital economy. 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. Today, the app ecosystem is worth more than $1.3 trillion globally and serves as a key driver of the internet of things (IoT) revolution.[3]

Unfortunately, the same app developers that drive the global economy are also subject to an estimated loss of $3-4 billion annually due to pirated apps[4] and intellectual property rights (IPR) violations. Piracy presents a major threat to the success of the App Association's members and the billions of consumers who rely on digital products

[1] Department of Commerce, *Comment Request; Report on the State of the Counterfeit and Pirated Goods Trafficking and Recommendations*, 84 FR 32861(July 10, 2019).

[2] *See* https://actonline.org/about/.

[3] Medium, "Internet of Things booming 15 Trillion Market" (Sept. 16, 2018), available at https://medium.com/datadriveninvestor/internet-of-things-booming-15-trillion-market-88fde1da2113.

[4] *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-in-the-last-5-years-says-tapcore/#740b2fdf7413.

and services. Piracy, whether originating within the United States or abroad, threatens not only the creators of digital content by undermining their ability to innovate, invest, and hire, but it also threatens end-users' confidence in products and services as there is potential for consumers to be victimized by illegal sellers who pose as legitimate content owners and sellers. Counterfeit software apps can lead to customer data loss, interruption of service, revenue loss, and reputational damage. Further, with the rise of enterprise mobile app development, apps are being used as a means to attack mobile users of an entire enterprise. Counterfeit software programs have caused significant damage, and continue to pose substantial hazards, to app development companies that service every sector of the economy for countless end-users. 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.

- ***"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 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.

For example, App Association member Busy Bee Studios' children's app Zoo Train[5] was featured in the Google Play app store for sale at $0.99. This app uses colorful animal shapes and animations in providing educational puzzles and spelling lessons for young children. During a search for the product, the developers found another app in the Google Play store using the same name and artwork, but from a different publisher. This pirated app was free in the Google Play store, was displayed as a result of a search query for "Zoo Train," and—unlike the true Zoo Train app—displayed advertisements to earn bogus revenue as well as gained permission to control a user's device in order to access phone dialer information, the address book, and the network stack to install itself to run in the phone's operating system background to collect this information (in other words, a malware "stub" that sits inactive but can be activated with a command).

The Department of Commerce should look to the industry-led efforts to curb IP piracy through the Trustworthy Accountability Group (TAG) to assist in formulating ideas to combat IP piracy. TAG has developed certification programs for companies throughout the digital advertising supply chain designed to help industry collectively fight ad-supported piracy, as well as to combat malware, stop ad fraud, and increase transparency.[6] The TAG Certified Against Piracy Program not only recognizes the IP theft problem, but effectively addresses the harms that come with such IP theft. Research conducted by Ernst & Young (E&Y) in 2017 found that anti-piracy steps taken by the digital advertising industry through the TAG certification have reduced ad revenue for pirate sites by between 48 and 61 percent, notable progress against E&Y's earlier finding of the $2.4 billion problem of infringing content.[7]

[5] https://itunes.apple.com/us/app/zoo-train/id407870968?mt=8.

[6] https://www.tagtoday.net/.

[7] TAG, "About the Certified Against Piracy Program" available at https://www.tagtoday.net/about-certified-against-piracy-program/.

Conclusion

The App Association appreciates the opportunity to submit these comments to the Department of Commerce OIPR, and we are committed to working with all stakeholders to address the issues of intellectual property piracy online.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Debbie Rose
Intellectual Property Fellow

Alexandra McLeod
Policy Counsel

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