How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces

By Sujai Shivakumar | March 2021

Counterfeits—fake goods that infringe on the intellectual property of legitimate businesses—harm consumers, businesses, and the economy. Addressing the proliferation of counterfeits in online marketplaces will require better collaboration between stakeholders in government and industry. To foster these efforts, U.S. policymakers should amend existing laws and regulations that limit stakeholders from sharing data and establish a data sharing partnership to use advanced analytics to disrupt counterfeiting networks. If successful, these efforts could substantially reduce counterfeit imports, creating an additional 15,000 to 20,000 manufacturing jobs in America.

INTRODUCTION

Counterfeits—fake goods that infringe on the intellectual property (IP) of legitimate businesses—threaten the health and safety of U.S. consumers, lower public confidence in businesses and markets, harm U.S. innovation and economic growth, and unfairly prop up Chinese economic growth. When counterfeiters, most of whom are located in China, fraudulently misrepresent themselves as the manufacturers of products and as brand sellers, the legitimate manufacturers suffer financial and reputational losses—including job losses—while consumers are harmed by being sold knockoffs they believe to be reliable and legitimate products.
While brand sellers, online marketplaces, and law enforcement agencies all share an interest in stopping counterfeits, their efforts to detect and prevent their sale remain siloed and uncoordinated. Counterfeiters are strategic, adaptive, and opportunistic—and often evade these countermeasures.

The need for a coordinated approach to counterfeiting has become more urgent as the number of Americans shopping online continues to grow. The U.S. Government Accountability Office (GAO) recently found that “the growth in e-commerce has contributed to a shift in the sale of counterfeit goods in the United States, with consumers increasingly purchasing goods online and counterfeiters producing a wider variety of goods that may be sold on websites alongside authentic products.” Similarly, a 2020 report by the Office of the U.S. Trade Representative observes that “the rapid growth of e-commerce platforms has helped fuel the growth of counterfeit and pirated goods into a half trillion-dollar industry. This illicit trade has an enormous impact on the American economy by eroding the competitiveness of American workers, manufacturers, and innovators.” In addition, this illicit trade has an enormous positive impact on the Chinese economy, both by eroding the competitiveness of their U.S. competitors, and by providing revenue to a wide array of Chinese companies.

This proliferation of counterfeits has accelerated during the COVID-19 pandemic. As they practice social-distancing, consumers are shifting to e-commerce platforms to purchase essentials such as food, medicines, and personal protective equipment as well as non-essentials like cosmetics, household products, and children's toys. Counterfeiters see this shift in shopping habits as a growth opportunity and are taking advantage of e-commerce platforms to distribute fake products to American consumers.

To better address this vulnerability, the Customs and Border Protection Agency (CBP) at the Department of Homeland Security (DHS) should help establish a public-private partnership to share information across brand sellers, online marketplaces, and U.S. enforcement agencies—and foster data-driven strategies to both reduce the spread of fake goods and disable counterfeit networks.

Congress should direct CBP to use its authority in the 2015 Trade Facilitation and Trade Enforcement Act (TFTEA) to establish such a partnership through the National Intellectual Property Rights Coordination Center (IPR Center). A well-crafted data-sharing partnership could staunch the harm from counterfeiting and exploit advances in data analytics and artificial intelligence (AI) to identify and respond to the strategies and tactics of counterfeiters. Congress should also promote the needed coordination among brand sellers, online marketplaces, and enforcement agencies by removing legal
impediments to cooperation concerning the creation of common standards for data collection and analysis.

If these efforts could cut counterfeit goods imports by 50 percent, it would create an additional 15,000 to 20,000 manufacturing jobs in America, while at the same time reduce the trade deficit. In this regard, expanding funding for federal agencies to fight counterfeit imports could very well be a cost-efficient strategy while offering a World Trade Organization (WTO)-legal way to defend against Chinese mercantilist practices.

COUNTERFEITING IS GLOBAL, PERVASIVE, AND ADAPTIVE

Counterfeiting is increasingly a resilient, globally networked operation. According to the Organization for Economic Cooperation and Development (OECD), the volume of international trade in counterfeit and pirated products in 2016 amounted to $509 billion, representing 3.3 percent of world trade. Common counterfeited goods include footwear, clothing, leather goods, electrical equipment, watches, medical equipment, perfume, cosmetics, toys, jewelry, and pharmaceuticals.

CBP seized 27,599 shipments of goods that violated IP rights in fiscal year 2019. The retail value of these counterfeit goods amounted to $1.5 billion, meaning that the seized goods would retail for that much if they were actually real. Of course, only a portion of all counterfeit shipments are interdicted.

Forty-eight percent of the pirated goods seized by U.S. customs originate in China, and a further 35 percent come from Hong Kong. While counterfeit and pirated goods originate from virtually all economies in all continents, as much as 86 percent of all globalcounterfeits originate in China. It is also important to realize that a significant share of counterfeits from China do not come from underground organizations—they come from companies operating openly. Previous analysis also indicates that the People’s Liberation Army has owned counterfeit businesses in order to supplement its government budget.

Organizations that manage the manufacture and distribution of counterfeit goods exploit the complexity and efficiency of modern supply chains to bring fake goods to consumers, either in brick-and-mortar stores or through e-commerce. Counterfeiter organizations ship their sham products via complex trade routes using several transit points in order to hide information about the original point of production. To further obscure the provenance of counterfeits, they often label goods with imitation logos and place them in trademark-infringing packages in third countries. Such practices make it particularly difficult for CBP inspectors to trace counterfeits to the country of origin.

Counterfeitors also exploit the procurement and distribution networks of online marketplaces such as AliExpress, Amazon, eBay, Etsy, Facebook,
Walmart, and Wish to sell fake goods to consumers. They also take advantage of the aura of authenticity and trust that online platforms provide. An online marketplace is an e-commerce site wherein multiple third parties sell their products. Consumers make purchases on these sites, and the marketplace operator passes the orders along to the sellers. Marketplace operators typically offer additional services to sellers, such as allowing them to advertise their products and handle order fulfillment. Sellers gravitate toward online marketplaces because they have large customer bases, and using an online marketplace eliminates the need for sellers to build their own ecommerce websites. Counterfeiters further complicate enforcement efforts by rapidly proliferating on third-party online marketplaces, hopping from one seller profile to the next even if the original posting is taken down or blocked. Online marketplaces are a significant source of counterfeit goods. In 2017, 39 percent of unwitting purchases of counterfeit goods globally were through online marketplaces.\textsuperscript{14}

Counterfeiters are tapping into the surge in packages being imported into the United States, including through online marketplace procurement networks. Between 2013 and 2019, the number of small packages imported into the United States via express carriers nearly doubled, and the number imported via international mail more than tripled.\textsuperscript{15} Between 2000 and 2018, seizures of infringing goods at U.S. borders increased 10-fold, from 3,244 seizures per year to 33,810. The sheer volume and distributed nature of this flow of products is straining the ability of e-commerce companies and law enforcement agencies to identify and remove the counterfeits.\textsuperscript{16}

**COUNTERFEITS CAUSE HARM TO CONSUMERS, BUSINESSES, AND THE ECONOMY**

The volume of counterfeiting activities causes actual harm to U.S. businesses and their workers. As fakes—ranging from common consumer goods to business-to-business products to luxury items such as fashion apparel and deluxe watches—make their way to consumers, they hurt sales of legitimate products, damage the brand value of sellers, and taint reputations of online marketplaces.

Fake medications and personal protective equipment peddled by counterfeiters are particularly pernicious and can cause injury, threatening the health and safety of Americans. In February 2021, for example, in the midst of the COVID-19 pandemic, federal agents seized approximately 10 million Chinese-made counterfeit N95 face masks bearing the 3M logo. In announcing the seizure, Steve Francis, director of the Intellectual Property Center for DHS’s Homeland Security Investigations unit, urged thousands of hospitals and medical facilities to stop using the suspected fakes, adding that “they are providing a false sense of security to our first-line responders and to the American consumers.”\textsuperscript{17}
By diverting sales away from the purchase of legitimate products, counterfeits also damage U.S. firms and workers. Counterfeits not only represent lost revenue for legitimate businesses, but they also siphon the rewards of innovation and entrepreneurship and shift production and service jobs away from the legitimate owners of the IP. Overall, U.S. sales of tangible counterfeit goods are estimated to between $29 billion to $41 billion per year.\textsuperscript{18} Assuming the number is closer to $40 billion, and that closer partnerships with manufacturers, sellers, and the federal government could reduce that number to $20 billion, that could lead, by a rough calculation, to the creation of approximately 15,000 to 20,000 more U.S. manufacturing jobs.\textsuperscript{19}

CURRENT ANTI-COUNTERFEITING EFFORTS

Brand sellers, online marketplaces, and law enforcement agencies are all pursuing strategies to address counterfeits.

Strategies of Brand Sellers

In their war against counterfeits, brand sellers are investing in a variety of defensive measures. The luxury industry, notably, is seeking to combine advances in AI with massive data feeds in order to monitor the flow of their products through supply chains and identify intrusions.\textsuperscript{20} This battle is also encouraging innovation. One potential application, for example, uses machine learning algorithms on microscopic images of physical objects to distinguish between genuine and counterfeit versions of the same product.\textsuperscript{21}

Another strategic option for some luxury brand sellers is to reassert direct control over production runs and distribution networks. As one analyst noted, “If they bring manufacturing back to their home countries, where stricter controls are easier to implement, Louis Vuitton, Gucci, and Burberry can better control supply and distribution issues that have facilitated counterfeiters.”\textsuperscript{22} With closer vigilance, brand sellers could more easily prevent the distribution of these counterfeit goods to consumers.

Moreover, after decades of offshoring production, some manufacturers are rediscovering the advantages of colocating research, development, production, and marketing within their own regional economic ecosystems.\textsuperscript{23} Some brand sellers find that closer geographic integration is an effective way to link evolving consumer preferences in home markets (e.g., for “green” renewable and biodegradable products) while sustaining local manufacturing know-how. In this way, luxury makers could also advertise regional heritage and local traditions of craftsmanship as a part of their brand appeal.\textsuperscript{24}

Strategies of Online Marketplaces

Seeking to preserve their own reputation and maintain customer trust, online marketplaces are using a variety of methods to address counterfeits on their platforms.
AliExpress

AliExpress is an online marketplace owned by the Alibaba Group that directly connects Chinese manufacturers and distributors with buyers around the world. According to the company, Alibaba has invested significantly to address the concerns various rights holders have raised regarding the prevalence of pirated and counterfeit products on the site, “including through the development of cutting-edge proactive and reactive IPR enforcement technology, the creation of institutionalized coordination and consultation mechanisms targeted at both large and small rights holders, and cooperation with law enforcement.”

Amazon

Amazon, the world’s largest online marketplace, has declared that it views “counterfeiting as an existential threat—if customers do not trust what they purchase through Amazon’s stores, they can and will shop elsewhere.”

One thrust of Amazon’s strategy is to deploy AI to protect brand sellers. Its Project Zero initiative utilizes machine learning to “proactively and continuously scan more than 5 billion attempted daily product listing updates globally to look for suspicious listings.” Once alerted, registered brand sellers can then directly remove illicit products from Amazon’s marketplace. Not only does this machine learning model check text and images of logos from third-party sellers for discrepancies that reveal fraud, but it could also combine patterns found from scans with information tracked from customer reviews and behaviors, as well as from movements in social media postings, to produce predictive heuristics about counterfeit placements on Amazon’s online marketplace.

Amazon also partners with brand sellers to thwart counterfeits. Launched in 2017, Amazon’s Brand Registry collects specific data about branded products, including images of logos and other identifying characteristics, and information on countries wherein the brand sellers manufacture and distribute their products. The over 350,000 brands worldwide now participating in this registry can use this database to search Amazon’s stores and report products that infringe on their IP. Upon receiving an alert, Amazon can investigate and follow up by variously removing the product from sale, destroying the inauthentic merchandise, terminating the seller’s account, referring the case as applicable for civil or criminal prosecution, or some combination of these options.

Indeed, Amazon is intensifying its efforts to prosecute criminals involved in the manufacture and distribution of counterfeits. In 2020, the company launched the “Counterfeit Crimes Unit” to bring together former federal prosecutors, experienced investigators, data analysts, and others to track down and prosecute counterfeiters. Working closely with brands such as Maison Valentino and the Department of Justice (DOJ) and DHS, the Unit has already
filed lawsuits and seized inventory from multiple sellers of counterfeit goods. In addition, Amazon now provides law enforcement and designated government entities quarterly reports of counterfeits they have detected and blocked from their stores.

eBay
Like other e-commerce companies, eBay is building up its internal defenses by investing in machine learning and other tools to help identify unlawful listings, including counterfeit goods, that appear on the company’s platform, and then quickly remove prohibited items and take actions against bad actors. Alongside, eBay has created a Verified Rights Owner (VeRO) program to allow IP rights owners to report listings of products that infringe on their copyrights, trademarks, or other IP rights. eBay also shares information with its customers and other e-commerce retailers that can help them identify bad products and actors as well as best-practices lessons based on its own anti-counterfeiting efforts.

Further, eBay supports law enforcement in their investigation of fraudulent sellers. Actively partnering with the IPR Center, eBay has referred to them a variety of cases over the past few years, in addition to making referrals to other partners such as the FBI and the U.S. Postal Inspection Service.

Etsy
Etsy’s online marketplace connects buyers with sellers offering handmade, vintage, custom, or unique products. Etsy has instituted a Legal Response and Enforcement team that reviews and responds to notices of alleged infringement on its site. Whenever a shop on Etsy is closed for infringement, the termination also applies to any other shops Etsy considers to be related to that seller—while also blocking any attempts to open new shops. In 2019, Etsy closed nearly 14,000 shops for repeat infringement (more than double the previous year). Of all the sellers whose items Etsy took down for IP infringement, 51 percent were in North America, 24 percent were in Europe, and 18 percent were in Asia.

Facebook
Users buy and sell with other people within their community on Facebook Marketplace. These people are “nearly exclusively individual sellers who exchange second-hand goods directly and off-platform, and who are subject to clear policies prohibiting counterfeiting in the first instance and subjected to measures taken to enforce those policies.” In addition to establishing terms of service and community standards for these individuals, Facebook also investigates and takes down products that violate its standards.

Facebook has also developed specialized tools to help rights holders effectively identify and report counterfeit content at scale. The company’s Commerce & Ads IP Tool allows rights holders to search across ads on
Facebook and Instagram, and listings and buy/sell groups on Facebook Marketplace, to report any infringements.

As with other online marketplaces, Facebook has invested in machine learning, AI, and other technologies to block or limit the distribution of potentially infringing content on Facebook and Instagram. Automated reviews compare Facebook Marketplace posts and other commerce listings against established commerce and advertising policies before they go live, including by incorporating signals of misleading, deceptive, or low-quality content such as posts that may be promoting counterfeit products. These signals include brand names, logos, keywords, prices, discounts, and other suspicious indicators.

**Walmart**

Walmart is taking a series of steps to keep counterfeits from appearing on its online marketplace. Its business model relies on a strategy of verification and transparency. The company has instituted a strong authentication process designed to vet third-party sellers before they can sell on in its marketplace. These third-party sellers are bound by a strict anti-counterfeiting policy that prohibits the sale of inauthentic products, and face documentation requirements for invoices and authorizations. In addition, at the point of purchase, Walmart provides its customers with the identity of both third-party sellers and shippers. Customers can also initiate complaints against third-party sellers, thereby triggering an investigation and the possible ejection of vendors found to be selling fakes. Walmart finds this vetting strategy effective, estimating that only 0.01 percent of items sold on its marketplace are counterfeits.34

Walmart also partners with brand sellers and government enforcement agencies to detect and punish fraud. For example, the company is working on a brand portal (similar in concept to Amazon’s Brand Registry) that would allow brand sellers to look up their own items and report the presence of counterfeits.

Walmart is considering an expansion of its data sharing strategy to combat counterfeit. The company has long leveraged the benefits of data sharing among its suppliers—integrating data from retailers and suppliers with information regarding customer behavior, pricing, and promotional data, as well as internal shipping and invoicing data—to drive new business insights, higher margins, decreased costs, and improved data accuracy.35 Walmart is also working more closely with law enforcement agencies in order to interdict counterfeit shipments coming into the United States and disrupt counterfeit networks.
Wish

Wish is an online marketplace connecting buyers to mostly Chinese and other international sellers. Wish uses a combination of software tools, AI, and human investigation to combat counterfeiting on its platforms. Wish’s merchants must complete a merchant-screening and onboarding process designed to help the company verify the identity and risks involved with particular merchants. Wish also works with IP rights holders, who can report suspected infringements for investigation. Its Brand Partner program gives brands and rights holders specialized access to the company’s platform in order to identify infringing products. In addition, Wish employs various automated detection processes, including machine learning automation and certain counterfeit-detection technologies, that take in vast amounts of information—including product images, titles, descriptions, and prices—to identify potentially infringing products at scale.36

While these companies have different business models, they are each making major investments to detect and remove fakes before they reach their platforms, cooperating with enforcement agencies, and working to better inform consumers about third-party sellers.

Strategies of Law Enforcement Agencies

While there are some 25 agencies across the federal government that are engaged to varying extents in efforts to monitor, deter, and prevent the importation and sale of counterfeit goods, CBP is the primary federal agency responsible for preventing goods that infringe U.S. copyrights, registered trademarks, and certain patents from entering the United States.37 This includes the operation of the National Targeting Center, which identifies IP rights violators and refers them for further investigation. CBP also partners with the private sector to conduct risk assessments of shipments, share specific industry standards with CBP field officers, as well as discuss emerging trends, technologies, and ways to cooperate on the enforcement of IP rights.

In addition to inspecting international shipping containers and air freight, CBP also cooperates with the U.S. Postal Service and international parcel courier companies to monitor individual shipments. Stepping up its inspection and monitoring efforts in this regard, CBP recently initiated Operation Mega Flex, which targets high-risk violators that are shipping and receiving illicit contraband through international mail facilities and express consignment hubs. Periodic “blitz operations” conducted under the auspices of Operation Mega Flex have examined thousands of parcels from China and Hong Kong and have cataloged the range of contraband seized.38

Even so, the sheer volume of small packages from overseas makes it difficult for customs officials to thoroughly identify counterfeit goods—and those goods below a de minimis threshold in declared value may not even receive routine
In addition, the priority for customs officials is often to interdict illicit drugs or weapons, rather than stop counterfeits. CBP is also home to the IPR Center, whose role is to coordinate diverse federal efforts related to interdiction, investigation, and outreach to the public and law enforcement. As a part of this effort, rights holders, online marketplaces, payment processors, and companies involved in all points across the supply chain regularly meet with members of the IPR Center to share their best practices, concerns, and suggestions. This information could enable further collaboration on complex cross-cutting challenges, including enhanced information sharing, joint enforcement actions, and specialized, targeted training and outreach. For example, Amazon’s new Counterfeit Crimes Unit is already sharing and analyzing data to assist targeted inspections by CBP aimed at preventing counterfeit products from entering the U.S. markets. Amazon is also working with the IPR Center to develop an “information exchange that will enable industry participants—stores, payment service providers, banks, and shipping companies—to better identify and stop counterfeiters before they can reach consumers.”

In addition to inspection and interdiction activities, CBP is working with other federal agencies to coordinate data sharing and analysis with brand sellers and online marketplaces in order to identify and stop the import of counterfeit goods. According to a 2020 DHS report, CBP is seeking to obtain statutory authority to create an e-commerce enforcement framework that, among other features, would allow CBP to seize discovered IPR-infringing goods (as is already allowed for narcotics).

The DHS report also anticipates the formation of an Anti-counterfeiting Consortium To Identify Online Nefarious actors (ACTION). ACTION would create a mechanism for sharing information within the consortium on sellers, shippers, and other third-party intermediaries involved in counterfeiting. ACTION members could also enter into memoranda of understanding with the IPR Center to clarify legal understanding supporting the sharing of data and IP enforcement going forward.

LACK OF COORDINATION UNDERMINES ANTI-COUNTERFEITING EFFORTS

Despite dedicated efforts by brand sellers, online marketplaces, and law enforcement agencies, counterfeiters continue to evade detection. As noted, counterfeiters use multiple merchant accounts, withhold their business information, and provide false information to CBP (this includes covering or obscuring infringing trademarks until the counterfeit goods clear with CBP). Counterfeiters also avoid detection by shipping infringing marks separately from the goods, relying on in-country assembly and distribution after the separate components have crossed the U.S. border. Counterfeiters also minimize detection by CBP by intentionally mislabeling shipping containers.
For example, CBP recently seized fake Nike shoes that were incorrectly labeled as napkins on the shipping containers in an attempt to hide the counterfeit goods. And data for shipping manifests of small packages is often incomplete or of poor quality, which makes it difficult for CBP to use it for identifying packages at high risk of containing counterfeits.

Today, all three stakeholders—brands, online marketplaces, and law enforcement agencies—recognize the need to create and share up-to-date information about authorized manufacturers and sellers, the geographic origin of products, and key identifying aspects of authentic products and their packaging. This information could help them work together to remove fakes from the market as well as get to the root of counterfeiting operations. At present, online marketplaces and law enforcement agencies do not share sufficient information about counterfeits to address the problem. There are three main reasons for this.

First, antitrust concerns regarding the sharing of corporate information have forestalled cooperation among various brand sellers and online marketplaces. Antitrust law focuses on improving consumer welfare by preventing collusion among market participants. However, active cooperation—targeted to share and analyze data concerning suppliers and map logistics networks to detect flows of counterfeit products—is needed among these participants in order to improve consumer welfare. To the extent legal and academic conceptions of antitrust lag behind advances in data innovation, the resulting ambiguity could restrain advances in anti-counterfeiting policy.

Second, U.S. laws prohibit CBP from sharing any more information about counterfeits with e-commerce platforms and common carriers (such as FedEx, UPS, and DHL). A 2019 report by the Senate Finance Committee notes that TFTEA allows CBP to share information that “appears on the merchandise and its packaging and labels” with rights holders if it believes that the good in question may infringe upon a registered copyright or trademark, but that TFTEA does not authorize CBP to share information with e-commerce platforms or common carriers. Sharing this information more broadly would allow these actors to work together to stop the distribution of counterfeit products. Further, TFTEA does not provide CBP sufficient authority to disclose information to rights holders regarding the containers used to ship the goods to the United States (exclusive of retail packaging). Sharing this information would improve tracking of counterfeit shipments.

The Senate report also notes that the Trade Secrets Act (TSA) prevents CBP officers from sharing information on counterfeit goods that have been seized or detained at U.S. ports with e-commerce platforms and common carriers. While such information could be used by retailers to curtail sales of counterfeits and warn consumers, CBP officials fear that this action might
reveal trade secrets regarding importers’ supply chains, thereby placing it at odds with the law.51

Third, while CBP is able to provide rights holders with information about seized counterfeit goods under existing regulations, it is unable to provide them with information about abandoned goods that are suspected of being counterfeit.52 In response, CBP has proposed amending customs regulations to allow it to disclose to rights holders details about abandoned infringing goods, such as the date of importation, port of entry, a description of the merchandise, and the country of origin. Rights holders could use this information to help CBP identify IPR violations and identify channels of counterfeit shipments.53

Disclosing information about abandoned goods is a further step in the right direction, but it only goes so far. In comments to the proposed rule, the International Anti-Counterfeiting Coalition (IACC) welcomed this proposal but pointed out that “the abandonment process must also provide a lasting deterrent to those counterfeiters attempting to evade CBP’s efforts, particularly in light of the fact that they’ve already pocketed their profits by the time the merchandise has been detained.”54 Noting the adaptive strategies of counterfeiting organizations, IACC has recommended that deterrence should come from “improved targeting against future shipments, joint criminal actions, civil enforcement by rights-holders, and voluntary collaborative efforts among industry stakeholders to identify and effectively remove bad actors from the ecosystem.”55 Such proactive actions require enhanced cooperation among enforcement agencies, rights holders, and e-commerce retailers, for which a shared partnership platform is required.

CURRENT LEGISLATIVE PROPOSALS WOULDN’T FIX THE INFORMATION SHARING PROBLEM

To be able to cooperate effectively, brands, e-commerce sites, and law enforcement agencies need a shared platform to legally collect, share, analyze, and act on emerging information about counterfeit products and supply chains in a timely manner. Current legislation pending in Congress, however, does not fulfill this need.

Congress is considering two legislative proposals. S. 3431—the “Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act” or the “INFORM Consumers Act”—is sponsored by Senator Bill Cassidy (R-LA). This act would require online marketplaces to verify “on at least an annual basis” the identity of all high-volume third-party sellers that list products in their medium. It would also mandate that online marketplaces require high-volume third-party sellers to label products with information about themselves, including their business and email addresses.

Another bill, H.R. 6058—the “Stopping Harmful Offers on Platforms by Screening Against Fakes in E-commerce Act of 2020” or the “SHOP SAFE Act
of 2020”—was introduced by Rep. Jerrold Nadler (D-NY). This legislation would amend the Trademark Act of 1946 to hold online third-party marketplaces liable for contributory infringement of a counterfeit mark in “connection with the sale, offering for sale, distribution, or advertising of goods that implicate health and safety.”

However, neither of these approaches—both of which seek to place the onus on online marketplaces—is adequate to fix the problem. Even if online marketplaces were able to gather the information required annually by the proposed INFORM Act, counterfeiting organizations could move faster to evade detection.

The presence of added liability that would be introduced by the SHOP SAFE act would increase the motivation for online marketplaces to deter counterfeiters but would not provide the means to take proactive and meaningful action. Instead, it may foster risk avoidance (such as online marketplaces imposing restrictions on third-party sellers on their platforms) that would not only limit consumer choice, even from legitimate sellers, but also potentially inhibit further innovations in marketplace platforms. Indeed, these legislative proposals, which emphasize increased verification of third-party sellers and increased liability for online marketplaces, could, in the end, be more harmful than effective.

**RECOMMENDATIONS**

Brand sellers, online marketplaces, and law enforcement agencies need additional capabilities to cooperatively address the scourge of counterfeiting. To this end, Congress should amend existing laws to facilitate real-time data sharing about authorized manufacturers, distributors, and sellers and resellers regarding the geographic origin of products and key identifying aspects of authentic products and their packaging. Congress should also establish a public-private partnership that can assimilate this information and foster new data-driven technologies to proactively disrupt the flow of counterfeits and other related threats to the nation’s commerce and public welfare.

**Amend Existing Laws and Regulations that Pose Barriers to Real-Time Anti-Counterfeiting Data Sharing**

There are statutory and regulatory barriers arising from TSTEA and TSA that inhibit some types of information sharing on counterfeit goods and distribution networks between law enforcement agencies and retailers as well as among retailers. Congress should remove these barriers. In addition, CBP should update its rules to permit disclosing to rights holders details about abandoned infringing goods.

Legal and regulatory changes that encourage cooperation on data sharing, including by overcoming antitrust concerns, could go a long way to encourage standard setting, research, and innovation. Congress should enact a selective
antitrust exemption to foster collaboration among e-commerce firms. As precedent, the Cooperative Research Act of 1984 granted a partial antitrust exemption to certain research joint ventures by firms in the semiconductor industry.59 This could be modified to allow companies to seek DOJ exemptions to cooperate in the fight against counterfeiting. More recently, the Cybersecurity Information Sharing Act of 2015 authorized cybersecurity information sharing among private firms and state and federal governments, thereby exempting it from federal antitrust laws.60

Establish a Public-Private Partnership to Share Anti-Counterfeiting Data

Congress should direct CBP to establish a public-private partnership wherein enforcement agencies, brand sellers, and online marketplaces work together to stop counterfeiters and disrupt their networks by creating a shared data repository, developing common industry standards, and conducting research on proactive measures to identify and disrupt counterfeiter networks.

First, this partnership should create a shared data repository—a cloud-based, common-pool resource to share and manage across many stakeholders. The architecture for this repository might include a data layer to normalize and integrate data from diverse sources; an analytics layer in which competing software algorithms translate data into alerts that can be used by government enforcement agencies, brand sellers, and online marketplaces; and finally an application layer for entrepreneurial firms and research organizations to experiment with available data to develop innovative products and services. The National Oceanic and Atmospheric Administration (NOAA) Big Data Program is one example of such a data repository. The National Weather Service performs a comparable function wherein it aggregates data from multiple data sources and fuses it together in order to provide weather data to its customers and the larger community.

Second, this partnership should establish commonly accepted standards and best practices for information sharing among enforcement agencies, brand sellers, and online marketplaces. In this regard, there is a need to create mechanisms for a common system of digital identification for third-party verification. Private actors could work in partnership with CBP to standardize the process by which customs brokers verify the identity of their client importers. This partnership organization could combine this verification scheme with enhanced information sharing between CBP and e-commerce platforms to keep counterfeiters off of online marketplaces.61 A system could be established that would foster information sharing while at the same time protecting sensitive business information from disclosure to either competitors or the public.

Third, this partnership should provide a forum to conduct shared research. Normally, firms may be reluctant to share such research for fear that other
competitors might free-ride on this activity. In this regard, a partnership with CBP and other law enforcement agencies taking the lead, along with brand sellers and online marketplaces, could advance research in AI algorithms that look for patterns in the movement and behavior of counterfeiting networks.

**CONCLUSION**

The proliferation of counterfeits, including in online marketplaces, threatens the health and safety of American consumers and damages U.S. workers and firms by diverting earnings from the legitimate U.S. businesses whose IP is counterfeited.

Brand sellers, online marketplaces, and federal enforcement agencies are each increasing their own efforts to interdict and destroy counterfeit imports. While they are employing a series of defensive approaches to protect supply chains and stop the sale of counterfeits, these efforts are often siloed and uncoordinated.

Congress has also sought to address this problem through proposed legislation that would place the onus on online marketplaces to identify and remove counterfeit products. These proposals may instead foster risk avoidance by these e-commerce firms, ultimately narrowing consumer choice and inhibiting innovation.

A more proactive and systemic approach is needed to identify and disrupt counterfeiter networks. In this regard, a public-private partnership could provide the coordination needed among brand sellers, online marketplaces, and enforcement agencies to disrupt counterfeit networks by developing common standards for data collection and building a platform for advanced analytics and innovative solutions. Using the authority already found in the TFTEA. Congress should urge CBP to facilitate the timely operation of such a partnership.
REFERENCES

1. The World Trade Organization (WTO) defines product counterfeiting as, “Unauthorized representation of a registered trademark carried on goods identical or similar to goods for which the trademark is registered, with a view to deceiving the purchaser into believing that he/she is buying the original goods.” See World Trade Organization (WTO), Glossary: Counterfeit Definition. (Geneva: WTO, 2011), https://www.wto.org/english/thewto_e/glossary_e/glossary_e.htm.


19. This is a rough estimate based on the following assumptions: Enhanced data sharing and cooperation could reduce 50 percent of counterfeits entering the United States; 50 percent of counterfeits are for foreign goods; and 50 percent of reduction in counterfeits would be spent on U.S. economic activity. This estimate also assumes every $1B increase in U.S. economic activity translates to 4,000 U.S. jobs. For details on this latter estimate, see Adams Nager, “Trade vs. Productivity: What Caused U.S. Manufacturing's Decline and How to Revive It” (ITIF, February 2017), https://itif.org/publications/2017/02/13/trade-vs-productivity-what-caused-us-manufacturings-decline-and-how-revive.

20. Karen Butner, “AI is reshaping the supply chain” (IBM Corporation, June 2017).


28. Ibid.

29. Ibid.


31. Hearing before the United State House of Representatives Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce (March 4, 2020), statement of Amber Leavitt, Associate General Counsel and Head of Intellectual Property eBay, Inc.


37. The federal effort includes various bureaus of the Department of State, the Patent and Trademark Office of the Department of Commerce, the U.S. Postal Service, and the Federal Bureau of Investigation.


39. United States Government Accountability Office (USGAO), Intellectual Property, CBP has taken steps to combat counterfeit goods in small packages but could streamline enforcement.

40. Ibid.


46. United States Government Accountability Office (USGAO), Intellectual Property, CBP has taken steps to combat counterfeit goods in small packages but could streamline enforcement.


50. Ibid.

51. Protecting E-Commerce Consumers from Counterfeits: Hearing before the United States Senate Finance Committee (March 6, 2018), statement of Brenda Smith, Executive Assistant Commissioner, Office of Trade, Customs, and Border Protection.

52. United States Government Accountability Office (USGAO), Intellectual Property, CBP has taken steps to combat counterfeit goods in small packages but could streamline enforcement.


55. Ibid.


58. United States Government Accountability Office (USGAO), Intellectual Property, CBP has taken steps to combat counterfeit goods in small packages but could streamline enforcement.


60. Non-federal entities sharing cyberthreat indicators and defensive measures with Cybersecurity and Infrastructure Security Agency in compliance with its requirements are eligible for multiple protections including exemption from

ABOUT THE AUTHOR

Sujai Shivakumar is associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. He has two decades of experience in directing studies, convening high-level dialogue, and preparing and disseminating reports of the National Academies of Sciences, Engineering, and Medicine and the National Academy of Public Administration. He has deep experience in the assessment of public-private technology partnerships and technology transfer from the National Laboratories, analyses of policies supporting advanced manufacturing and the skilled technical workforce, policy studies relating the governance of near-earth orbit, and comparative reviews of international innovation policies and their impact on the U.S. innovation system.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C., and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is a part of the nonprofit, nonpartisan Information Technology and Innovation Foundation.

contact: info@datainnovation.org

datainnovation.org