October 2, 2024

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 2024 Review of Notorious Markets for Counterfeiting and Piracy* [Docket Number USTR-2024-0013]

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 2024 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. App Association members are active in new platforms, like Web3, develop using new technologies (i.e., artificial intelligence), and innovate on top of technical standards. The small businesses and startups we represent both hold and license patented technologies, rely on a fair and consistent patent ecosystem, and are directly affected by the approach to patent rights and litigation by the United States Patent and Trade Office (USPTO). 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]

I. General Comments

The continued success of the mobile app economy provides strong support for private industry solutions to online piracy and counterfeiting, yet infringers still undermine current protections relied upon by app developers. Online enforcement activities include a range of tactics, including software platform protective measures and a variety of technological protection measures (TPMs) such as digital rights management (DRM) tools, firmware, encryption,

[1] 89 FR 66754.
[2] The App Association, State of the U.S. App Economy, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

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. Much of IP theft comes through apps or services that are 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.

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 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. A survey of App Association members indicates that one-third of sampled members with trademarks have experienced brand-jacking.[3]

[3] Survey Says: IP is Essential to Innovation (June 21, 2022), https://actonline.org/2022/06/21/survey-says-ip-is-essential-to-innovation/.

- **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.

Trends in global online counterfeit and piracy spiked during the peak of the COVID-19 pandemic, with software piracy increasing 20 to 30 percent.[4] 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 businesses (SMBs), including our members, rely heavily on platform mechanisms to protect their IP and help avoid the cost of litigation.

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),[5] 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.[6] Although they may not qualify as "gatekeepers" under the DMA, small developers will suffer significant consequences from the obligations introduced in the DMA. Small and medium-sized entities (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 should continue to designate the DMA as a barrier to digital trade as the agency did in past National Trade Estimate Report on Foreign Trade Barriers.[7] Pirates that operate on websites

[4] *See* https://www.smartprotection.com/articles/the-hard-reality-of-software-piracy#:~:text=Today%2C%20global%20software%20companies%20are,with%20Ipsos%20supports%20this%20evidence.
[5] European Commission, Online Platforms, available at https://ec.europa.eu/digital-single-market/en/policies/online-platforms.
[6] https://actonline.org/wp-content/uploads/ACT-The-App-Association-DMA-Position-Paper-March-.pdf.
[7] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/march/ustr-releases-2023-national-trade-estimate-report-foreign-trade-barriers.

and in app stores are profiting an estimated $1.34 billion a year in revenue;[8] in 2021 alone, the top apps offering stolen content generated $259 million in global annual ad revenue, with the top five of these apps making an average of $27.6 million in ad revenue.[9] USTR should continue to track the relationship between the DMA in creating or enabling notorious markets for future Reviews of Notorious Markets for Counterfeiting and Piracy.

The United States Trade Representative (USTR) has identified 39 online markets that have experienced a high volume of counterfeiting and piracy activity.[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.[11] 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.

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 (e.g., NFTs).

II. Threats to New Digital Spaces

In addition to the current and ongoing challenges that we have identified above, concern for counterfeit and pirated goods exist in new digital spaces and technologies, notably Web3 and artificial intelligence (AI) systems. It is important to consider that IP protections for digital goods are often easily manipulated outside the jurisdiction of the issuing nation. Therefore, it should be anticipated that the protection and enforcement of such goods will have to be integrated into existing international treaties and newly drafted international agreements.

a. Web3 and NFTs

On February 3, 2023, the App Association provided detailed comments to the United States Patent and Trademark Office (USPTO) and the United States Copyright Office (USCO) (the "Offices") on their *Joint Study on Non-fungible Tokens (NFTs) and Related Intellectual Property Law Issues*.[12] In parallel to our comments, we provided our community views in a listening session held on January 24, 2023, by the Offices on trademarks and NFTs. Per our presented

[8] Digital Citizens Alliance, White Bullet, *Breaking* Bads*: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market* (August 2021), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf.
[9] *Id.* at 1.
[10] *See* https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/february/what-they-are-saying-ustr-releases-2023-review-notorious-markets-list.
[11] *See* https://www.ndrc.gov.cn/xwdt/tzgg/202203/t20220325_1320233.html?code=&state=123.
[12] *See* https://www.regulations.gov/comment/COLC-2022-0005-0026.

views, we noted that the NFT mechanism may alleviate barriers that some innovators face to properly enforce their IP ownership against bad actors. Small innovators often find it difficult to protect and enforce their IP while operating with minimal resources.

The unmovable, unchangeable, and undividable nature of an NFT has, in large part, relieved this issue by allowing IP owners to secure their IP in the blockchain while tracking the chain of possession for each NFT linked to their protected asset. A smart contract within an NFT performs a task when predetermined conditions are satisfied, which allows IP rights holders to license, transfer, or execute payments related to their linked IP-protected asset upon presetting conditions. The transparency of the blockchain provides all relevant parties the ability to track and review the agreements. The capabilities of a smart contract also make it possible for NFT creators to use them as a digital rights management (DRM) tool. App Association members rely on technical protection measures (TPMs) like the DRM tool to protect their IP.

While there is great potential in the Web3 platform infrastructure and in the use of an NFT contributing to an efficient IP licensing system, the blockchain is still encumbered by counterfeiting and piracy. Software developers can still be harmed by online piracy occurring on the blockchain when an NFT is utilized to protect the IP of an asset. The greatest challenge that affects the sale or transfer of IP protected assets through NFTs is that the blockchain does not distinguish ownership from possession. Therefore, if the minter of an NFT holding an underlying IP protected asset is not the IP owner, the blockchain will not recognize the creation, sale, and use of the NFT as theft or fraud. Similarly, if a bad actor can steal an NFT from its owner's wallet through, for example, a phishing scam, the blockchain will recognize the theft as a transfer, and the thief will be identified as the new owner of the NFT.[13]

Other challenges that may enable counterfeiting and piracy activity in NFT markets are costs, IP registration, and the application of existing laws and legal mechanisms. The Ethereum blockchain is the most widely accessed platform for NFTs, where a gas tax is applied when an NFT is created, sold, bought, or transferred to compensate data miners who use computing energy to validate transactions. Due to the popularity of the Ethereum blockchain, the high volume of transactions has imposed a high tax on transactions. This means that the decision to use this blockchain to store, protect, or license an IP-protected asset largely relies on the number of resources available. Small businesses are less likely to be able to afford to utilize NFTs as a protection mechanism on the Ethereum blockchain, barring them from an emerging market and efficient enforcement mechanisms for their IP. This issue should not only be considered as it relates to Ethereum, but as it relates to any existing or future blockchain that becomes a popular venue to store IP-protected assets.

We note the case law currently developing on NFTs does not accurately represent all users of NFTs. For example, our community of software developers may not be challenged with the issues faced by visual artists, but they are sure to be faced with uncertainties regarding what nuances on the blockchain affect the infringement and fair use of their digital IP.

b. Artificial Intelligence (AI) Systems

AI systems are advanced technical tools that have become essential to creators of IP-protected goods. This area of law and policy is being contemplated and has invoked fear around how AI might enable counterfeiting and piracy activity, whether intentional or unintentional. Generative

[13] *See* https://www.wired.com/story/nfts-dont-work-the-way-you-think-they-do/.

AI platforms are AI systems that invoke the most fear because of the potential for these systems to train on and output data that could be IP protected.

The App Association believes that the existing copyright laws sufficiently support concerns around how the use of generative AI platforms assist in piracy and counterfeit-related efforts. Whether the analysis of fair use may lean towards infringement in the case of copyright or trademark law is attributed to the conduct of these platforms and their users. The platform outputs are not often a direct translation from what it receives. Much like a human brain, AI systems train on data to understand patterns and create rules that help them make decisions. Therefore, AI systems can create something novel. It is conceivable that, like a human, an AI system might output, in part or in whole, an image, writing, wordmark, or other IP protectable work. In those cases, generative AI platforms and users of those platforms must adhere to best practices and principles that we expect will develop over time with the guidance of relevant agencies, including the United States Patent and Trademark Office (USPTO) and the United States Copyright Office (USCO).

Like app developers and an app store, the interdependent relationship between a generative AI platform and its users is important. Generative AI platforms are essential for software developers to compete because it speeds up the coding process by recognizing patterns in the code and helping complete lines of code. Some generative AI platforms allow developers, for a nominal fee, to choose to ensure that the AI does not train on the developer's data. As this type of relationship grows, standards of practice will be used as protective measures against digital counterfeiting and piracy.

The App Association appreciates 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 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.[14] The TAG Certified Against Fraud Program not only recognizes the IP theft problem, but it also effectively addresses the harms that come with such 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.[15]

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.

[14] *See* https://www.tagtoday.net/certifications.

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

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Priya Nair
Intellectual Property Policy Counsel

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