October 1, 2025

Mr. Daniel Lee
Assistant U.S. Trade Representative for Innovation and Intellectual Property (Acting)
Office of the United States Trade Representative
Executive Office of the President
600 17th Street NW
Washington, District of Columbia 20508

**RE:** ***Comments of ACT | The App Association to Request for Comments in the 2022 Review of Notorious Markets for Counterfeiting and Piracy*** **[Docket Number USTR- 2025-0018]**

Dear Mr. Lee:

ACT | The App Association (the App Association) writes in response to the Office of the United States Trade Representative's (USTR) request for comments to inform its 2025 Review of Notorious Markets for Counterfeiting and Piracy.[1]

The App Association is a 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. The value of the ecosystem the App Association represents—which we call the app ecosystem—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.[2]

The continued success of the mobile app economy requires dynamic solutions to online piracy and counterfeiting. Online enforcement activities include a range of tactics, including software platform protective measures and a variety of technological protection

[1] 90 FR 40134.
[2] The App Association, State of the U.S. App Economy, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

measures (TPMs) such as digital rights management (DRM) tools, firmware, encryption, obfuscation, monitoring, and analytics to protect applications from unauthorized copying and distribution. 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. Curated platforms and embedded software on devices provide critical protection against piracy and counterfeits.

Although license control by platforms has drastically improved the landscape for small developers, piracy is still a serious issue for app developers. IP theft can occur in the form of apps or services built to hack or displace legitimate app stores and platforms (i.e., "sideloading"). Legitimate applications are stolen, their copy protection is removed, and the apps are placed in illicit stores for download where no revenue goes to the original developer. Moreover, even in the world of free, ad supported applications this criminal activity still occurs with the original application's ad network stripped away and replaced by a pirate ad network that siphons the ad revenue to the pirate app developer. Trusted platforms' curation practices play a critical role in addressing such harmful piracy.[3]

Online piracy threatens consumer welfare by undermining the ability of creators of digital content to innovate, invest, and hire. 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. Piracy, whether originating within the United States or abroad, 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, these counterfeiting activities reduce the competitiveness of U.S.-developed apps and expose workers employed for illicit activity to exploitive labor practices. 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 intellectual property rights (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

[3] *See* https://actonline.org/2024/06/12/safeguarding-innovation-ip-concerns-and-the-dma/.

to prevent apps from running on devices with removed software restrictions (jailbroken devices).

- **"Brandjacking" 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.
- **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 to access their market.
- **Government Failure to Protect Trade Secrets**: An infringer will intentionally steal a trade secret, and subsequently benefit from 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.

While exact figures for total pirate app market revenue are scarce, industry analyses indicate growth beyond the prior $1.34 billion estimates in ad revenue lost yearly due to pirate apps, with increasing sophistication of piracy and ad fraud.[4] IP piracy is also responsible for a notable job losses to U.S. industries, including software development.[5]

While those threats persist, a large move from physical stores to e-commerce platforms have IP rights holders more aware of the protections at their disposal. As the economy shifts to new and emerging technologies, counterfeiters and pirates find clever ways to continue infringement activities through seemingly unregulated technologies and platforms. Our community believes that the laws and policies in place are adequate to handle infringement. However, platforms must continue to develop strong and effective mechanisms to remove infringing works and notify third-party users about any illicit activities on their platform. Small and medium-sized entities (SMEs), including our members, rely heavily on platform mechanisms to protect their IP and help avoid the cost of litigation.

[4] https://electroiq.com/stats/piracy-statistics/.
[5] *Id*.

Major jurisdictions aside from the United States are enacting and proposing regulations today that would disrupt platforms' ability to protect IP rights. As a prime example, the European Union has advanced new regulations for online platforms, via the Digital Markets Act (DMA),[6] intending to address contractual clauses and trading practices in relationships between platforms and businesses, which pose significant risks to U.S. small business engagement in the global digital economy.[7] Although they may not qualify as "gatekeepers" under the DMA, small developers will suffer significant consequences from the obligations introduced in the DMA. SMEs are particularly vulnerable if those obligations threaten the tangible advantages currently provided to them by digital platforms. Specifically, the DMA, through mandating sideloading, will prevent digital platforms from taking measures to protect IPR on their platforms and therefore in the digital economy. With the DMA now in place, USTR has appropriately designated the DMA as a barrier to digital trade in its National Trade Estimate Report on Foreign Trade Barriers.[8] In the context of its 2025 Review of Notorious Markets for Counterfeiting and Piracy, USTR should consider the role of the DMA in creating or enabling notorious markets and include discussion of the same in its 2023 Review, and should further track this relationship for future Reviews of Notorious Markets for Counterfeiting and Piracy.

We note that challenges still exist where some foreign jurisdictions undercut the ability to use TPMs by requiring businesses to comply with government oversight of confidential business information to participate in its domestic market, ultimately undercutting the viability of a business's products and services. For example, China's use of vague encryption laws provides them the ability to override mechanisms in copyright law such as TPMs, although this violates China's obligation as a member of the WTO TRIPS and WIPO Internet Treaties (WCT and WPPT) to not interfere with the IPR's issuing jurisdiction's ability to determine its protection and enforcement. This current challenge chills innovation across various industries, including the app industry, and will likely be prevalent in new markets.

The App Association supports USTR's efforts to identify markets of concern for counterfeiting and piracy, as well as USTR's efforts to promote industry awareness, best practices, and lawful behavior. When USTR is successful in identifying infringers, it encourages industry-led efforts to curb IP piracy. For example, Trustworthy Accountability Group (TAG) has developed certification programs for companies throughout the digital advertising supply chain designed to help industry collectively combat malware, stop ad fraud, and increase transparency.[9] The TAG Certified Against Fraud Program not only recognizes the IP theft problem, but effectively addresses the harms that come with such

[6] European Commission, Online Platforms, available at https://ec.europa.eu/digital-single-market/en/policies/online-platforms.
[7] https://actonline.org/wp-content/uploads/ACT-The-App-Association-DMA-Position-Paper-March-.pdf.
[8] *E.g.*, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/march/ustr-releases-2023-national-trade-estimate-report-foreign-trade-barriers.
[9] *See* https://www.tagtoday.net/certifications.

IP theft. Research conducted by the 614 Group found that anti-fraud steps taken by the digital advertising industry combated invalid traffic through the TAG certified channels by 88 percent compared to non-certified channels.[10]

The App Association appreciates the opportunity to submit these comments to the United States Trade Representative. We look forward to continuing to provide our perspective on the annual review of notorious markets for counterfeiting and piracy.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

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

[10] TAG FRAUD BENCHMARK STUDY, The 614 Study, November 2019, available at https://cdn2.hubspot.net/hubfs/2848641/TAG%20Benchmark%20Study%202019-1.pdf.