NOVEMBER/DECEMBER 2021

DEVOTED TO LEADERS IN THE INTELLECTUAL PROPERTY AND ENTERTAINMENT COMMUNITY

VOLUME 41 NUMBER 10

THE Licensing Journal®

Edited by Gregory J. Battersby and Charles W. Grimes

Wolters Kluwer

Beyond whack-a-mole[1]*: Maximizing the Impact of Your Internet Monitoring Program*

James J. Saul

J. J. Saul, a Partner in the Faegre Drinker Chicago Office, protects clients' brands and content from counterfeiting, piracy, and other trademark and copyright infringement worldwide. An efficient, results-driven attorney, he executes cost-effective strategies for global trademark and copyright clearance, registration, monitoring, and enforcement.

E-commerce was already booming when the pandemic struck, and now it feels ubiquitous. Consumers spent $861.12 billion online with U.S. retailers in 2020, up 44.0% from $598.02 billion in 2019, representing 21.3% of total retail sales last year compared with 15.8% the year prior.[2] The statistics only underscore what we're all witnessing—technology stocks appreciating rapidly, a steady drumbeat of brick-and-mortar retailer bankruptcies, shopping mall closings, conversion of massive properties to logistics centers, catch-up efforts by traditional retailers to offer online sales and curbside pickup, and our own increasingly online shopping habits. Even when the sale of goods and services are not executed online, brick-and-mortar sellers are nonetheless utilizing the internet like never before to reach potential customers, educate them about their products, and coax them into stores. Whatever the world looks like after the pandemic ends, these e-commerce gains are likely here to stay.

It has never been more important therefore for brand owners to monitor and protect their brands online. E-commerce is a counterfeiter's paradise, as explained succinctly by the OECD, "E-commerce platforms represent ideal storefronts for counterfeits and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers."[3] Why is this? E-commerce enables counterfeiters to send cheap knockoffs, which garner high margins, to unwary purchasers across the globe with little risk of legal repercussions.[4] The first obstacle to legal enforcement is the anonymity afforded by both the internet generally and e-commerce platforms specifically. ICANN's interpretation of Europe's GDPR privacy legislation has generated a blackout of Whois information, making it more difficult to identify the perpetrators behind many illicit webshops.[5] Moreover, e-commerce platforms do not operate by the same "know your seller" obligations burdening brick-and-mortar retailers. Whereas a brick-and-mortar retailer could be found liable for selling a counterfeit product in its store, and therefore presumably conducts diligence on and obtains contractual protections from each of its sellers, e-commerce platforms are considered mere intermediaries connecting sellers with buyers, ignorant of and without liability for the nature or quality of the products transacted. As summarized by the U.S. Department of Homeland Security, "While the U.S. brick-and-mortar retail store economy has a well-developed regime for licensing, monitoring, and otherwise ensuring the protections of intellectual property rights (IPR), a comparable regime is largely non-existent for international e-commerce sellers."[6]

Even when counterfeiters can be identified and located, they frequently operate across multiple jurisdictions, change locations, and cause considerable damage before any legal enforcement has the chance to be successful. Local enforcement can be slow, difficult, and uncertain—for many but the largest companies, the expense of pursuing such enforcement may be too substantial to take on. The result, as expressed by DHS, is one that many brand owners know all too well:

Counterfeits pose risks to human health and safety, erode U.S. economic competitiveness and diminish the reputations and trustworthiness of U.S. products and producers. Across all sectors of the economy, counterfeit goods unfairly compete with legitimate products and reduce the incentives to innovate, both in the United States and abroad.[7]

Particularly unfortunate for brand owners is the reality that customers blame *them* for counterfeits—after all, theirs is the name on the product, and consumers hold brands responsible for protecting them from knockoffs. Besides, who else is there to blame? Some nebulous, nameless network of illicit traders spread across unknown parts of the world?

The foundation for any successful internet anti-counterfeiting program is knowing what's out there. But when embarking on an internet monitoring program, many brand owners can quickly become deterred, coming to believe that internet enforcement is nothing but an endless game of whack-a-mole—one infringement gets knocked down only for another to pop up, or for the same infringement to pop up elsewhere. Rather than let themselves be deterred, brand owners should both remember their obligation to protect customers from fakes and consider these recommendations for moving their program beyond whack-a-mole:

1. **Monitor broadly, but strategically**—The most basic program is merely reactive, responding to customer complaints about online knockoffs or notifications from business teams about what they encounter in the marketplace. As this often is only the tip of the iceberg, the next level of enforcement can consist of internal personnel running periodic searches on relevant platforms (*e.g.*, Amazon or Facebook). Perhaps they even develop expertise with specific platforms' enforcement tools to have certain problematic listings removed (*e.g.*, eBay VeRO, Amazon Brand Registry and Project Zero, etc.). These efforts can quickly expand to address additional trademarks and platforms (ever proliferating in number and each carrying its own unique enforcement rules and protocols) and can become unwieldy, while still only uncovering portions of the broader problem. Fortunately, internet-monitoring vendors have become ever more adept at combing vast expanses of the internet with precision and doing so increasingly cost-effectively. Searching broadly is not critical so much for the sake of identifying and addressing every online infringement, but rather for the sake of identifying what's doing the most harm to your brand and prioritizing enforcement efforts accordingly. Those customer complaints and business team reports are often a good place to start, and the vendor will often offer free scanning to gauge the scope of the problem and the proper contours of a monitoring program, whether it be online marketplaces, social media, websites, domain names, and app stores and across what geographies. Vendors are typically able to search foreign-language listings as well. Ultimately, it's about tailoring online monitoring to your business's strategic needs, and that can't happen until you understand the scope of what's damaging your brand.
2. **It takes a village**—On the business side alone, anticounterfeiting often involves multiple stakeholders—supply chain, product security, packaging, and legal are just a few of the functions that may need to be consulted before taking action. Even beyond the company, the cooperation of multiple outside service providers may be necessary to operate successfully and cost-effectively. The relationship between internet-monitoring vendors and outside trademark counsel is one example. Some vendors take a go-it-alone approach, asserting that their high-tech monitoring systems and user-friendly enforcement tools make trademark counsel extraneous, and replacing them is even part of their value proposition. The better vendors recognize their symbiotic relationship with trademark counsel—whereas the vendors offer the sophisticated software tools required to crawl the internet and identify connections between infringers, as well as the managed services to take enforcement action at scale, trademark counsel can help wield those tools much more adeptly, successfully, and ultimately, cost-effectively. As the most basic example, trademark counsel understands the client's trademark portfolio, can help provide the necessary certificates and powers of attorney, and can work with the client to expand the portfolio to address uncovered infringement. Trademark counsel also helps interpret the monitoring results provided by the vendor, gauging the damage to the client's brand and developing corresponding enforcement priorities and can help the vendor identify the most effective enforcement bases afforded by the relevant platforms' terms of use according to the client's product types. Moreover, trademark counsel can often develop creative strategies for leveraging the client's existing trademark portfolio, or its other IP rights, without resorting to additional expensive registrations. The takedown notices that internet-monitoring vendors offer are not always successful, and counsel may be tasked with strategizing and executing on any escalation efforts, in some cases leveraging their own networks with in-house counsel at relevant platforms. Finally, as discussed further below, takedown notices are only one enforcement approach, and counsel can evaluate whether others may better accomplish the client's goals along with the corresponding action steps.
3. **Don't overlook brand reputation**—The online sale of infringing goods and services is not the only problem; as we know all too well, the internet

is also full of commentary, opinions, and "news," some factual and some not. When it comes to your brand, false or misleading information can seemingly come from nowhere, quickly proliferate, and deter legitimate customers. As but one example, companies are routinely dragged into lawsuits over matters to which they are only tangentially related, and aggressive plaintiffs' lawyers and other commentators can engage in online hyperbole in their hunt for clients and clicks. Such online content can be enough to deter would-be customers from reaching out. Often, this problematic content can be removed, and even when it cannot, it's important to offer rebuttals, set the story straight, or otherwise offer the brand's perspective. An effective monitoring program helps to identify these situations early so that countermeasures can be taken before they gain damaging momentum.

4. **Organize your intelligence**—Internet monitoring generates lots of data, and this information can be much more valuable than a mere list of infringing marketplace listings or social media advertisements. The best internet-monitoring vendors store and continuously cross-reference this and other provided client data, along with the corresponding seller and contact information associated with each "hit." In this manner, commonalities are identified, and a seller's activities can be linked across multiple platforms, or entire networks of perpetrators can be uncovered. In these cases, it can make sense to hold off on takedown notices and first conduct pretext or other investigations to learn more about the scope of the counterfeiting activities and the involved companies and personnel. This information can not only aid in identifying the elusive roots of a counterfeiting problem, but it can also serve as the foundation for a compelling dossier in persuading law enforcement to take action.
5. **Identify chokepoints in counterfeiters' business operations**—The objective of anticounterfeiting enforcement is to take the minimum action to make the maximum impact obstructing a counterfeiter's business. Attacking an impermeable aspect of the counterfeiter's operation can yield unsatisfactory and discouraging results; when a criminal network is established and sophisticated, for example, a program focused on sending takedown notices may have limited impact. In other instances however, a broad-based program of takedown notices can indeed show the counterfeiter that a brand is a "hard target," leading it to move on to less vigilant prey. Certain elements of the counterfeiter's online operation may present vulnerabilities, such as the selection of infringing domain names for its websites or its reliance on social media advertising. Or its supply chain for shipping knockoffs from overseas may present opportunities to collaborate with customs agents. As discussed above, it may even make sense to use the intelligence gleaned from internet monitoring as the basis for further investigation with the objective of soliciting the help of law enforcement. In this manner, since counterfeiters' vulnerabilities are not all the same, the appropriate enforcement tool will vary.
6. **Choose your enforcement tools carefully**—As indicated above, takedown notices are but one arrow in a quiver of different anticounterfeiting enforcement tools available. In some cases, monitoring and subsequent investigation may yield enough scale of activity to interest local law enforcement, which may conduct a raid of the relevant facilities or conduct other criminal enforcement action, even potentially resulting in a restitution award to the brand. Alternatively, such investigation may yield specific, actionable information on the counterfeiter's supply chain, and customs recordation and training in one or more ports will not only obstruct the counterfeiter's business, but also potentially yield seized products. Alternatively, the counterfeiter's reliance on infringing domain names for its webshops can make UDRP[8] actions a robust means of enforcement, as without the domain names, consumers will suddenly be unable to find the counterfeiter's wares online. If a particular platform is the main conduit for the counterfeiter's business, seeking the platform's collaboration in removing the activity (making sure to address aliases as well) may be worthwhile, and platforms are showing increasing willingness to collaborate with brand owners in enforcement actions. If a broader takedown campaign is warranted, instead of trademark rights it may sometimes be more productive and efficient to leverage blanket product prohibitions based on applicable regulations (*e.g.*, for prescriptions drugs), copyrights associated with products or packaging, false-advertising argumentation, or even patent rights in certain cases. In such circumstances, trademark counsel can train the internet-monitoring vendor in these alternative approaches to streamline the overall enforcement process and corresponding expense. Finally, where the counterfeiter can be pinpointed, with a specific physical presence and identifiable assets, civil litigation can allow for favorable remedies,

including enhanced statutory damages and attorney fees.

7. **Consider partnering to change the rules**—Yours is not the only brand pummeled by knockoffs or other illicit online activity. Anticounterfeiting is an area where partnering with similarly situated companies, even competitors, can make sense in pursuit of broader solutions, and the time may be ripe to change the rules for internet trade, both in the United States and abroad. Internet platforms are drawing increasing attention from both the public and lawmakers. The earliest laws affecting e-commerce took a light touch to nurture its development. Now, there is robust debate about whether internet companies continue to need delicate treatment, and even whether brick-and-mortar businesses are the ones in need of protection.[9] Newly proposed laws have been introduced to combat online counterfeits, including the SHOP SAFE Act and the INFORM Consumers Act, and even the Communications Decency Act is under review. If brand owners want to influence this debate, now is the time. Consortia of common industry partners can maximize influence in support of particular interests. Being at the table to influence the internet rules of the future could dramatically impact not only the effectiveness and expense of future brand enforcement, but also its necessity.

Some brand owners struggle with internet enforcement, skeptical of the return on investment. Undoubtedly getting control of your brand online is a daunting challenge, but you don't have to play whack-a-mole. With the right approach, you can change the game entirely.

1. WHAC-A-MOLE® is a registered trademark for games and other goods owned by Mattel, Inc., and no affiliation, sponsorship, or endorsement with or by Mattel exists or is implied by the use of "whack-a-mole" in this article. The game is so iconic that, "the term 'Whac-a-mole' (or 'Whack-a-mole') is used colloquially to depict a situation characterized by a series of repetitious and futile tasks, where the successful completion of one just yields another popping up elsewhere." *See https://en.wikipedia.org/wiki/Whac-A-Mole* ("In law enforcement it refers to criminal activity popping up in another part of an area after increased enforcement in one district reduces it there"). We have used the alternate spelling whack-a-mole in lower case letters to emphasize that ours is only the colloquial meaning.
2. *See https://www.digitalcommerce360.com/2021/02/15/ecommerce-during-coronavirus-pandemic-in-charts/*.
3. *See* 1 OECD (2018), Governance Frameworks to Counter Illicit Trade, Illicit Trade, OECD Publishing, Paris, *https://doi.org/10.1787/9789264291652-en*.
4. *See* DHS Report, p. 10, "Selling counterfeit and pirated goods through e-commerce is a highly profitable activity: production costs are low, millions of potential customers are available online, transactions are convenient, and listing on well-branded e-commerce platforms provides an air of legitimacy."
5. *See https://www.tcamtoday.com/2020/restricted-access-to-whois-data-jeopardizes-brand-owners-online/*.
6. *See https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf*, page 6.
7. *See https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf*, page 7.
8. The Uniform Domain Name Dispute-Resolution Policy (UDRP) is maintained by the Internet Corporation for Assigned Names and Numbers (ICANN).
9. *See* DHS Report, p. 10, "The ability of e-commerce platforms to aggregate information and reduce transportation and search costs for consumers provides a big advantage over brick-and-mortar retailers."