



July 29, 2019

Filed electronically via [www.regulations.gov](http://www.regulations.gov); Docket No. 190703544-9544-01

Earl Comstock  
Office of Policy and Strategic Planning  
Department of Commerce  
1401 Constitution Avenue, NW  
Washington, DC 20230

**Re: Comment Request on the State of Counterfeit and Pirated Goods Trafficking and Recommendations, 84 Fed. Reg. 32861, pp. 32861-32863 (July 10, 2019)**

Dear Mr. Comstock:

The Entertainment Software Association (“ESA”) welcomes the opportunity to comment on the proliferation of counterfeit goods sold through e-commerce websites. Our response to the Department of Commerce’s (“Department”) request for stakeholder input will also address the industry’s copyright and trademark concerns as well as offer our perspective on potential “best practice” guidance as noted in the Department’s Federal Register notice. The Department seeks perspectives and information on (1) the impact of industry interests affected by counterfeit or pirated goods available on third-party platforms; (2) the factors that contribute to trafficking in these types of goods; (3) the availability of effective technologies that could substantially reduce the sale and importation of counterfeit and pirated goods; (4) the role of collaboration and information-sharing; (5) effective policies, procedures or best practices of private sector stakeholders; and (6) any remedies, including administrative, regulatory, or legislative, to be implemented by the U.S. Government that would substantially reduce the trafficking in illegitimate goods and promote effective law enforcement. ESA intends to address these questions in its filing.

ESA is the U.S. trade association for companies that publish interactive entertainment software for video game consoles, handheld devices, personal computers, and the internet.<sup>1</sup> It represents nearly all of the major video game publishers and gaming platform providers in the United States. In 2018, the industry generated \$43.4 billion in total revenue, with consumers spending \$35.8 billion on software, downloadable content and subscriptions, up from \$29.1 billion in 2017. Also in 2018, consumers spent a total of \$5.1 billion on video game consoles and \$2.4 billion on accessories and virtual reality hardware, including headsets, up from \$4.7 billion and \$2.2 billion in 2017, respectively. The industry added more than \$11.7 billion in value to U.S. GDP in 2017 and directly employed more than 65,000 people in the United States and 220,000 indirectly.

---

<sup>1</sup> A list of ESA members is available at <http://www.theesa.com/about-esa/members/>.

The video game industry is at the forefront of both innovation and job creation, which are buoyed by the strong protection and effective enforcement of intellectual property rights. Strong IP rights also ensure that gamers have access to authentic games, services and hardware accessories. With this purpose in mind, the video game industry, individually and also through ESA, has fostered and maintained constructive relationships with U.S. law and border enforcement, e-commerce platforms and online intermediaries in several countries as a key part of its global content protection program.

### **The Impact of Counterfeit and Pirated Goods on the Video Game Industry**

The video game industry is negatively impacted by the sale and importation of counterfeit and pirated goods via third-party marketplaces and intermediaries. Like many industries, the video game sector has to contend with the infringement of copyright in software, the infringement of trademarks and trade dress through the counterfeiting of hardware, accessories and merchandise and, additionally, issues of security such as the hacking of games and game networks and account reselling. Demand for our compelling products and services plus the desire for cheaper alternatives combined with the ease of sale to a worldwide market and the ease of delivery after purchase have given rise to problems involving infringement. The conditions that give rise to the sale and availability of illegitimate goods may cause substantial loss of revenue for our members and may pose health and safety risks for consumers, like, for example, counterfeit batteries or adapters. The most commonly counterfeited items include accessories such as video game controllers—which traditionally pair with game consoles and “plug-n-play”<sup>2</sup> devices that appear to be genuine. Although circumvention devices are not necessarily counterfeit items, they pose significant challenges to video game companies, especially console and accessories manufacturers, because these devices facilitate the mass infringement of intellectual property rights and other unauthorized uses of video game consoles. To assist the Department in understanding the nature of the problem, a brief description of counterfeits and also circumvention devices, follows.

#### ***Counterfeits***

Members’ wireless controllers designed for use with video game consoles, such as Microsoft’s Xbox and Sony’s PlayStation 4 console, are also targeted by sophisticated counterfeiters, who produce counterfeit controllers that look so close to the original that it can be difficult to tell legitimate from illegitimate products. ESA members also encounter user-generated counterfeits/unlicensed merchandise, such as print-to-own t-shirts or other print-to-sell merchandise as well as toys and figurines. Some prominent social media websites have become havens for the marketing and sale of counterfeits such as these and due to limited search functionality of these websites, it is difficult to perform scanning of the platform for unauthorized merchandise.

---

<sup>2</sup> A recent and troubling trend in the video game industry is the production of legacy game consoles that come pre-loaded with popular games (often referred to as “plug-and-play devices”). High nostalgia value and low manufacturing costs make certain popular consoles prime targets for scalping and counterfeiting that can result in plug-and-play consoles.

Despite ESA members' efforts to search for and remove counterfeit products from e-commerce platforms through takedown notices, cease-and-desist letters, litigation or law enforcement raids, the volume and availability of counterfeit goods produced primarily in Asia, in online marketplaces, pose a continuing challenge. Social media networks also provide unauthorized sellers with the ability to better target consumers through aggressive advertising and also sales of counterfeits.

### ***Circumvention Devices***

A circumvention service or device bypasses the technological protection measures employed by rights holders to protect their video game software and hardware such as a video game console. There are a number of different types of circumvention devices including modification ("mod") chips, game copies and even circumvention through software modifications ("soft mods"). A mod chip is a semiconductor chip that contains a program that circumvents the technical protection measures of a console system. When a "mod chip" is affixed to the circuit board of a console, it allows the systems to run illegitimate copies of games. Soft mods use software to modify the normal operation of video game console hardware in a way that can unlock or disable security features used to prevent the play of illegal games. Once the security features are unlocked, users can circumvent copy protections employed by rights holders on game cartridges or discs and within a video game console. A popular circumvention device today is the "game copier", which is designed exactly like the video game cartridge, in the greatest detail, includes features (*i.e.*, shape, size, thickness, connections, sockets and pin configuration) of a video game cartridge. These types of circumvention devices allow users to copy, download and play unlimited illegal copies of games on hardware.

### **Countering the Sale and Importation of Counterfeit and Pirated Goods Online**

The Department requests a description of technologies that are used or could be utilized by both rights holders and platforms to counter the sale and importation of counterfeit and pirated goods online. Effective technologies and means with which to counter the sale of counterfeit and pirated goods do exist and are in use by ESA members. However, measures can be taken by platforms to augment the effectiveness of methods used to stymie the sale of illegitimate goods on platforms.

ESA member companies who manufacture hardware accessories use, for example, copy-resistant logos and seals on products assist in verifying authenticity, while others use serial numbers for authentication. These companies work with retailers to ensure that counterfeit/infringing products are not sold in legitimate stores. However, distribution under the radar, such as to individual buyers in small packages, can be difficult to detect. In addition, ESA produces a training manual for law enforcement that details some of the common elements of counterfeit controllers, such as the poor reproduction of trademarks, the lack of labels or quality seals, or labels that include incorrect information.

Also helpful, we believe, in countering the sale of counterfeit and pirated goods online would be the institution by platforms, particularly those that are small- and medium-sized, of

easy-to-use portals with easy-to-fill-out forms and limited formalities capable of tracking and reporting the takedown notices submitted by IP rights holders. Not only would tracking that data lead to greater and more useful data-sharing between rights holders and platforms, but it could also assist in identifying repeat offenders to be flagged for action by intermediaries. Although large, well-known online marketplaces may already employ these kinds of enforcement tools, it is crucial to effective enforcement that smaller platforms also adopt these types of technologies.

### **Stakeholder Collaboration and Information-Sharing**

Coordination between rights holders and platforms is extremely important to address counterfeit and pirated goods occurring on e-commerce platforms. ESA participates in non-public and/or informal trusted-notifier programs with online intermediaries. ESA monitors many of the major online platforms for infringing goods and has found that the larger platforms generally respond promptly to requests to remove unauthorized listings. When novel forms of infringement are identified, larger platforms are generally responsive and collaborative in their approach to working with ESA. ESA also trains platforms to identify and address listings of products and services that infringe member companies' intellectual property or that violate their terms of service.

ESA and its members collaborate closely with federal law and border enforcement necessitating constant information-sharing with the U.S. government. For example, ESA engages with federal law enforcement to address the issue of counterfeit products with the Department of Homeland Security's Office of Homeland Security Investigations and U.S. Immigration and Customs Enforcement. In addition, ESA members support and coordinate with U.S. law enforcement to authenticate suspected counterfeit merchandise or investigate into the hacking of video game consoles or the illegal distribution of hacking software tools.

On behalf of its members, ESA conducts nationwide trainings and education for local, state and federal law and U.S. Customs and Border Protection ("CBP") enforcement personnel on the protection of video game software, hardware and accessories and, to date, ESA's program has delivered free trainings to thousands of enforcement officers in the United States and around the world. ESA and its members also provide officials from CBP with the support and tools required to confirm the illegality of suspected infringing imports or devices designed to bypass technological measures put in place to protect video game consoles.

Given our positive history with CBP, ESA supported the Trade Facilitation and Trade Enforcement Act of 2015 ("TFTEA"), which called for heightened cooperation between U.S. government agencies as well as between the U.S. government and industry on intellectual property rights enforcement. Section 303 of TFTEA dealt specifically with the seizure of circumvention devices, including a directive that CBP notify affected companies not later than thirty days after seizure of information regarding the merchandise seized. Unfortunately, some of our member companies report that communication between CBP and rights holders about seized merchandise at the border is not occurring despite the statutory mandate. In fact, CBP still has not promulgated regulations implementing Section 303. Given the crucial role border enforcement plays in stemming the importation of illegitimate goods into the United States, we

encourage CBP to work with rights holders to facilitate the intention of TFTEA in order to improve intellectual property rights enforcement.

### **Existing or Additional Policies, Procedures or Best Practices of Online Intermediaries That Have a Positive Impact**

As stated previously, ESA, its member companies and its online enforcement vendors participate in “trusted-notifier” and brand registry programs offered by e-commerce platforms that allow rights holders to send a high volume of notices of infringing content or products to the platform for removal. ESA members also have independent relationships with online marketplaces, maintain an ongoing dialogue with them to identify infringing listings and to provide background on emerging threats. The benefits of these types of programs include a more streamlined process for identifying and removing counterfeit products, access to key points of contact at platforms for better support, and the enhanced capability to collect enforcement metrics (e.g., complete seller information, sales volume, related product offerings and accounts) to guide resource allocation. We believe that “trusted notifier” programs, in particular, should be expanded with fewer limitations on how long one takes to qualify as a “trusted notifier” as well as more information and search options available to rights holders. Along with robust repeat infringer policies and reliable enforcement of those policies (which are key to effective enforcement), the enforcement burden on rights holders would diminish.

ESA members periodically conduct test buys to determine the authenticity of products. If a product turns out to be counterfeit, the members initiate a takedown through a removal notice to the relevant website or ISP. Some member companies find utility in making test buys to evaluate new counterfeit products that were not previously known or to identify targets or potential distribution networks. However, it can be very difficult to track unauthorized sellers through test buys because much of the platform account information is false or hidden behind anonymous accounts. Stronger verification of the identities of sellers and vendors on platforms by the platforms themselves and measures to ensure sellers cannot set up multiple accounts to evade enforcement, is crucial to the effective tracking of repeat infringers as well as determining the source of illegitimate goods. Meanwhile, a high volume of takedown notices, particularly over a sustained period of time, is indicative of a significant problem that calls for proactive efforts. Platforms should take proactive measures to prevent the posting and sale of counterfeit and pirated goods in the first place. For example, platforms should work with rights holders to develop key words and meta tags associated with high likelihood of infringement and block listings with those terms. In addition, law enforcement collaboration directly with platforms to tackle egregious offenders would be beneficial and would be greatly aided by information the platform would have on repeat infringers, drawn from the tracking and reporting of takedown notices.

### **Recommendations for Government Remedies**

ESA believes that the U.S. Government could help to improve the health of the online marketplace by: (1) amplifying U.S. Government cooperation on policy and exchanges of best

practices and information-sharing with foreign governments; (2) enhancing communication between rights holders, law and border enforcement officials through greater coordination and rulemaking, if appropriate; and (3) advancing interagency coordination and alignment in a manner that involves all relevant stakeholders.

### ***Cooperation and Rulemaking***

As noted earlier, a major obstacle to enforcement is the lack of communication between rights holders and CBP, especially when CBP still does not send the required seizure notices as mandated by TFTEA. We continue to urge CBP to promulgate regulations implementing Section 303 to aid in the effective enforcement of intellectual property rights.

The U.S. Government maintains valuable channels and programs through which it collaborates with foreign counterparts on ways to tackle and combat problems in the online marketplace related to infringement. This type of cooperation is particularly important particularly because these issues, bad actors and consumers frequently in different jurisdictions. The ability of stakeholders to participate adds even greater value. ESA engages with foreign governments through trainings and education. For example, ESA works with the U.S. Patent and Trademark Office's Global Intellectual Property Academy to educate foreign officials, including judges and prosecutors, on the video game industry, its enforcement challenges in a particular country and what can be done to improve laws and regulations governing intellectual property rights enforcement. ESA also supports constructive dialogue with foreign governments through our participation in U.S. trade policy on intellectual property, such as the Special 301 review process and report, the related Notorious Markets List and free trade negotiations.

The U.S. Government should also prioritize efforts to work with foreign governments to enhance their intellectual property laws and enforcement tools (both criminal and civil self-help remedies), including rules relating to circumvention devices and services. Free trade agreements (FTAs) have proven to be an effective approach, but are also inherently slow (i.e., multi-year negotiations) and narrow (i.e., with one or a small number of partners). The development of other tools that can effectively and more quickly improve the legal and enforcement environment in overseas markets would be beneficial.

### ***Coordination and Best Practices***

We encourage a sustained interagency effort, led by the Office of Intellectual Property Enforcement Coordinator ("IPEC"), located within the Executive Office of the President, to address the problems of counterfeit and pirated goods online using an approach combining both policy and field work and from a holistic perspective. For example, as it did with payment processors and advertising networks in recent years, the IPEC could bring together stakeholders with dissimilar views to draw up agreed-upon best practices, without the need for legislation or other regulation, on important issues such as notice-and-takedown of listings, information-sharing, verification/know-your-customer policies, proactive measures, heightened obligations for warehousing and distribution service providers, and/or repeat infringer policies. ESA members have noted that infringers employ shipping tactics to avoid detection, such as shipping products via third party shipping agencies that are delivered via fulfillment centers to avoid tracing back to their distribution networks. This is a problem that will require the input of all

stakeholders, including shippers, delivery services and online e-commerce platforms, to address effectively; hence, we believe it is a good candidate for IPEC stakeholder engagement.

IPEC, along with the interagency, should also consider working to improve the availability of internet domain WHOIS information because doing so will aid industry efforts to combat trafficking in counterfeit and pirated goods. WHOIS is a publicly -accessible database that historically has contained the identity and contact information for the entity that registered a particular domain name. With the advent of the European Union’s General Data Protection Regulation (GDPR), internet domain name registries and registrars, who supply registrant information to the WHOIS database, have begun to mask critical WHOIS data (without regard for the distinction between legal or natural persons) necessary to discover who may be responsible for websites that host or link to downloads or sales of pirated, infringing video games, counterfeit video game hardware and circumvention accessories. This practice by registrars and registries has significantly hampered enforcement by industry and law enforcement alike. ESA member companies must now rely on internet service providers (ISPs) and other online intermediaries in order to have takedown notices forwarded to site operators. If positive action is not forthcoming, then companies have no meaningful way to conduct enforcement and safeguard their intellectual property rights without expending even greater resources; this is especially difficult for ESA members that are small businesses and that do not conduct their own enforcement in-house.

ESA urges the U.S. government to continue to support limiting the cascading effects of the loss of WHOIS information for U.S. consumers and business owners by advocating for the distinction between collection of information for legal versus natural persons and that U.S. registrars and registries abide by the terms of their contracts with ICANN including continuing to provide WHOIS information about U.S. persons as before. In the case of non-U.S. registries and registrars, we ask the U.S. government to lend its support to discussions on a viable tiered access model that prioritizes rights holders and members of law enforcement. Although a potential candidate for best practices, the U.S. government should do more to determine if legislation or regulation is needed to remedy the gap in enforcement due to the loss of WHOIS data for rights holders.

### **Comment on Potential “Best Practices” Guidance**

ESA believes it is useful that the U.S. government is considering ways in which to improve the online marketplace for all stakeholders; however, this goal must be accomplished in ways that are not overly burdensome on platforms or intermediaries, taking into account the scale of the problem. In its request for industry input, the Department of Commerce listed some potential guidance currently under consideration for stakeholder feedback. They include (1) conducting an advance vetting of potential sellers and vendors, (2) establishing and enforcing a “prohibited” list of goods that should not be sold, (3) taking down listings of counterfeit and pirated goods and notifying other third-party intermediaries and (4) notifying law enforcement that an online third-party marketplace has determined that particular seller or vendor has been supplying counterfeit or pirated goods. Each of these items is addressed below.

First, ESA supports the notion of enhanced vetting and verification of sellers and vendors on online platforms, including e-commerce or social media. Enhanced vetting has the potential to reduce the incidence of fake information and credentials resulting in more effective enforcement.

Second, we believe that a “prohibited list” of goods, as proposed by the Department, would also be helpful to ESA and its members who must contend with counterfeit goods bearing a specific mark that should be barred from sale in the online marketplace.

Third, ESA, its vendors and its members already work with online platforms as partners in an effort to clear the marketplace of harmful products. However, best practice guidelines that call for the streamlining and standardization of takedown processes would be useful for rights holders and so we encourage the U.S. government to work towards such guidelines.

Fourth, ESA’s concern with the proposed practice of notifying law enforcement (i.e., notifying law enforcement that an online third-party marketplace has determined that a particular seller or vendor has been supplying counterfeit or pirated goods) is the potential for misuse. Guardrails would need to be put in place to ensure that such notification could not be used in bad faith against largely sellers of “one-offs” and instead keep the focus on large-volume, commercial-scale infringers and counterfeiters.

**Conclusion**

The video game industry faces serious challenges from infringers and counterfeiters who are making products that not only deceive consumers, but also cut into industry revenue and endanger American jobs. In order to effectively combat the sale of counterfeit goods on e-commerce platforms, ESA and its members support collaboration, communication and information-sharing amongst stakeholders in e-commerce including state and federal law and border enforcement, platforms, rights owners, advertisers and payment processors. Only when there is agreement for shared responsibility from all stakeholders in electronic commerce can there emerge effective measures to address the problems articulated here.

Should the Department have any questions or comments concerning ESA’s response, please contact Bijou Mgbojikwe at (202) 223-2400.

Respectfully submitted,



Bijou Mgbojikwe  
Senior Counsel, Intellectual Property Policy