Written testimony of

JONATHAN BERROYA
SENIOR VICE PRESIDENT AND GENERAL COUNSEL
INTERNET ASSOCIATION

before the

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET
JUDICIARY COMMITTEE
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

The SHOP SAFE Act: Stemming the Rising Tide of Unsafe Counterfeit Products Online

Thursday, May 27, 2021

Subcommittee Chairman Johnson, Ranking Member Issa, and members of the Subcommittee.

Internet Association[1] (IA) appreciates the opportunity to testify at today's subcommittee hearing on behalf of the association and its members about the SHOP Safe Act.

IA represents over 40 of the world's leading internet companies. IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. The internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, we ensure stakeholders understand these benefits.

Internet companies, including IA's members, are at the forefront of protecting consumers from counterfeits. The experiences of IA's members demonstrate that anti-counterfeiting policy must reflect the necessary partnership between brands and marketplaces, and focus on measures that encourage effective technology and target bad actors. A thriving online economy benefits all stakeholders, including millions of innocent small and medium-sized businesses that are able to access global customers thanks to IA's member companies.

We can all agree that protecting consumers from harmful counterfeit products - no matter how they enter the supply chain - is an important priority. But because professional counterfeiters are incredibly resourceful and adept at circumventing enforcement activities, it is also critical to examine and understand the unintended consequences of proposed solutions.

I. COUNTERFEITING IS NOT UNIQUE TO THE INTERNET

In the last two decades, U.S. internet services have become a significant driver of the U.S. economy. The internet sector contributes 10.1 percent of the U.S. GDP and 4.0 percent of jobs (non-farm employment). IA estimates the internet sector supported another 13.1 million indirect jobs and that the sector invested over $60 billion into the

[1] *Members,* Internet Association, https://internetassociation.org/our-members/ (last visited Dec. 22, 2020).

economy.[2] Since the mid-90s, consumers have increasingly been shopping online. In 2017, global e-retail sales amounted to $2.3 trillion and projections show a growth of up to $4.48 trillion in 2021.[3]

A small percentage of bad actors misuse online marketplaces to offer counterfeit goods. But counterfeiting did not begin with the internet. Spurious trademarks are as old as trademarks themselves; by the early 1980s, long before the commercial internet, 30 percent of businesses responding to an ITC questionnaire reported that their goods had recently been subject to counterfeiting.[4] Nor did counterfeiting through brick and mortar stores end with the growth of online services. Some of the most significant recent secondary liability trademark cases in the United States involved physical storefronts, not online companies.[5]

Even as the sale of goods has moved increasingly online, physical markets continue to play the dominant role in facilitating the trade in counterfeit goods, including markets in China, Russia, and Vietnam, among other places. In 2019, the Organisation for Economic Co-operation and Development ("OECD") released a report titled *Illicit Trade: Trends in Trade in Counterfeit and Pirated Goods*, which provides a comprehensive, "quantitative analysis of the value, scope and magnitude of world trade in counterfeit and pirated products."[6] The report demonstrates the complex issues with tracking and identifying counterfeit goods. The problem is only compounded as "parties that engage in the trade of counterfeit and pirated products tend to ship infringing products via complex routes, with many intermediary points... to facilitate falsification of documents in ways that camouflage the original point of departure, establish distribution centers for counterfeit and pirated goods, and repackage or re-label goods."[7] This often makes it nearly impossible for external experts, and even trained government officials, to spot counterfeit goods.

Efforts to stem the flow of counterfeit goods should not focus solely on online marketplaces. To protect consumers, any proposal must also take into account the dominant role that physical marketplaces continue to play, and should also be directed at the sources of counterfeits manufacturing.

II. IA'S MEMBERS INVEST MILLIONS OF DOLLARS A YEAR TO COMBAT COUNTERFEITING

Nobody benefits when counterfeit goods are sold online: not consumers, not online marketplaces or their users, and not trademark owners. IA's member companies depend on consumers' trust. Any suggestion that internet companies are uninterested in combating counterfeiting, or are inadequately incentivized to support enforcement efforts by brand owners and law enforcement agencies, is simply false.

Internet companies are thoroughly incentivized to help brands combat intellectual property crimes, because they depend on consumer and brand trust to succeed. People who are duped into purchasing fake goods through a particular online marketplace will vote with their dollars and shop elsewhere, and brand owners will refrain from entering into partnerships with services that fail to take counterfeiting seriously.

As a result, IA members have made protecting consumers from counterfeit goods a top priority, investing millions of dollars a year in these efforts, and going far beyond what the law requires to collaborate with brand owners and others

[2] Christopher Hooton, *Measuring the U.S. Internet Sector: 2019,* Internet Association (Sept. 26, 2019), https://internetassociation.org/publications/measuring-us-internet-sector-2019/

[3] Nina Angelovska, *Top 5 Online Retailers: 'Electronics and Media' Is The Star of E-commerce Worldwide*, Forbes (May 20, 2019, 11:45 AM), https://www.forbes.com/sites/ninaangelovska/2019/05/20/top-5-online-retailers-electronics-and-media-is-the-star-of-e-commerce-worldwide/

[4] *The Effects of Foreign Product Counterfeiting on U.S. Industry*, United States International Trade Commission, at ix (Jan. 1984), https://www.usitc.gov/publications/other/pub1479.pdf ("Of a total of 274 responses, 82 were affirmative.").

[5] *See, e.g.*, *Luxottica Grp., S.p.A. v. Airport Mini Mall, LLC*, 932 F.3d 1303 (11th Cir. 2019) (contributory trademark infringement case against the owners of a mall); *Coach, Inc. v. Goodfellow*, 717 F.3d 498, 499 (6th Cir. 2013) (contributory liability case against a flea market operator).

[6] *Illicit Trade: Trends in Trade in Counterfeit and Pirated Goods*, OECD, at 11 (Mar. 18, 2019), https://www.oecd-ilibrary.org/docserver/g2g9f533-en.pdf?expires=1608660670&id=id&accname=guest&checksum=ADC423225FD0EB5F444F7F5BE78CD0E3.

[7] Id.

to stem the flow of counterfeits. IA member companies have taken the lead by implementing clear policies, proactively creating transparent and innovative counterfeit reporting and prevention tools that allow third parties to identify counterfeit items listed for sale on their online marketplace and remove them in a timely manner.

Internet services have also developed close relationships with law enforcement to combat counterfeit goods, including active engagement with the U.S. Customs and Border Protection, the National Intellectual Property Rights Center, and other federal and state enforcement agencies. Services regularly report misconduct and respond to ongoing law enforcement investigations, and several have proactively created training programs to ensure that law enforcement officials understand how their services work, and to provide information about evolving internet-based investigative techniques, and other emerging trends. IA member companies also encourage users to report illegal activities to appropriate authorities and have created links to facilitate such reporting.

IA's members have implemented transparent and innovative practices. The following are a few examples, but IA could list many more.

A. Amazon

Amazon strictly prohibits the sale of counterfeit products, invests heavily in prevention, and takes proactive steps to reduce the number of counterfeits offered in Amazon's online stores to zero. In 2020, Amazon's global proactive efforts successfully prevented over 6 million suspected bad actor accounts from offering a single product for sale in their stores and blocked over 10 billion suspected bad listings from being published on its stores. Fewer than 0.01% of all products sold on Amazon received a counterfeit complaint from customers. Those complaints were investigated for accuracy and acted upon as appropriate. Every claim of potential counterfeit is investigated thoroughly, and in the rare instance where a bad actor gets through, Amazon takes swift action, including removing the allegedly infringing items, permanently banning bad actors, pursuing legal action, and working with law enforcement when appropriate.

In 2017, Amazon launched Brand Registry, a free service that gives a brand owner— regardless of whether they sell in Amazon's store—access to a set of powerful tools that help them manage and protect their brand and intellectual property rights. More than 500,000 brands were enrolled in Brand Registry in 2020, and on average, they reported 99% fewer suspected infringements than before the launch of the service.[8]

In 2018, Amazon launched Transparency, a serialization service that protects each individual product unit. Brands apply a unique 2D code, similar to a QR code, to their products, and Amazon scans the code to verify authenticity before shipping it to a customer. In 2020, more than 15,000 brands were using Transparency, and the service has enabled the protection of more than 500 million product units.

Additionally, Amazon's Project Zero provides brands with the ability to directly remove counterfeit product listings from the store in near real-time. In 2020, there were more than 18,000 brands enrolled in Project Zero. For every listing removed by a brand through the self-service counterfeit removal tool, automated protections removed more than 600 listings through scaled technology and machine learning that proactively addresses potential counterfeits and stops those listings from appearing in the store.

Other programs like IP Accelerator, the Utility Patent Neutrality Program, and the Counterfeit Crimes Unit have also recently launched to attack the issue from multiple angles. In short, Amazon's policies and innovative tools help customers feel confident in their purchases on Amazon stores.

B. eBay

As threats against consumers and rights holders evolve, eBay continuously seeks to improve its efforts to fight against counterfeiters and bad actors. eBay invests millions of dollars annually to fight unlawful listings, proactively deploying

[8] *Amazon brand registry*, Amazon, https://brandservices.amazon.com/ (last visited Dec. 22, 2020).

sophisticated technologies and investing heavily in partnerships with rights holders and governments across the globe to help protect consumers and support rights holders against bad actors. eBay partners with more than 40,000 rights holders through its Verified Rights Owner (VeRO) program, which allows rights holders to quickly and easily report instances of alleged intellectual property infringement.[9] eBay also works closely with governments and law enforcement around the globe to help ensure the safety of consumers and protect rights holders.

In addition to those partnerships, eBay has multiple teams and tools in place focused on enforcing its policies and proactively identifying and addressing any generally suspicious or potentially harmful seller behavior. These efforts help eBay flag and remove potentially problematic sellers, including sellers of counterfeit goods, or prevent these harmful actors from obtaining an eBay account in the first place. eBay's policies, teams, partnerships, and tools help create a global commerce platform that enables sellers, including hundreds of thousands of American entrepreneurs and small businesses, to sell their inventory, and buyers to find and purchase items, virtually anytime and anywhere. eBay's core purpose, since its founding in 1995, is to safely connect buyers and sellers through its marketplace and help American entrepreneurs, including small and micro-businesses, reach markets around the world. eBay's commitments to consumer safety and rights owner protection are longstanding and are at the center of its corporate values.

C. Etsy

Etsy is committed to maintaining an environment that promotes trust and safety for its vibrant community of buyers and sellers. When sellers open a shop on Etsy, they agree to Etsy's Seller Policy,[10] which outlines their rights as well as the platform's expectations. This includes adhering to the Prohibited Items Policy, which asks users to consider the safety of others when listing goods. Beyond Etsy's seller policies, it also seeks to reinforce appropriate product safety practices, which are reflected in its Product Safety Pledge.[11]

In 2020, Etsy received close to 4 million flags regarding potentially noncompliant listings, a 400% increase in flags from 2019; breaches of its handmade policy were among the most commonly flagged violations. This increase is in large part due to the exponential growth of the marketplace last year. The vast majority of flags were generated by Etsy's internal automated systems and our enforcement scaled with the marketplace. In 2020, 20% of shop and listings flags came from users in comparison to the 80% generated from our tools — a proportion that remained consistent with 2019. Overall, Etsy saw a 58% increase in the number of intellectual-property related takedowns compared to 2019.[12]

In addition to upholding Etsy's commitment to transparency, it has worked to scale its policy enforcement resources, allowing it to better detect and remove prohibited items. In the last two years, Etsy has nearly doubled the size of its Trust & Safety team, adding more monitoring capabilities. This includes growing its Content Moderation team by five times (5x) and adding a new Handmade & Counterfeit team dedicated to fighting counterfeits and handmade violations.

Since the beginning of last year, Etsy has significantly increased its investments in Trust & Safety technology, including building a dedicated trust and safety machine learning engineering team and exploring computer vision technology, with the goal of using powerful algorithms to drive improvements in the precision of automated risk detection. Etsy has taken steps to ensure that Etsy sellers are positioned for success by making its policies easy to understand, refining its violation notification process, and providing resources so that sellers can get help when they have questions about their compliance.[13]

---

[9] *Verified Rights Owner Program*, eBay, https://pages.ebay.com/seller-center/listing-and-marketing/verified-rights-owner-program.html (last visited Dec. 22, 2020).

[10] Etsy's Seller Policy. https://www.etsy.com/legal/section/sellers

[11] Product Safety Pledge. https://medium.com/etsy-impact/etsy-joins-eu-product-safety-pledge-46e22b608eea

[12] Etsy 2020 Transparency Report. https://blog.etsy.com/news/2021/etsy-releases-2020-transparency-report/

[13] https://blog.etsy.com/news/2021/our-commitment-to-the-trust-and-safety-of-the-etsy-marketplace/

D. Facebook

As part of its IP protection program, Facebook has established dedicated channels for rights holders to report infringing content, including a specific counterfeit channel.[14] Reports of alleged infringement are handled by a global IP Operations team that provides around-the-clock multilingual coverage, promptly removing reported content—often within minutes. Facebook's Commerce & Ads IP Tool goes further, offering enrolled rights holders a streamlined interface to easily identify and report infringing content. Built based on rights holder feedback, the tool provides the ability to search text and images and to report counterfeit, trademark or copyright infringement in ads on Facebook or Instagram, Shops content, Instagram posts with product tags, Marketplace posts, and group sale posts.[15] Facebook also maintains comprehensive repeat infringer policies to disable profiles, pages, and groups on Facebook, along with accounts on Instagram, where appropriate.

Additionally, IP infringements are strictly prohibited in Facebook's and Instagram's respective Terms of Service and Terms of Use,[16] as well as more specialized policies relating to ads[17] and commercial posts.[18] Consistent with these policies, Facebook has collaborated closely with rights holders and invested heavily to build numerous measures to combat counterfeits. This enforcement is done both in response to rights holders' IP reports as well as proactively—that is, before a rights holder ever needs to see an infringement and often before it even goes live. As part of its commitment to making its platforms safer for people and businesses to connect, share, buy, and sell, in 2019 Facebook launched a new dedicated website[19] describing its range of IP protection and anti-counterfeiting measures.

Facebook has launched several other proactive measures that target counterfeits. These include a pre-publication review of ads and Marketplace posts, that uses technologies such as artificial intelligence and machine learning to identify suspicious indicators like keywords and discounts and, based on these indicators, to proactively block suspected counterfeits before they go live. Facebook also takes measures proactively to disable and/or reduce the visibility of suspected counterfeits on its organic products as well, such as Facebook Pages and groups, and Instagram content, hashtags, and accounts. In May 2021, Facebook published its semiannual Transparency Report,[20] which for the first time included data relating to the amount of content it removes proactively as potentially infringing IP rights. Notably, the data show that from July to December 2020, the vast majority of content Facebook took action on for counterfeit-related violations was removed proactively.

III. BRAND OWNERS AND ONLINE SERVICES MUST WORK TOGETHER TO APPROPRIATELY ENFORCE ANOTHER COMPANY'S TRADEMARKS

Anyone who has enforced IP rights can tell you that identifying counterfeit goods can be difficult - if not impossible - unless you have a high level of expertise and familiarity with the brand and products that are being counterfeited. Trademark owners often hire employees and consultants who are solely focused on expertly identifying the subtle differences between genuine products and counterfeits in support of their enforcement efforts. These individuals work with a host of federal, state, and local agencies, including the U.S. Department of Justice ("DOJ"), U.S. Customs and Border Protection ("CBP"), and state and local police departments, as well as district attorneys' offices that have staff

[14] *Counterfeit Report Form*, Facebook, https://www.facebook.com/help/contact/counterfeitform (last visited Dec. 22, 2020); *Counterfeit Report Form*, Instagram, https://help.instagram.com/contact/instagramcounterfeitform (last visited Dec. 22, 2020).

[15] https://www.facebook.com/business/help/828925381043253?locale=en_US

[16] *Terms of Service*, Facebook, https://www.facebook.com/terms.php (last visited Dec. 22, 2020); *Terms of Use,* Instagram, https://help.instagram.com/581066165581870 (last visited Dec. 22, 2020).

[17] *Advertising Policies*, Facebook, https://www.facebook.com/policies/ads (last visited Dec. 22, 2020);

[18] *Commerce Policies*, Facebook, https://www.facebook.com/policies/commerce (last visited Dec. 22, 2020).

[19] *How Facebook helps protect against counterfeits*, Facebook for Business, https://www.facebook.com/business/tools/anti-counterfeiting/guide (last visited Dec. 22, 2020).

[20] *Intellectual Property Transparency Report,* https://transparency.facebook.com/intellectual-property (last visited May 25, 2021).

dedicated to enforcing criminal anti-counterfeiting laws.[21]

Regardless of whether enforcement activities are occurring online or offline, U.S. trademark law puts the onus of identifying counterfeit goods on those who have the requisite expertise to accurately perform that task: brand owners and their agents. Brand owners are in the best position to know when a product being sold online is counterfeit; online services cannot have expertise in every trademark. For example, online services don't know whether a particular seller is authorized by the brand owner or not, nor whether a listing for a product depicts a counterfeit product. Indeed, identifying counterfeits based on the quality, design and specifications of a product is often, if not exclusively, within the expertise of the brand itself. Further, since many online services never possess the counterfeit goods, they cannot examine the goods for obvious signs of counterfeiting, even if such signs were known to them. Nor would they know what to look for concerning any particular problem. And as hard as detecting counterfeiting is for large companies, that problem is even worse for small- and medium-sized companies, who cannot afford to build systems to police all possible counterfeiting on their sites.

However, it would be a mistake to conclude that online services can get off scot-free anytime a counterfeit product is sold via their services. On the contrary, even though identifying counterfeit goods can be incredibly difficult for anyone other than a trademark owner—especially online services which might never come into physical contact with the products—the law today does not exempt an online service from liability where a service knows that a particular listing is infringing, or where a service is willfully blind to infringing listings. IA's members have invested heavily in developing collaborative and productive relationships with brands across industries and around the world, and worked cooperatively with brand owners to take down infringing listings and make the online environment as safe as possible for consumers.

Accordingly, existing trademark law protections, coupled with the natural incentive to maintain a trustworthy environment for consumers and business partnerships, encourage online service providers to work proactively to support enforcement by brand owners and remove listings for counterfeit products whenever they are identified.

IV. REMOVING PROTECTIONS FOR ONLINE SERVICE PROVIDERS IS NOT THE SOLUTION TO THE COUNTERFEITING PROBLEM.

Changing the secondary liability standards, as SHOP Safe does, will not address the true cause of counterfeiting—the actual infringer. A company that delivers the products consumers order from third parties may have no way to know whether the third-party seller of those products, in turn, bought them from a legitimate supplier. Cloud storage companies have no way to tell whether documents stored on their sites violate a third party's trademark rights. But all could be subject to incredibly onerous obligations if this overbroad legislation becomes law.

Instituting a strict legislative regime could backfire. Currently, online services are working cooperatively with rights holders and the government to stop counterfeiting; but in the face of a legislative mandate, companies may hesitate to do anything other than what the law requires to avoid the risk of future liability. For example, companies may not explore alternative counterfeiting solutions, even if those solutions would ultimately be *more* effective at getting counterfeits off of the internet than the legislative framework. That would help nobody—not the brand owner, not the online service, and not the consumer. People who commit intellectual property crimes are adept at adjusting their sales and distribution methods to evade detection as intellectual property enforcement techniques improve. Because enforcement can be such a cat-and-mouse endeavor, flexibility and good faith collaboration, not legislative mandates, are most likely paths to effective solutions.

There is no one-size-fits-all solution for all of these companies. Trying to create one would effectively penalize companies for counterfeiting activity that they cannot reasonably detect or control. For example, a search engine

[21] *See, e.g.*, U.S. Dep't of Justice Office of Public Affairs, *22 Charged With Smuggling Millions of Dollars of Counterfeit Luxury Goods From China Into the United States*, Justice News (Aug. 16, 2018), https://www.justice.gov/opa/pr/22-charged-smuggling-millions-dollars-counterfeit-luxury-goods-china-united-states.

merely indexes web pages a webmaster has designated as searchable in the search index. It indexes trillions of web pages and has no direct contact with the seller of the counterfeit item. It would make no sense to hold the search engine liable if, after running a search, a user purchases a counterfeit item from the site of an unrelated third party.

Payment processors are another example. Payment processors offer services that individuals may use to facilitate the purchase of counterfeit goods, but they are neither the seller nor the buyer of the goods at issue, and they generally have no visibility into whether the underlying payment is for a product or a service, much less whether a product is genuine or counterfeit. Yet payment processors who have done nothing more than unknowingly process payments to infringers have *already* faced lawsuits[22]—and at least one judge would have allowed a case to go forward merely because he concluded that the allegedly infringing website could not "operate without the use of credit cards."[23]

Changing the secondary liability standards also does not address the true cause of counterfeiting—the actual infringer. Although several U.S. agencies have the authority to investigate criminal counterfeiting (as noted above), only 229 counterfeiters were referred to the U.S. Sentencing Commission in the 2019 fiscal year.[24] Indeed, the U.S. Sentencing Commission reported that counterfeit offenses *decreased* by 37.4 percent between the Fiscal Year 2015 and Fiscal Year 2019.[25] But law enforcement agencies—not online services—have the expertise and mandate to investigate criminal counterfeiting. Accordingly, IA respectfully suggests that it might be more impactful to focus legislative efforts on increasing resources allocated to agencies that are charged with investigating and enforcing existing laws against the counterfeiters themselves (an effort that IA's members are already helping with) than to change the standards for secondary liability.

Another key issue not addressed is that while most brand owners act in good faith, some abuse the system. For example, brand owners have brought trademark infringement lawsuits to stop the sale of parody products,[26] or labeled as counterfeiting the resale of their genuine branded products to control distribution channels in contravention of perfectly legal and valid commercial activity as to authentic goods.[27]

In addition, so-called "trademark bullying" is a well-recognized problem. Trademark bullies are brand owners (often large companies) who use the threat of trademark infringement lawsuits to pressure smaller companies or individuals to stop engaging in lawful activity that the brand owner does not like.[28] Trademark bullying reduces competition and harms free speech, imposing real costs on both companies and consumers.[29] Because smaller companies and individuals lack the resources to fight a large brand owner, they are often forced to comply with the brand owner's demands, no matter how frivolous.[30] Changing the secondary trademark liability standards could make bullying

[22] *See, e.g.*, *Gucci Am. v. Frontline Processing Corp.*, 721 F. Supp. 2d 228 (S.D.N.Y. 2010) (lawsuit brought by Gucci against companies who provide online credit card processing services); *see also Nike, Inc. v. Wu*, No. 13 Civ. 8012 (CM), 2020 WL 257475 (S.D.N.Y. Jan. 17, 2020) (motion brought by Nike to hold banks in contempt based on their failure to comply with asset restraints imposed by the court on defendant counterfeiters and those acting "in concert or participation" with the counterfeiters).

[23] *See Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788, 806–808 (9th Cir. 2007); *id.* at 822–823 (Kozinski, J., dissenting).

[24] *See Quick Facts: Counterfeit Offenses,* U.S. Sentencing Commission, https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Counterfeiting_FY19.pdf (last visited Dec. 22, 2020).

[25] *Id.*

[26] *See, e.g.*, *VIP Prod. LLC v. Jack Daniel's Properties, Inc.*, 953 F.3d 1170 (9th Cir. 2020) (declaratory judgment case brought by the maker of "Bad Spaniels" dog toy following a cease and desist letter sent by Jack Daniels); *Louis Vuitton Malletier S.A. v. Haute Diggity Dog, LLC*, 507 F.3d 252 (4th Cir. 2007) (lawsuit brought by Louis Vuitton against the maker of the "Chewy Vuiton" dog chew).

[27] *Williams-Sonoma, Inc. v. Amazon.com, Inc.*, Case No. 3:18-cv-07548-EDL, Dkt. No. 39 at 9 (N.D. Cal. May 2, 2019) (denying Amazon's motion to dismiss in a case brought by Williams-Sonoma but observing that Williams-Sonoma's theory that Amazon had set up a counterfeit Williams-Sonoma website was not plausible).

[28] *See, e.g.*, Irina D. Manta, *Bearing Down on Trademark Bullies*, 22 Fordham Intellectual Prop. Media & Entm't L. Journal 853 (2012); Leah Chan Grinvald, *Shaming Trademark Bullies*, 2011 Wis. L. Rev. 625 (2011).

[29] Leah Chan Grinvald, *Shaming Trademark Bullies*, 2011 Wis. L. Rev. 625, 650–653 (2011).

[30] *See id.* at 645–649.

behaviors worse.

Combating counterfeiting is incredibly important. But so is ensuring the continued availability of online commerce to many individuals and small businesses that depend on it as a core source of their income. The goal of the law must be to balance those concerns.

V. UNINTENDED ISSUES WITH THE SHOP SAFE ACT

The SHOP Safe Act establishes that an electronic commerce platform shall be liable for contributory trademark infringement by a third-party seller of goods that "implicate health and safety" unless the platform takes certain actions. In addition to the fact that almost any product could "implicate health and safety" as that phrase is defined in the bill text, several other provisions included in the language would impose unworkable compliance obligations. While IA strongly encourages the committee to confer with individual e-commerce platforms to discuss their specific concerns with the legislation, we have included a non-comprehensive list of examples of unintentional problems the SHOP Safe Act would create.

The bill would require platforms to verify the identity of each third-party seller, presumably using government identification that the platforms are not in a position to physically inspect or properly verify. They would also be required to investigate and periodically confirm the physical address of each seller or their US-based registered agent to determine that the address exists and, presumably, its nexus to the seller.

The SHOP Safe Act would create significant and unreasonable impediments for small and "micro" businesses that rely on platforms to sell and resell products to other businesses and consumers. The bill would make it difficult for such businesses to use trademarks to describe the products they are offering, by requiring platforms to use reasonable technological tools to scan nearly every third-party listing or advertisement that includes a trademark, and to rely on such automated processes to make determinations that brand-trained experts are expected to make in every other legal context, including in alleging copyright infringement under the DMCA. Technology is not perfect, and by threatening platforms with legal liability if they fail to take action to remove potential "false positives," the bill would incentivize overenforcement at a potentially massive scale. The bill would also require companies to impose punitive consequences on sellers who have used trademarks that are presumed to be counterfeit—including permanently banning them from the platform, but the draft language is remarkably devoid of any semblance of due process to allow sellers to confront brand owners and assert that their use of a trademark was valid.

There are several additional problems with the legislation that should be reviewed. The bill includes a provision that would appear to require platforms to prevent any sellers who have been terminated—regardless of whether the termination is related to the use of counterfeit trademarks—from rejoining or remaining on the platform. The legislation indicates that platforms must determine that sellers have designated a registered agent in the U.S. or risk facing liability. This could be quite burdensome, requiring periodic searches of various secretary of state registries. Another new provision states that "reasonable awareness [of counterfeits/IP infringements]. . . may be inferred based on information regarding the use of a counterfeit mark on the platform generally, general information about the third-party seller, identifying characteristics of a particular listing, or other circumstances as appropriate."[31] This clarification is highly problematic in that it essentially defines constructive knowledge in terms of general knowledge, which is the opposite of how the law had previously handled it.

Finally, the legislation would introduce unnecessary confusion into the Lanham Act by establishing requirements that are, in some cases, unhelpfully specific, and in other cases concerningly broad and vague. The legislation targets only one sector even though its goal is to address an economy-wide problem that requires all stakeholders to work together in good faith to stop bad actors. The bill also "requires each third-party seller to use images that the seller owns or has permission to use." IA members already prohibit sellers from using images that they do not have rights to use, but the unlawful use of copyrighted images is already covered by the DMCA, and adding copyright protections into a trademark

[31] SHOP Safe. See (a)(4)(A)(ix). https://judiciary.house.gov/uploadedfiles/shop_safe_act_bill_text.pdf (last visited May 26, 2021).

law could create confusion between the two statutes with no added benefit. The bill also fails to precisely define the term "electronic commerce platform." The definition of that term is so vague that it would include websites well beyond online marketplaces including social media platforms, discussion communities, cloud services, video chat services, and even email service providers. If the scope of the bill is intended to be that broad, it would be difficult for many of the impacted companies to comply with several of the enumerated obligations.

VI. CONCLUSION

IA appreciates the opportunity to provide comments on behalf of its member companies and to highlight some of the proactive policies they have implemented. IA's member companies share the Subcommittee's goal of promoting consumer health and safety, which is why they have created a range of tools and programs to help brand owners police the misuse of their trademarks, and developed strong working relationships with law enforcement officers who investigate and prosecute intellectual property crime. IA strongly encourages the committee to work with individual e-commerce platforms to talk through concerns with the SHOP Safe Act. The internet industry looks forward to continuing to engage with the Subcommittee members on these matters in the future.