Responsibility for the sale of trademark counterfeits online: Striking a balance in secondary liability while protecting consumers

Kari Kammel,[1] Jay Kennedy[2], Daniel Cermak[3], and Minelli Manoukian[4]

WORKING PAPER FEBRUARY 2021

[1] Kari P. Kammel, Esq., is the Assistant Director of Education and Outreach, Michigan State University, Center for Anti-Counterfeiting and Product Protection, kkammel@msu.edu; 517-353-2163. She is an adjunct professor of law at Michigan State University College of Law and is a licensed attorney in Illinois and Michigan.
[2] Jay P. Kennedy is the Assistant Director of Research for the Center for Anti-Counterfeiting and Product Protection and an Assistant Professor in the School of Criminal Justice at Michigan State University. jpk@msu.edu; 517-353-2162.
[3] Daniel Cermak, J.D. is Court Officer/Research Clerk for the 30th Circuit Court in Michigan and is a recent graduate of Michigan State University College of Law and previously worked as a Legal Researcher for the Center for Anti-Counterfeiting and Product Protection at Michigan State University. danielwcermak@gmail.com
[4] Minelli E. Manoukian, J.D., is a recent graduate of the Michigan State University College of Law and previously worked as a Legal Researcher for the Center of Anti-Counterfeiting and Product Protection at Michigan State University. manoukianminelli@gmail.com.

I. Introduction[5]

The second decade of the twenty-first century saw e-commerce explode in the US and across the world, particularly for consumer goods.[6] For the first time in history, merchants and sellers could reach buyers and consumers instantly breaking down traditional barriers of jurisdiction--time and space. Consumers now can get virtually any product or good with a click of a button and the e-commerce platforms that provide the marketplace for these sales are recognized and trusted brands themselves. This phenomenon has only accelerated since the spread of COVID-19 in l ;ate 2019 through the time of publication forced consumers globally to go on lock downs at home, resorting often to online shopping exponentially more than they had prior.

E-commerce platforms[7] provide ease of access to consumer goods from one's computer or smartphone; however, they also by their nature provide counterfeiters easy access to sell their wares-- counterfeit products. The questions before us initially appear straightforward: a seller of a counterfeit product could be directly liable for trademark infringement[8] and could it be exposed to possible criminal prosecution[9] and strict products liability claims. But the more complex current issue is whether a platform has any liability for the sale of a counterfeit product by a third party on its site and if the platform can be liable if the consumer is harmed by that product. This paper will explore (1) the current state of trademark counterfeits on e-commerce platforms with a focus on the US, (2) the history of case law in the US addressing whether e-commerce platforms incur primary or secondary liability for trademark counterfeiting; (3) strict products liability cases against e-commerce platforms for injury from the purchase of third-party sales; (4) e-commerce liability for trademark counterfeits through copyright; (5) possible criminal culpability for platforms; (6) other possible legal issues; and (7) a potential way forward that focuses on the importance of public policy in the protection of consumers.

II. All that Glitters: Trademark counterfeits in E-Commerce

We will first explore the economic, health and security implications that trademark counterfeiting can have. Despite both deceptive and non-deceptive counterfeits existing online

[5] A special thanks to Deepu Karchalla (MSU, BA expected 2021); Joseph Longo (MSU, BA 2020), and Tyler Armstrong (J.D. expected 2022).
[6] Saeed Fayyaz, *A Review on Measuring Digital Trade & E-Commerce as New Economic Statistics Products*, STATISTIKA (2019), https://www.czso.cz/documents/10180/88506450/32019719q1_057.pdf/37dfdce8-0aca-4859-b774-641d7c9c40f3?version=1.0.
[7] E-commerce sites include Amazon.com, EBay.com, Walmart.com, Rakuten.com, AliExpress.com, Tmall.com, Taobao.com, Mercadolibre.com, and many others.
[8] Lanham Act (Lanham-Trade-Mark Act) (Trademark Act of 1946), 15 U.S.C. §§ 1051-1141 (West, Westlaw through Pub. L. No. 116-130).
[9] 18 U.S.C.A. § 2320 (West, Westlaw through Pub. L. No. 116-130).

and many consumers believing that no harm comes from buying a 'fake' shirt or handbag, counterfeiting impacts multiple stakeholders globally, including the consumers themselves. Recent reports from the Organisation for Economic Cooperation and Development (OECD) detail a narrative of counterfeits saturating more of the market than ever before, increasing from a combined value of counterfeits from $200 billion in 2005 to $509 billion in 2016.[10] Further detailing this disturbing image, the US Department of Homeland Security (DHS) reported that seizures of infringing goods at US borders have increased tenfold between 2000 and 2018.[11] Operation Mega Flex, a 2019 US Customs and Border Protection operation, found that nearly 5% of all goods shipped from China and Hong Kong contained illicit products.[12] E-commerce sites served as the purchasing medium for many of these shipments.[13] From the industry perspective, the International Anti-Counterfeiting Coalition stated that every sector of its membership classified counterfeit and pirated goods purchased via e-commerce sites as a top priority.[14]

While the growth of counterfeits continues, e-commerce traffic, including both that of licit and illicit goods, has also experienced tremendous growth in the last decade[15] and particularly since COVID-19 led consumers to increase online shopping.[16] With the advent of virtual storefronts and online transactions, e-commerce sites provide the opportunity for businesses of all sizes to realize global profits and reach consumers they might not have been able to access previously. Counterfeiters have also taken advantage of the opportunity this technology provides. Items previously sold in back-alleys and on street corners are now paraded on the front pages of third-party marketplaces. One major e-commerce platform (Amazon) reported that its proactive efforts have removed over one million suspected bad actors before these individual could publish a listing for even a single product, while blocking an additional three billion suspected counterfeit listings.[17] Yet, even with these initiatives, MarkMonitor, a former brand protection, antipiracy, and antifraud company, found that nearly 40% of all unwitting purchases of counterfeit goods occurred through online, third-party marketplaces.[18]

---

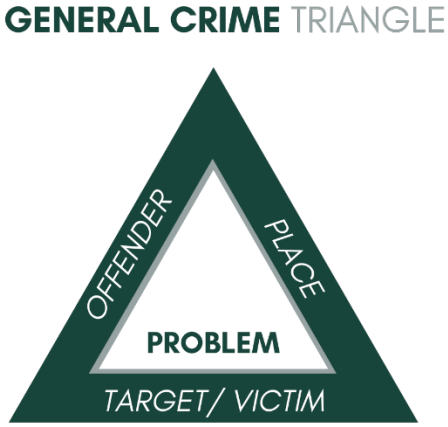
[10] OECD, Trends in Trade and Counterfeit Goods (2019).
[11] US Customs and Border Control, Intellectual Property Rights: FY 2018 Seizure Statistics (2019).
[12] Alan Rappeport, *U.S. Cracks Down on Counterfeits in a Warning Shot to China*, The New York Times, January 24, 2020, https://www.nytimes.com/2020/01/24/us/politics/us-cracks-down-on-counterfeits-in-a-warning-shot-to-china.html.
[13] *Id*.
[14] Department of Homeland Security, Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States (2020).
[15] Department of Commerce, Quarterly Retail E-Commerce Sales 2nd Quarter 2019 (2019).
[16] https://www.worldipreview.com/article/health-warning-covid-19-and-the-rise-of-counterfeits; *see also* https://www.cbp.gov/newsroom/national-media-release/cbp-reminds-consumers-beware-counterfeit-goods-when-shopping-holiday
[17] Department of Homeland Security, *supra* note 13, at 5.
[18] MarkMonitor, MarkMonitor Online Barometer: Global Online Shopping Survey 2017—Consumer Goods (2017).

Financially, counterfeit goods affect both state (or national) economies, as well as companies of all sizes. Counterfeit goods have been estimated to have displaced roughly $500 billion worth of global sales in 2013, with forecasts predicting that this displacement would grow to over one trillion by 2022. These displaced sales have been estimated to account for the loss of over two million employment opportunities.[19] From a business standpoint, from the moment a company exposes itself to the benefits of the online marketplace it also faces increased challenges related to illicit online actors. Even if a company does not intend to sell online, it may find that its products or counterfeit versions of its products are already being sold online, filling consumer demand for their products. Third party e-commerce platforms foster an air of legitimacy, shielding, albeit possibly unintentionally, counterfeit goods from consumer scrutiny and punitive action. The onus is currently on the brand owner, or trademark owner, to notify the e-commerce platform to remove a suspicious listing or a seller that could be selling an illicit or unauthorized product. For every listing that a brand owner successfully petitions to have removed from an online marketplace, several more illicit listings will likely take its place. In response to these threats, an entire industry of online anti-counterfeiting providers selling their services to brands has developed services to scrape the web, e-commerce sites, and social media platforms for counterfeits.

These third party service providers understand, as do many brands, e-commerce platforms and law enforcement agencies, that the opportunity for online counterfeiting rests upon a stable base of consumer-counterfeiter interactions. Here, we introduce an important criminological theory to help inform public policy considerations and guide our discussion of how e-commerce might be regulated fairly given multiple actors. Online counterfeiting is a routine criminal activity [20] that can be visually described through the use of the crime triangle shown in Figure 1.

[19] Frontier Economics, The Economic Impacts of Counterfeiting and Piracy (2016).
[20] Cohen, Lawrence E., and Marcus Felson. "Social change and crime rate trends: A routine activity approach." *American sociological review* (1979): 588-608.

Figure 1



As displayed in Figure 2, the crime triangle for e-commerce trademark counterfeiting consists of trademark counterfeiters in the role of motivated offenders, consumers in the role of suitable targets/potential victims, and the platform itself as the place wherein offender and target meet and interact. What is absent from the triangle presented in Figure 1 is the active effort of the e-commerce platform operator. In the basic form of the crime triangle, which represents the elements essential for a crime to occur, the e-commerce platform simply functions as a place, or vehicle through which individuals interact. No action is supposed here, but rather a lack of action or guardianship on the part of the e-commerce operators, which facilitates meetings among offenders and targets.

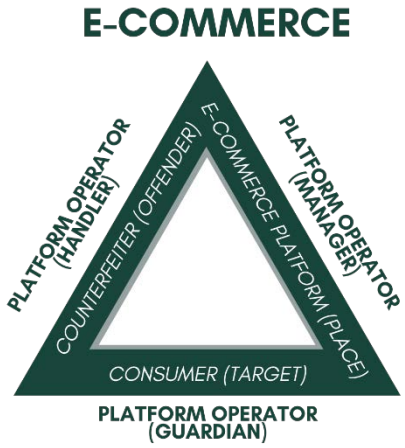


Figure 2

The motivated offender is the counterfeiter who operates as an "unseen competitor" to legitimate companies, using the e-commerce platform as a place to hide from detection and reap illicit economic benefits.[21] In combination with the low-cost of production and lack of marketing costs (since counterfeiters rely on the brand's marketing of the product), counterfeiters can realize larger amounts of revenue. This inherent advantage creates unfair competition for genuine products, driving out high-quality brands in exchange for low-cost counterfeits.

Though the trade of counterfeit goods may damage an economy and a brand's reputation, the products themselves can also harm a consumer's health and wellbeing. From a general perspective, the production and quality of materials used for manufacturing counterfeit goods can lead to personal injury. Potentially unsanitary and hazardous, these environments and materials pose significant risks to both consumers and possibly manufacturing employees, particularly in the cases of counterfeit cosmetics, electronics and pharmaceuticals. In one finding, seized counterfeit cosmetic products contained dangerous levels of arsenic, mercury, aluminum and lead.[22] When used by consumers, these products have had disastrous consequences.[23] In March of 2019, Europol seized thirteen million doses of counterfeit medicine, ranging from opioids to heart medication.[24] Estimates place fake antimalarial drugs as contributing to over 450,000 deaths every year, defrauding a population of consumers afflicted with serious illnesses.[25] For counterfeit electronics, the US Government Accountability Office (GAO) reported that in a study of over 400 counterfeit iPhone adapters, 99% failed tests for safety, fire and shock hazards.[26] US Customs and Border Protection (USCBP) reported that for all contraband seized in 2016, 16% posed direct and obvious threats to the consumer.[27]

---

[21] Jeremy M. Wilson & Rodney Kinghorn, *A Total Business Approach to the Global Risk of Product Counterfeiting*, 10 Global Edge Bus. Rev. No.1, 1-6 (2016).
[22] Sasha Grabenstetter, What's the Cost? Cheap Counterfeit Cosmetics (2020).
[23] *Fake Cosmetics Found to Contain 'Toxic' Chemicals, BBC News, https://www.bbc.com/news/uk-45313747* (last visited April 3, 2020).
[24] More than €165 million of trafficked medicines seized in Operation MISMED 2, , Europol , https://www.europol.europa.eu/newsroom/news/more-%E2%82%AC165-million-of-trafficked-medicines-seized-in-operation-mismed-2 (last visited Apr 30, 2020).
[25] Kaliyaperumal Karunamoorthi, *The Counterfeit Anti-Malarial is a Crime Against Humanity: A Systematic Review of the Scientific Evidence*, 13 Malar. J., art. 209 (2014).
[26] Underwriters Laboratory (UL), *99 [p]ercent failure rate for counterfeit phone adapters*, (Dec. 20, 2016), https://www.ul.com/news/99-rercent-failure-rate-counterfeit-phone-adapters (last visited March, 26, 2020). *See* U.S. Government Accountability Office, *Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market*, Report to the Chairman, Committee on Finance, U.S. Senate, GAO-18-216, 18(Jan. 2018), https://www.gao.gov/assets/690/689713.pdf.
[27] *See supra*, note 18.

In terms of national security, counterfeit products can pose risks a number of substantial risks. First, illicit producers have managed to weave counterfeit intermediate parts into the supply chains of the defense industrial base in the U.S.[28] In 2018, approximately 12% of counterfeit seizures conducted by DHS included versions of technology necessary to the nation's defense.[29] These seizures included components for automotive and aerospace parts, batteries, and machinery.[30] The illicit substitutes are not only of a lower quality, but the US Bureau of Industry and Security highlighted the dangers associated with "Trojan Chips," which can infect defense systems with viruses or malware.[31] Another risk to national security shifts the focus to the organizations responsible for counterfeit products. Counterfeiters can be criminal generalists, engaging in other criminal activity alongside counterfeit schemes.[32]The Better Business Bureau noted that counterfeit production operations often rely on strong central coordination, creating attractive, profitable opportunities for organized crime, such as the Japanese Yakuza or Italian Mafia.[33] In some cases, the proceeds from counterfeit sales even support acts of terrorism and authoritarian dictatorships across the globe.[34]

Though often seen solely as a profit thief from large and successful companies, counterfeit products have the potential and capability to affect several aspects of society. Because of these risks, the U.S. has passed legislation at the federal and state level to protect against trademark counterfeiting, including both civil and criminal statutes.[35] Given this brief examination of the current impact of counterfeits, we will now turn to our exploration of US caselaw.

III. Many Attempts, As Many Failures: A History of E-Commerce Platforms' Ability to Avoid Liability for Counterfeiting

To date, nearly every U.S. court has found that e-commerce platforms are not liable for counterfeit products sold on their website. The lack of liability is not for lack of trying by brand owners, or trademark owners. Plaintiff trademark owners have brought multiple actions against e-commerce platforms in an effort to hold them liable for the actions of third party sellers that

[28] Brandon Sullivan & Jeremy Wilson, *An Empirical Examination of Product Counterfeiting Crime Impacting the U.S. Military.*, 20 Trends in Organized Crime 316–337 (2017).
[29] Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics (2010).
[30] See supra, note 25.
[31] Joe Doyle, *Deterrence in Depth: One Stakeholder's View of DLA and the Counterfeit Electronics Invasion,* Def. Stand. Prog. J. (2013).
[32] Jay Kennedy, *A-CAPP Center Product Counterfeiting Database: Insights Into Converging Crimes,* (Jan. 2019).
[33] Better Business Bureau, *Fakes are Not Fashionable: A BBB Study of the Epidemic of Counterfeit Goods Sold Online* (2019),https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf.
[34] United Nations Office of Drugs and Crime, Focus On: *The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime*.
[35] *See generally*, Jeremy Wilson, Brandon Sullivan, Travis Johnson, Roy Fenoff, and Kari Kammel, *Product Counterfeiting Legislation in the United States: A Review and Assessment of Characteristics, Remedies, and Penalties,* 106 J. CRIM. LAW & CRIMINOLOGY 521-526 (2017)

are utilizing their platforms including: direct trademark infringement, secondary trademark infringement, strict products liability, Digital Millennium Copyright Act[36] claims, and negligence claims all of which will be discussed in this paper. This section will explore the case law and regulation efforts directed at counterfeits sold by third parties on e-commerce platforms. Though *Tiffany (NJ) Inc v. eBay, Inc.*[37] is the flagship case for contributory liability for trademark infringement by e-commerce platforms, we will also review several other cases to provide an understanding of the Court of Appeals for the Second Circuit's reasoning in its landmark decision in *Tiffany*.

A. The lead-up to *Tiffany v. eBay*

We begin our analysis in 1981, long before the advent of e-commerce platforms with the development of the court-made doctrine of secondary trademark liability and track the development of caselaw through the early appearance of counterfeits showing up in flea markets and later in online markets. We will explore first the creation of secondary trademark liability.

1. *Inwood Labs* and the Creation of Secondary Trademark Liability

In 1981, the Supreme Court of the U.S. considered the case of *Inwood Labs v. Ives Labs*, in which Ives brought suit against Inwood for producing tablets that intentionally looked like Ives' tablets of the same medicine.[38] The *Inwood* court interpreted the Lanham Act and asked the question whether liability under the statute "extended beyond those who actually mislabel goods with the mark of another."[39] The Court noted that yes, it could be extended, as a manufacturer that does not control everyone in the chain of commerce and can be held liable for others' infringement "under certain circumstances."[40] The *Inwood* court then ruled the following, which has been upheld for over 35 years:

> Thus, if a manufacturer or distributor *intentionally induces* another to infringe a trademark, or if it continues to supply its product to one whom *it knows or has reason to know is engaging in trademark infringement*, the manufacturer or distributor is contributorily responsible for any harm done as a result of the deceit.[41]

The *Inwood* case thus set the stage for the first judge-made doctrine of secondary liability for trademark infringement by those who play a role within the "chain of commerce", or the supply chain, by creating the test of either (1) intentionally inducing another to infringe, or (2) knowing

[36] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860, (1998).
[37] Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010).
[38] Inwood Labs. v. Ives Labs., 456 U.S. 844, 849-50 (1981).
[39] *Id.* at 853.
[40] *Id.* at 853-54.
[41] *Id.* (emphasis added)

or has reason to know that someone is engaging in trademark infringement. *Inwood* involved pharmaceutical company Ives alleging that several companies were manufacturing a drug produced by defendant Inwood and passing it off as an Ives product.[42] Ives decided to contain the drug in a blue capsule, imprinted with "Ives 4124[.]"[43] Eventually, Ives' patent expired, and other companies began producing cyclandelate, and the generic manufacturers used capsules that utilized the same colors as the Ives capsules.[44] The consumer's only interaction with branding in terms of cyclandelate is on the pills themselves, as the bottles are generic bottles used by pharmacists, unconnected to a drug manufacturer.[45]

As a result of the generic brands using similar colors to Ives' capsules, Ives brough suit against a number of people that were allegedly mislabeling generic cyclandelate as CYCLOPASMOL, including a major generic distributor, Inwood Labs.[46]

Notably, Ives did not allege that the petitioner themselves applied infringing labels to the pills, merely that Inwood and others "contributed to the infringing activities of pharmacists who mislabeled generic cyclandelate."[47] Ives went on to argue that the use of colors similar to those used by CYCLOPASMOL meant that Inwood was falsely designating the origin of their generic product, and noted that the use of color was not functional.[48]

The district court denied Ives' request for a preliminary injunction against Inwood.[49] The court justified the ruling by stating that while Inwood could be held responsible for the infringement if they could show that Inwood knowingly and deliberately instigated the mislabeling of the products by the pharmacists, "Ives had not established that the petitioners conspired with the pharmacists or suggested that they disregard physicians' prescriptions."[50] The court of appeals affirmed and, relying mostly on a 1946 case from Massachusetts,[51] noted that Inwood would be liable only if Ives suggested, or even implied, that pharmacists fill bottles with the generic pills while labeling the bottles with Ives' trademark or "if the petitioners continued to sell cyclandelate to retailers whom they *knew* or *had reason to know* were engaging in infringing practices."[52]

---

[42] *Id.* at 104.
[43] *Id.*
[44] *Inwood*, 456 U.S. at 850.
[45] *Id*
[46] *Id.*
[47] *Id.* at 850.
[48] *Id.* at 850-51.
[49] *Id.* at 851.
[50] *Id.*
[51] Coca-Cola Co. v. Snow Crest Beverages, Inc., 64 F. Supp. 980 (Mass. 1946) (emphasis added).
[52] *Inwood*, 456 U.S. at 854.

The *Inwood* court continued the court of appeals' analysis and utilized the test first set forth in *Coca-Cola*.[53] The *Inwood* court noted that the pharmacists themselves were not responsible. According to the Court in *Inwood*, "if a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorily responsible for any harm done as a result of the deceit."[54] This case thus created a new space for liability of conduct in the supply chain for the manufacturer.

2. Building on *Inwood* with *Hard Rock* and *Sony*: Trademark Infringement as a Tort

Following the *Inwood* decision, the question became whether the same *Inwood* test could be applied beyond manufacturers, and *Hard Rock Cafe Licensing Corp. v. Concession Servs.*[55] presented that question in 1992. The parties involved in *Hard Rock* included the famous restaurant chain and a flea market owner where counterfeit Hard Rock Cafe merchandise was discovered.[56] The *Hard Rock Cafe* Court utilized the Restatement of Torts to note that the flea market owners would be liable for torts committed on their property when they knew or had reason to know that someone on the property was using it tortiously.[57] The Court then determined that without evidence to the contrary, secondary trademark infringement should be treated as a tort, and therefore *Inwood* applies.[58] Importantly, *Hard Rock* supplied a rule for contributory infringement when a service is involved, as opposed to a product: "direct control and monitoring of the instrumentality" the infringer uses to infringe the brand owner's mark allows the *Inwood* standard to apply to services as opposed to just products.[59]

From there, *Lockheed Martin Corp v Network Solutions, Inc.* built upon the principle noted in *Inwood* and *Hard Rock* but explored for the first time an internet issue.[60] The facts of *Lockheed* involved the description of a service, as opposed to a product in the above mentioned cases; Lockheed was challenging Network Solutions Inc.'s (NSI), allowance of multiple domain names that utilized "skunk works," the name of one of Lockheed's construction laboratories for jets.[61] The court described NSI as not unlike the U.S. postal service, merely directing internet users to a specific domain name, or address, by running the domain name and routing the information so the user's computer travels to the correct domain, it does not supply the domain name, it merely

[53] Coca-Cola Co. v. Snow Crest Beverages, Inc., 64 F. Supp. 980 (Mass. 1946).
[54] *Inwood*, 456 U.S. at 854.
[55] Hard Rock Cafe Licensing Corp. v. Concession Servs., 955 F.2d 1143 (7th Cir. 1992).
[56] *Id.* at 1146.
[57] *Id.* at 1148-149; *see* Restatement (Second) of Torts § 877(c) & cmt. d (1979).
[58] *Id.* at 1149.
[59] *Id.* at 1148-1149
[60] *Lockheed Martin Corp. v. Network Solutions, Inc.*, 194 F.3d 980 (1999)
[61] *Id.* at 982-84.

directs information and users there using the domain name.[62] The court held that NSI could not possibly exercise sufficient control over the infringing domain names to be contributorily liable, noting that requiring NSI to monitor the entire internet was a stretch that "would reach well beyond the contemplation of *Inwood Lab.*" and *Hard Rock*.[63] This concept in 1999 would set the stage for the courts perception of what companies were able or not able to control given technology at the time. Something that, as we know now, evolved and continues to do so at a rapid pace.

Another instrumental case is *Sony Corp. of America v. Universal City Studios,*[64] a case that the later *Tiffany* court "f[ou]nd helpful" to reach their conclusion.[65] In *Sony*, Universal Studios and Disney brought action against Sony because of VCR users recording programs protected by copyright.[66] Though their conclusion mostly rested on the fair use doctrine of copyright and the majority refused to apply the *Inwood* standard, the *Sony* Court briefly hypothetically applied the *Inwood* standard.[67] The *Sony* court decided that Sony, the manufacturer, would not be contributorily liable for the actions of the users because "Sony certainly does not 'intentionally [induce]' its customers to make infringing uses of respondents' copyrights, nor does it supply its products to identified individuals known by it to be engaging in continuing infringement of respondents' copyrights."[68] While the *Sony* majority declined to accept Universal's argument that Sony had "constructive knowledge" that VCR users would use the items to infringe copyrights, the concept would come back in *Tiffany* in a major way.[69]

This taking of the tort concept of liability for activities on a property that the owner had control over and combining it with the *Inwood* standard was an important step in U.S. courts' realization that as the nature of sales changed, liability needed to shift based on who was in the best position to stop the infringing product once they became aware of it. Revisiting the crime triangle for e-commerce described above can help to frame the need for this shift.[70] In physical marketplaces, offenders and targets meet in physical places that are controlled and monitored by an individual or organization with the ability to affect the types of activities that occur at the place. When a vendor at a flea market sells counterfeit goods, the flea market owner can remove the vendor as a way to prevent the sale of counterfeits in that space. Additionally, the flea market operator might have other vendors sign rental agreements stipulating that they will not offer counterfeit or infringing goods for sale to consumers.

---

[62] *Id.* at 984-85.
[63] *Id.* at 985.
[64] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).
[65] Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93,108 (2d Cir. 2010).
[66] *Sony Corp.*, 464 U.S. at 420.
[67] *Id.* at n.19.
[68] *Id.* On a final note on the *Sony* case, Justice Blackmun felt that *Inwood* could also be applied to a copyright case. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 490 (1984)(J. Blackmun, *dissenting*); (
[69] Sony Corp., 464 U.S. 417, 439 (1984).
[70] *See supra* note 20, Figs. 1-2.

The operators of brick-and-mortar establishments have a large amount of direct control over the goods sold within the spaces they control, because they can actually see and monitor the products offered to consumers. They also have indirect control through their ability to sanction rule violators when infringing goods are sold to consumers, as well as the ability to dissuade illicit activity through the threat of removal of desired benefits (i.e., sales, revenue). In the analogy of these cases in the context of the crime triangle, the courts seem to be noting that in the physical marketplaces, the owners or managers are in a place to provide guardianship for the place, thus being responsible for and potentially liable for protecting the consumer from the sale of a counterfeit good. See Figure 3.

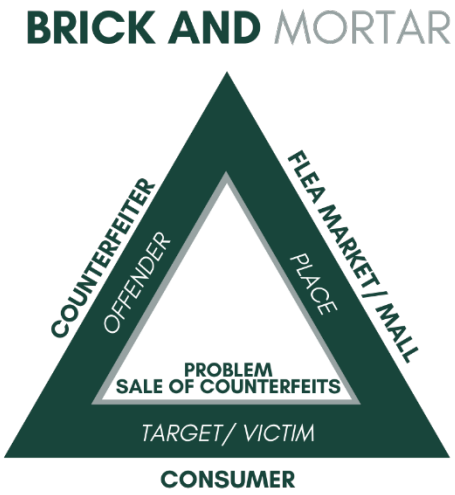


Figure 3

These series of decisions by appellate courts and the Supreme Court set the stage for the shift from brick and mortar to e-commerce and whether a brand may bring a successful direct or secondary trademark infringement suit against an e-commerce platform for a third party's sale of a counterfeit good. Although the question seems to be narrow and limited, the phenomenon of third-party sales of counterfeit goods on e-commerce sites continues to grow rapidly. However, we rely on a standard that was applied to the application of technology to the internet from over 11 years ago when the *Tiffany v. eBay* standard was created. That technology has been far surpassed but we still rely on it and will now explore.

3. *Tiffany v. eBay:* Secondary Trademark Infringement E-Commerce Platforms for the Sale of Counterfeits by Third Parties

In the landmark case of *Tiffany v. eBay*,[71]Tiffany brought suit against online marketplace eBay after a number of counterfeit Tiffany products were found being sold on the platform.[72] Tiffany's first claim against eBay was for direct trademark infringement under section 32 of the Lanham Act, which allows "the owner of a mark registered with the Patent and Trademark Office [to] bring a civil action against a person alleged to have used the mark without the owner's consent."[73] Tiffany brought this claim because of eBay's use of Tiffany's marks in advertisements.[74] The two-prong test the Court used was to first determine if Tiffany's mark was entitled to protection, and if so, second, if eBay's use of the protected mark "is likely to cause consumers confusion as to the origin or sponsorship of the defendant's goods."[75]

The Court of Appeals for the Second Circuit quickly analyzed and dispatched Tiffany's direct infringement claim against eBay. The court did so without going through a full analysis of direct trademark infringement because of the nominative fair use doctrine.[76] That doctrine allows for advertisements to utilize a mark usually protected under trademark "so long as there is no likelihood of confusion about the source of [the] defendant's product or the mark-holder's sponsorship or affiliation."[77] The court ruled that the advertisements and sponsored links on eBay's platform utilizing Tiffany's trademarks did not directly infringe Tiffany's trademark rights because the marks were only used to describe the products and never suggested that they were sponsored by or affiliated with Tiffany.[78]

Tiffany also advanced a contributory liability theory, which garnered the most analysis from the court.[79] As discussed above in Section 2 and cases leading up to Tiffany, the court noted that contributory liability for trademark infringement is a judicially created document deriving from the common law of torts.[80] The court then focused on their "most recent case involving contributory trademark infringement"—*Inwood.*[81]

While on its face the *Inwood* test may not fit non-manufacturer service providers like e-commerce platforms, the court has extended the possible distributors and manufacturers to service providers as well, namely flea market owners.[82] This extension of the distributor and

---

[71] Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010).
[72] *Id.* at 101-02.
[73] *Id.* at 102 (citing *ITC Ltd. v. Punchgini, Inc.*, 482 F.3d 135, 145-46 (2d Cir.), *cert. denied*, 552 U.S. 827, 128 S. Ct. 288, 169 L. Ed. 2d 38 (2007)).
[74] *See id.*
[75] *Tiffany*, 600 F.3d at 102 (citing Savin Corp. v. Savin Grp, 391 F.3d 439, 456 (2d Cir. 2004)).
[76] *Id.* at 102.
[77] *Id.* (citing Merck & Co. v. Mediplan Health Consulting, Inc., 425 F. Supp. 2d 402, 413 (S.D.N.Y. 2006)).
[78] *Tiffany supra note 1* at 103.
[79] *See Tiffany v. eBay supra* note 1. (discussing secondary trademark liability).
[80] *See id.* at 103 (citing Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1148).
[81] *See id.* at 104-09.
[82] *Id.* at 104.

manufacturer rule was first seen in *Hard Rock Cafe v. Licensing Servs.* [83] *Hard Rock*, as noted above, stated the common law "imposes the same duty…[as Inwood] imposes on manufacturers and distributors," as with a flea market owner or a landlord[84] The Ninth Circuit tightened service providers' contributory liability for trademark infringement to instances when the service provider "exercises sufficient control over the infringing conduct."[85] With *Inwood*, *Hard Rock* and *Lockheed* making up a large bulk of the eventual holding, the Court in *Tiffany* noted the lack of case law regarding contributory liability for trademark infringement on the internet, emphasizing that they were the first to apply the *Inwood* test to an online marketplace.[86]

In applying the rules to the facts, the Court in *Tiffany* quickly determined that *Inwood* does apply, adopting the reasoning of the district court that eBay was a service provider akin to the service provider seen in *Lockheed*.[87] The Court then moved on to the question of whether eBay was liable under *Inwood*, an endeavor that required much more analysis.[88] *Tiffany* did not focus on the first possible avenue for liability provided in *Inwood* that requires that the service provider "'intentionally induces another to infringe the trademark[,]'" but instead focused on the second factor that provides contributory liability if the service provider "'[c]ontinues to supply its [service] to one whom it knows or has reason to know is engaging in trademark infringement'"[89]—or the contemporary knowledge requirement.

a) Contemporary Knowledge Requirement

The Court ultimately ruled that eBay was not contributorily liable under the knowledge requirement discussed in the *Inwood*, holding: "For contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods. Some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary."[90] Because *Inwood* did not analyze the contemporary knowledge requirement further, the *Tiffany* Court looked elsewhere to ground their rule requiring contemporary knowledge. The Court's reasoning for requiring this "contemporary knowledge" factor is in fact based on dicta from a copyright case,[91] in which the Supreme Court in *Sony* stated:

---

[83] Hard Rock Cafe v. Licensing Servs., 955 F.2d 1143, 1148-49 (U.S. Ct. App. 7th Cir. 1992).
[84] *Tiffany*, 600 F.3d 93 supra note 1 at 104 (citing *Hard Rock*, 955 F.2d *supra* note 14 at 1149).
[85] *Tiffany supra note 1* at 104 (citing Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (1999)).
[86] *Tiffany supra note 1* at 105.
[87] *Id.* at 105-06.
[88] *See Id.* at 105-10.
[89] *Id.* at 106 (citing *Inwood*, 456 U.S. at 854).
[90] *Id.* at 107.
[91] *Id.* (citing Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984)).

> If Inwood''s narrow standard for contributory trademark infringement governed here, [the plaintiffs''] claim of contributory infringement would merit little discussion. Sony certainly does not ''intentionally induce[]'' its customers to make infringing uses of [the plaintiffs''] copyrights, nor does it supply its products to identified individuals known by it to be engaging in continuing infringement of [the plaintiffs''] copyrights.[92]

Utilizing this rationale, the *Tiffany* Court ruled that based on the authority of *Sony*, the *Inwood* rule allows for contributory liability for ecommerce platforms only when individuals performing the violation of the trademark of another are identified and allowed to continue.[93] This analysis of contemporary knowledge of what is currently infringing or will infringe in the future was logical at the time to balance liability and make sure it was reasonable and feasible. It would be illogical to hold a platform responsible for something that they do not have the capability to see or locate. Similarly, it would be logical if the apartment building owner would not be liable if they knew or should have known that criminal activity was occurring on their property. This concept is important as the methods for surveillance and technologies for monitoring and election has developed exponentially and given 'service providers', as the court describes, the ability to have extensive, real-time knowledge.

B. Consequences of *Tiffany v. eBay*

Tiffany v. eBay, in short, led to recognition that the current contributory trademark infringement route does not sufficiently protect rights holders, but some legal scholarship emphasizes the thought that too much of a swing in the other direction will place too much responsibility on e-commerce platforms and more generally, the market.[94] The emphasis on finding a balance between the two has become such a common question and point of emphasis in the contributory trademark infringement scholarship space, some have referred to the word and the general line of thinking as the "b-word."[95]

Due to the importance of the case, *Tiffany* has had its fair share of criticism. One such critic notes a number of problem areas that arose as an immediate consequence of the ruling, including placing a burden on intellectual property holders, legitimate eBay sellers and eBay shoppers alike.[96] Some legal scholars suggest that the Second Circuit based its holding on an analysis of the reasonableness of eBay's efforts to combat the counterfeiting, as opposed to a

---

[92] Sony Corp. of Am. v. Universal City Studios, Inc., n.19 (quoting *Inwood*, 456 U.S. at 855).
[93] *Tiffany*, 600 F.3d at 108-09.
[94] Yafit Lev-Aretz, *Combating Trademark Infringement Online:* Secondary Liability v. Partnering Facility, 37 Colum. J.L. & Arts, 639, 640 (2014).
[95] *Id.* (citing Annette Kur, Senior Research Fellow, Max Planck Inst. for Intell. Prop. & Competition Law, Address at the Columbia Law School Kernochan Center Symposium: Who's Left Holding the [Brand Name] Bag? Secondary Liability for Trademark Infringement on the Internet (Nov. 8, 2013)).
[96] Andrew Lehrer, *Tiffany V. Ebay: Its Impact And Implications On The Doctrines Of Secondary Trademark And Copyright Infringement*, 18 B.U. J. SCI. & TECH. L. 373, 392-97 (2012).

knowledge requirement.[97] While this was initially seen as a ray of light for brand owners to hope that courts could have enough discretion to find in their favor in future online marketplace secondary liability cases,[98] in practice, courts have generally followed *Tiffany* to the "T."[99]

1. **Proximity, Control, and Willful Blindness**

Despite the criticism of the judgment by some legal scholars, courts have generally followed and in fact somewhat expanded on the holding in *Tiffany* for the entirety of the decade since the ruling. Perhaps the most notable expansion comes from an unpublished flea market case, where the United States District Court of New Hampshire applied *Hard Rock, Tiffany, Inwood* and *Sony* to the facts of the case.[100] In *Coach v. Gata Corp.*, the court utilized the general knowledge standard to test if contributory liability extended to a flea market selling Coach merchandise.[101] In finding that the flea market was liable for contributory liability, the court emphasized proximity and control that a flea market exercises as opposed to eBay, a pharmaceutical company and DVR users: "[s]uffice it say that the operator of a flea market that rents spaces to vendors exercises substantially more control over potential direct infringers than the defendants in *Tiffany*, *Inwood*, and *Sony* exercised over the direct infringers in those case (sp.)."[102] The language of *Coach* is fascinating in that in 2011, the assumption is again made that an online platform has less control over an infringer than a flea market owner. The reasons for this may encompass many factors, including a perception, whether real or assumed, that in person control or monitoring is more thorough than online.

Following the application to a flea market, *Luxottica Group, S.p.A. v. Airport Mini Mall, LLC* applied *Tiffany's* willful blindness element to a shopping mall.[103] In this context, willful blindness to a party's direct infringement can serve as sufficient constructive knowledge for another party to be held contributorily liable for trademark infringement.[104] Applying this test to shopping mall owners, the court ruled that there was sufficient evidence to hold the mall owners as contributorily liable for one store's direct infringement.[105] In holding this, the court noted what the mall owners could have done in order to avoid being found willfully blind:

> "the jury reasonably could have found that Luxottica's notice letters would have prompted a reasonable landlord to do at least a cursory visual inspection of the Mall's

[97] Graeme B. Dinwoodie, *Secondary Liability for Online Trademark Infringement: The International Landscape*, 37 Colum. J.L. & Arts 463, 479 (2014).
[98] *Id.* at 479-80
[99] *See Infra*. § III(B)(1).
[100] Coach, Inc. v. Gata Corp., (2011 U.S. Dist. LEXIS 62317).
[101] *Id.*
[102] Id. *at 21*
[103] Luxottica Grp., S.p.A. v. Airport Mini Mall, LLC, 932 F.3d 1303 (11th Cir. 2019)
[104] *Id.* at 1312.
[105] *Id.*

> 130 booths to determine which vendors displayed eyewear with Luxottica's marks and sold it at prices low enough—$15 or $20 a pair for glasses that typically retail at $140 to $220 a pair—to alert a reasonable person that it was counterfeit."[106]

This generally suggests that after receiving notice of infringing activities, a reasonable service provider should "do at least a cursory visual inspection" of the price of products being sold in the marketplace compared to the usual retail price.[107] This language leads one to believe that the walk through is considered a reasonable investment of time and effort for a brick and mortar entity that is making profit from vendors in order to avoid liability—what would an equivalent be for an e-commerce platform today?

In some later e-commerce cases courts found in favor of the brand owner, albeit in limited circumstances. In *Spy Optic Inc. v. Alibaba.com Inc.*, the Court found that Alibaba could be found to be contributorily liable for trademark infringement based upon counterfeit products found on their website.[108] Alibaba argued that they could not be liable for contributory trademark infringement because they had a program, Aliprotect, which was a system that could be used by brand owners to take down infringing products.[109] The Court rejected that argument, noting that the plaintiff did use the Aliprotect system successfully, but the infringer continued to post successfully to Alibaba.com.[110] Because Alibaba.com knew that the company had engaged in trademark infringement and had the ability to prevent that company from posting on the website, Alibaba.com could be liable for contributory trademark infringement.[111]

Again, we turn to criminological theory to explore the balance of liability. These examples highlight the role that marketplace operators, be they flea markets or e-commerce platforms, play in affecting the stability of criminal opportunity structures. While e-commerce platform operators do not figure into the base crime triangle as mentioned above,[112] they do factor into a second layer triangle in the role of a crime controller.[113] Crime controllers serve an important role in crime prevention activities as they have a direct influence upon the elements of the crime triangle. Specifically, motivated offenders can be controlled by handlers who have the ability to de-motivate the potential offender, while guardians have the ability to protect suitable targets by deterring potential offenders or assisting targets in making themselves less suitable for victimization. Finally, place managers have the ability to control the conditions and circumstances that allow offender and targets to come together and interact. The elements

---

[106] *Id.* at 1314-15.
[107] *Id.* at 1315.
[108] *See* Spy Optic, Inc. v. Alibaba.com, Inc., 163 F. Supp. 3d 755 (C.D. Cal.).
[109] *Id.* at 766
[110] *Id.*
[111] *Id.*
[112] See Figures 2 and 3.
[113] Tillyer, Marie Skubak, and John E. Eck. "Getting a handle on crime: A further extension of routine activities theory." *Security Journal* 24, no. 2 (2011): 179-193.

essential to a criminal scheme (offender, target and place) come together when a crime controller fails to properly interact with its respective element in a way that would mitigate the risk of a crime occurring. E-commerce platforms can serve as a handler of motivated offenders, guardian of suitable targets, and a manager of risky places wherein product counterfeiting can occur. As such, the guardianship structure established through the crime element-crime controller relationship breaks down and allows online counterfeiting to proliferate.

C. Looking forward: Developments with E-Commerce

As with any major leap in technology, the advent of e-commerce has come upon the legal system too quickly for it to react with needed legislative changes—an occurrence that has been described as a law disruptive technology.[114] The test for a law disruptive technology is three-pronged. First, it must be a new technology. E-commerce is new and in the past ten years it has been used with increasing rapidity globally, allowing consumers and retailers to meet anywhere in the world with few barriers to access.[115] Secondly, it must have major economic and societal impacts, which e-commerce has shown through its impact on how consumers and sellers interact with each other and the access to goods and general behavior involved in buying and selling, but also for criminal activity in this space.[116] Finally, the laws that apply to trademark counterfeiting in brick and mortar situations do not apply easily to the e-commerce scenario in most of the current global legal framework.[117] We believe e-commerce clearly passes this test. Because of the nature of e-commerce and our view of it as law-disruptive technology, we believe the current statutory framework in the U.S. does not apply neatly to the space of e-commerce, nor does the current case law—thus, we are at a precipice where something will need to change to address the imbalance that has been created.

---

[114] *See* Kari Kammel, *Examining Trademark Counterfeiting Legislation, Free Trade Zones, Corruption and Culture in the Context of Illicit Trade: The United States and United Arab Emirates*, 28 Mich. Stat. Int'l L. Rev. 209 (2020); William Sowers, How do you Solve a Problem like Law-Disruptive Technology?, 82 L. & CONTEMP. PROBs. 193 (2019)

[115] *See* Kammel, *supra* note 6; Sowers, *supra* note 6; Alexandro Pando, *How Technology Is Redefining E-Commerce*, Forbes (Mar. 6, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/03/06/how-technology-is-redefining-e-commerce/#750d5b3862e3.

[116] Kammel, *supra* note 6; Sowers, *supra* note 6; *see, e.g.*, Abdul Gaffar Khan, *Electronic Commerce: A Study on Benefits and Challenges in an Emerging Economy*, 16 Global Journal of Management and Business Research, 2016, at 19; Jamsheer K, *Impact of e-Commerce On Society: Advantages and Disadvantages*, acowebs (Feb. 19, 2019), https://acowebs.com/impact-ecommerce-society/.

[117] Kammel, *supra* note 6; Kari Kammel, Examining Trademark Counterfeiting Legislation, Free Trade Zones, Corruption and Culture in the Context of Illicit Trade: The United States and United Arab Emirates, Mich. Stat. Int'l L. Rev. (2020); William Sowers, How do you Solve a Problem like Law-Disruptive Technology?, 82 L. & Contemp. Probs. 193 (2019); *See E-transactions Legislation Worldwide*, U.N. Conf. on Trade & Dev., https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Transactions-Laws.aspx, (giving an overview of e-commerce legislation of any kind globally and noting that 70% of countries have adopted some type of e-commerce laws) (last visited Dec. 6, 2019). *See also* Clark, *supra* note 46.

In 2019 and 2020, a series of e-commerce legislation was proposed by Congress in order to address the issues of third-party seller liability on e-commerce platforms.[118] While a detailed analysis of these pieces of legislation will not be discussed here, the SHOP SAFE Act of 2020 seeks to apply secondary liability to e-commerce platforms if they do not abide by terms of the statute.[119] While the other two pieces of legislation are silent as to secondary liability, none fully addresses the need for a balance with secondary liability between all stakeholders.

1. **Case Law**

Much has changed in the landscape of e-commerce since *Tiffany* was decided and since the initial *Inwood* case in 1981 regarding technology and control or ability to monitor content on platforms. In 2010, e-commerce was in its early years and the language and assumptions the courts make reflect this. For example, the courts noted that a flea market owner would have more control over direct infringers than e-commerce platforms[120] and that cursory inspections of a product's price could be used to determine counterfeit goods.[121] We now know the opposite may be true at the time this article was written; yet, this may change again as technology changes. The behavior of counterfeiters, like other criminals, shifts to avoid detection, so price point is no longer a sole indicator of counterfeit items and those in the field of brand protection note that these identifiers can change rapidly.

The current state of counterfeits on e-commerce has led to the development of a novel sub-industry. Because platforms themselves have not been held secondarily liable for trademark infringement, unless egregious infringement has occurred, brands have assumed some mantle of responsibilities- not because of legal liability, but because counterfeits cause injury to their mark, brand, reputation, and consumers. Many brands have outsourced their brand protection efforts to a well-developed sub-industry created to do web-scraping, monitoring and take downs of counterfeit listings, social media posts and even content on the dark web. Sometimes these service/technology providers can see a wider scope or pattern of counterfeit goods but are reluctant or cannot share patters in data because of contracts or other privacy concerns. However, neither the brand nor the service/technology provider is necessarily in the best position to prevent or monitor counterfeits on a website because they cannot initially prevent or exclude posts and cannot see the breadth of data and patterns that the e-commerce providers can.

The advent of artificial intelligence and its use in brand protection, and the active and publicly acknowledged use by e-commerce platforms of this and other cutting-edge technologies

---

[118] For a detailed analysis of these three bills, *see* John H. Zacharia & Kari Kammel, *Congress's Proposed E-Commerce Legislation for Regulation of Third-Party Sellers: Why It's Needed and How Congress Should Make It Better*, 21 U.C. Davis Bus. L.J. 91 (2020); SANTA Act, S. 3073, 116th Cong. (2019); SHOP SAFE Act of 2020, H.R. 6058, 116th Cong. (2020); INFORM Consumers Act, S. 3431, 116th Cong. (2020).

[119] Stopping Harmful Offers on Platforms by Screening Against Fakes in E-commerce Act of 2020 (SHOP SAFE Act of 2020), at Preamble.

[120] Coach, Inc. v. Gata Corp. *supra* at 21.

[121] Luxottica Grp., S.p.A *supra* at 1315.

shifts the ability of platforms to control and monitor sellers, making it vastly different than ten or twenty years ago. Additionally, with artificial intelligence, machine learning and other technologies that gather large amounts of data, there is an enhanced ability to provide significantly more information than general knowledge discussed in the prior contributory liability cases. The *Tiffany* requirement that a platform would have specific knowledge of particular listings has essentially become a reality with technology. The platforms now have access to vast amount of data, which also allows them to see patterns in the data across products and brands, to which a brand owner does not have access. In the case of the brand owner victim, they are limited to what they can see and what any additional third-party providers who they have hired can see. Thus, the platforms theoretically have specific knowledge on all of their products, which they can sort, find—all of which has now become easier and can be done from anywhere in the world. We argue this can be more effective and have more control, then any brick-and-mortar mall or flea market, where the owner is limited to products they can see. Alternatively, a platform cannot possibly know every legitimate mark for every product of every brand possibly sold the sites it operates. Accordingly, brands will need to be responsible for some type of recordation of marks in a way that is made available to the platform.

Additionally, platforms can have ultimate control over who is selling and what they are selling—they have the ability to vet products and sellers if they so choose—even more so than a flea market owner, but both profit off the sale of goods in their venue. The extension of this tort concept to the internet makes sense in many cases—where an owner or manager of a brick-and-mortar store or building is responsible for the safety of those who are purchasing or using the space. This begs the question of whether such an approach need to be applied to the e-commerce environment. While a platform may not be liable for direct trademark infringement or trafficking in counterfeit goods,[122] the law must still be able to hold them secondary liable if they are not adequately monitoring those sellers on their platform who are selling counterfeit goods.

With the concept of law disruptive technology, we must take a look at where the law can be changed. While not one person or entity should bear the entire liability for the sale of a counterfeit good on a platform, the onus of responsibility needs to shift appropriately with the shift in technology.

After all, many platforms now use their own marks and good will to create consumer trust in the platform. Additionally, with every sale of a legitimate or counterfeit product, the platform makes a profit from the transaction. Both of these factors argue in favor of a shift in how these cases are viewed in order to protect both the victimized brand owner and the consumer. Without it, platforms will continue to rely on their goodwill with little to no recourse ensuing from the sale of counterfeits on their platforms.

[122] Although they certainly may still if they are the "seller" of counterfeit goods as determined at the trial court level.

2. How the Crime Triangle Can Guide the Director for the Evolution of Secondary Liability for Trademark Infringement on E-Commerce

As mentioned previously, e-commerce platform operators can significantly mitigate opportunities for the sale of counterfeit goods on their platforms by engaging in crime controlling activities that target motivated offenders, suitable targets, and the platform itself. With regard to addressing motivated offenders, platforms have the ability to identify potentially infringing listings, as well as sellers who have previously sold counterfeit or infringing goods on the site. While it may be temporarily effective to terminate a seller's ability to post listings on the e-commerce platform, the "notice and take down procedure," it is well known that such an approach simply leads the bad actor to create a new seller profile and return to the platform with a new guise. A better approach may be to demotivate the offender by stopping infringing listings from being posted to the e-commerce site, while directing the individual to in-demand generic products or affiliate marketing opportunities. In such a situation, the individual is still able to achieve their goal of earning revenue through online commerce; yet they are doing so in a way that complies with the law and the platforms rules.

In terms of guarding suitable targets, e-commerce platforms should have a legal responsibility to ensure that consumers who visit their sites can do so in a safe way, within an environment that is as free from offenders as possible. However, undertaking guardianship activities can be some of the most frustrating and difficult crime controlling activities for an e-commerce platform. Consumers have free will and irrespective of the amount of warnings or the nature of protective activities undertaken by platforms, consumers have the choice to buy a product or not. Because many counterfeiters have adopted a strategy built around inundation – posting a large volume of listings to hedge against takedown efforts – consumers will generally have exposure to a sizeable amount of counterfeit listings. Platforms should be responsible and liable to take active steps to protect consumers, while understanding that consumers play a large part in the success of these schemes as well.

Because consumer decision making is something outside of the full control of target guardianship efforts, platforms must also engage in place management strategies that are designed to make their websites less conducive to counterfeit trade, in similar ways to brick and mortar stores or markets. Approaches that many platforms have already undertaken and have been highlights above – such as enhanced interactions with brands, expanded takedowns, pre-vetting of sellers, and others are all examples of place management strategies. The challenge for e-commerce platform operators is to remain cognizant of, if not ahead of, the curve being set by trademark counterfeiters. While it could be argued that the place management role is the most prominent crime controller function for platform operators, a comprehensive anti-counterfeiting strategy will see platforms engaged as handlers of potential offenders and guardians of potential targets as well. Thus, in this secondary layer as a crime controller, we posit that e-commerce platforms could be secondarily liable for trademark counterfeiting if they do not 1) take active steps to protect consumers on their sites, 2) engage in place management strategies that are

designed to make their sites less conducive to counterfeit trade, and 3) remain aware and ahead of the ever-changing curve set by trademark counterfeiters.

3. Conclusion

In summary, the case law that exists is few and far between and rests on very early issues with e-commerce and counterfeit goods. While those cases had a very specific set of facts that were pertinent at the time, they cannot be applied to the current state of affairs and technology. If they continue to be applied, the cases will leave major gaps for counterfeit sellers to sell products harmful to the consumer and the brand owner victim, disappear and have no one held liable in any aspect, as is the current situation, despite the ability of platforms to set up more safeguards and the profit that they are making from each transaction in the illegal sale of these goods. We recommend that courts or the legislature take this into perspective and focus on assigning liability based on the theory of the crime triangle and the e-commerce platform as a crime controller.

IV. Strict Products Liability

A. Brief History of Strict Products Liability

Strict products liability, at its onset, was meant to protect consumers from manufacturers. Put simply, it was intended that "those who profit from manufacturing a product should pay for the damage done by the reasonable use of that product."[123] While the tort took a while to gain hold, once it did, the claim of action "swept through the nation's courts faster than any other major doctrinal shift in the history of modern tort law."[124] We discuss it here as it pertains to several cases that are emerging regarding counterfeit or unsafe goods being purchased on e-commerce platforms.

The first case that began the process of the mass adoption of strict products liability is *MacPherson v. Buick Motor Company* in 1916.[125] In *MacPherson*, a Buick car "suddenly collapsed" and the owner brought suit, claiming the collapse result from a defunct wheel, provided to Buick by a components manufacturer and placed on the plaintiff's vehicle by Buick, without proper inspection, according to the plaintiff.[126] Buick's primary argument was one that had prevented liability for companies before this case; that plaintiff MacPherson lacked privity to

[123] Ellen Wertheimer, *UNKNOWABLE DANGERS AND THE DEATH OF STRICT PRODUCTS LIABILITY: THE EMPIRE STRIKES BACK*, 60 U. Cin. L. Rev. 1183, 1185 (citing Greenman v. Yuba Power Prods., 377 P.2d 897, 901 (Cal. 1962)).
[124] Kyle Graham, *STRICT PRODUCTS LIABILITY AT 50: FOUR HISTORIES*, 98 Marq. L. Rev. 555, 561 (2014).
[125] *Id.*
[126] MacPherson v. Buick Motor Co., 111 N.E. 1050, 1051 (N.Y. 1916).

sue Buick because he purchased the vehicle from a dealership.[127] Then-court of appeals Justice Cardozo rejected this argument however, noting previous cases have allowed for liability for manufacturers regardless of privity if the product was inherently dangerous.[128] This was originally meant for things such as explosives or poison, but previous cases had allowed for liabilities to such things as coffee urns and scaffolds; items that are not inherently dangerous on their own.[129] These previous cases led Cardozo to the holding of *MacPherson*, defining what makes something a thing of danger for strict products liability purposes: "[i]f the nature of a thing is such that it is reasonably certain to place life and limb in peril when negligently made, it is then a thing of danger."[130]

The holding in *MacPherson* coincided with changes in consumer actions seen over the preceding couple of decades towards the end of the 19th century and beginning of the 20th.[131] Manufacturers started building their own brands and began utilizing wholesalers and retailers to sell products as opposed to providing them directly. In the 44 years following *MacPherson*, a large majority of states had adopted the rule included therein.[132] In the 1940s, some states even extended upon the *MacPherson* rule, no longer requiring the product be dangerous.[133]

After years of academics such as William Prosser calling for widespread adoption of strict products liability, adoption snowballed after Prosser's changes to Restatement of Torts § 402 were adopted in 1964.[134] By 1976, 42 states adopted torts-based strict products liability through either courts or state legislatures, and today only five states have not adopted torts-based strict products liability.[135] With this background in mind, we jump to strict product liability's new frontier: e-commerce and the dilemma of the sale of counterfeits by third party sellers and the lack of protection of consumers when the manufacturers cannot be found. We will be exploring a series of cases brought since 2017.

B. Amazon Cases

Much like early strict products liability cases brought against product manufacturers as opposed to dealerships, lawsuits brought by plaintiffs harmed by counterfeit products brought against e-commerce platforms based upon strict products liability have generally been

[127] Graham, *supra* note 101(*citing* James A. Henderson, Jr., MacPherson v. Buick Motor Co.: Simplifying the Facts While Reshaping the Law, in Torts Stories 41 (Robert L. Rabin & Stephen D. Sugarman eds., 2003)).
[128] MacPherson v. Buick Motor Co., 11 N.E. at 1062.
[129] *Id.*
[130] *Id.* at 1057.
[131] Graham, *supra* note 101.
[132] *Id*.
[133] *Id.*
[134] *Id.* at 578.
[135] *Id.* at 579 (The five "hold-out" states, Delaware, Massachusetts, Michigan, North Carolina and Virginia, all favor their own enhanced consumer protections in regards to warranty).

unsuccessful. Several cases have been brought since 2017 against Amazon alleging strict product liability in the state courts in Pennsylvania, Ohio, Wisconsin, California, and Arizona, where there have been a wide variety of results, ranging from settlement to finding that Amazon is liable to finding they are not liable.

In Pennsylvania, in *Oberdorf v. Amazon.com, Inc.,* the case is on certification to the Pennsylvania Supreme Court with the question, "Under Pennsylvania law, is an e-commerce business, like Amazon, strictly liable for a defective product that was purchased on its platform from a third-party vendor, which product was neither possessed nor owned by the e-commerce business?"[136] Although the question posed to the Pennsylvania Supreme Court is based on the facts of the case, it raises the question of also what strict liability should look like if an e-commerce platform takes possession of it, such as if it is shipped from an Amazon warehouse, or any other variety of points in time when a platform might do something beyond just allowing a product to be listed on its website.

In a strict liability case in Ohio, the Ohio Court of appeals in *Stiner v. Amazon* found that Amazon was not considered a supplier and did not have sufficient control over the faulty product.[137]

In Wisconsin, a plaintiff survived a motion for summary judgement against Amazon, but ultimately settled in a strict liability case.[138] In the court's consideration of whether Amazon was a seller, they reasoned that response, the "sellers and distributors are liable, not because of any particular activity on their part, but because they are proxies for the absent manufacturer. This structure suggests that, in the absence of the manufacturer, the entity responsible for getting the defective product into Wisconsin is liable."[139] This particular concept described in Wisconsin but not further developed of a proxy provides an interesting outlook where the focus is making sure that the supply chain is accessible to the consumer as a remedy, when injury occurs.

In California state court, in *Bolger v. Amazon,* a state court of appeals found that e-commerce platforms could be liable under California's doctrine of strict products liability because a platform is "engaged in the business of selling … as an intermediary between an upstream supplier and the ultimate consumer".[140] The court noted a test

---

[136] Oberdorf v. Amazon.com, Inc., 2020 WL 3023064, 818 F. App'x 138 , at 139 (3d Cir. June 2, 2020). For a full discussion of the case history of Oberdorf v. Amazon, *see* John H. Zacharia & Kari Kammel, *Congress's Proposed E-Commerce Legislation for Regulation of Third-Party Sellers: Why It's Needed and How Congress Should Make It Better,* 21 U.C. Davis Bus. L.J. 91, 97-99 (2020) .

[137] Stiner v. Amazon.com, Inc., 120 N.E.3d 885 (Ohio Ct. App. 2019); *see also* Zacharia & Kammel, *supra* note, at 101.

[138] State Farm Fire & Cas. Co. v. Amazon.com., Inc., 390 F. Supp. 3d 964 (W.D. Wis. 2019); *see also* Zacharia & Kammel, *supra* note XX, at 99 (discussing the case in depth).

[139] *Id.* at 970.

[140] Bolger v. Amazon.com, LLC, 53 Cal. App. 5th 431 (2020); *see also* Zacharia & Kammel, *supra* note XX, at 99-101

where the platform: (1) "created the environment (its website) that allowed [the third-party seller] to offer the replacement battery for sale;" (2) "attracted customers through its own activities, including . . . its Amazon Prime membership program;" (3) "set the terms of [the third-party seller's] involvement, it demanded fees in exchange for [the third-party seller's] participation;" and (4) "required [the third-party seller] to indemnify it."[141] Here, the California case differed from the Pennsylvania one in that Amazon actually took possession of the good and fulfilled the customer's order directly.

In Arizona, *State Farm Fire & Cas. Co. v. Amazon.com, Inc.*, an Arizona case, applies a more liberal consideration of strict liability law under Arizona law.[142] However, the state court was overturned by the federal court in Arizona, which granted Amazon's motion for summary judgement finding that it did not exercise sufficient control over the products.[143]

From these cases, we can see plaintiffs arising all over the country bringing non-traditional strict products liability cases, as injuries and even deaths start to occur with more rapidly from the purchase of faulty or counterfeit products from third-party sellers on e-commerce platforms, because they have not other options available for a remedy for harm done.

C. Conclusion on Strict Liability

Generally, strict product liability attaching to e-commerce platforms for counterfeit products sold on their sites could bring about massive changes to how e-commerce platforms operate. As with secondary liability for trademark counterfeiting, the "crime triangle" can provide some useful insight into how counterfeiting would be affected by e-commerce platforms having strict liability for counterfeit products sold on their sites. The crime triangle, shortly summarized, is a representation of the factors that are necessary for a stable criminal opportunity to exist.[144] Crimes that are non-random and repeat themselves over time are generally composed to three essential elements: a motivated offender, a suitable target and place that lacks sufficient guardianship interventions that would otherwise mitigate or prevent the occurrence of crime.[145] Because of the lack of direct contact in the online marketplace, the crime triangle analysis for e-commerce platforms is generally limited to the guardianship and victim elements.[146] However, there also exists an opportunity for platforms to demotivate offenders in a way that does not continue a 'whack-a-mole' type pursuit of infringing sellers, but rather highlights opportunities for illicit actors to engage in legitimate behavior as discussed above.[147]

---

[141] *Bolger v. Amazon*, at 452.
[142] State Farm Fire & Cas. Co. v. Amazon.com, Inc., 407 F. Supp. 3d 848 (D. Ariz. 2019).
[143] State Farm v. Amazon.com, Inc., No. 19-17149, 2020 WL 6746745 (9th Circ. Nov. 17, 2020)
[144] *See supra*
[145] George T. Adams Jr., *Empowering Consumers as Capable Guardians to Prevent Online Product Counterfeiting*, Thesis submitted to Michigan State University, 35 (2016).
[146] *Id.* at 36.
[147] *See supra* discussion on crime triangle and secondary liability for trademark counterfeiting.

Applying these two factors to strict liability and e-commerce platforms, strict liability could mean that e-commerce platforms themselves act more as guardians. If there is increased liability for the e-commerce platforms, there could be more motivation for them to closely monitor the products listed on their sites, thus acting as guardians and limiting the amount of potential victims and limiting the space for victims to come into contact with the willing criminals.

Again, as above in the section on secondary liability, we face a dilemma of the sale of counterfeit or defective goods by third party sellers on e-commerce platforms and the phenomena of being a law disruptive technology. The strict liability doctrine was created to protect consumers from manufacturers cutting corners and endangering consumers, but now, without this additional consumer protection, legal avenue, or shift in how current legal doctrine is applied, consumers will continue to be exposed to injury or death with no legal recourse but profit still being made of the sale of the good.

V. Liability for Counterfeits from a Copyright Perspective: The Digital Media Copyright Act

Counterfeits encompass multiple forms of intellectual property such as designs, logos, slogans, and even product images of the legitimate goods they are pretending to be. Here, we analyzes the Digital Millennium Copyright Act (DMCA) and the potential influence it has on anti-counterfeiting efforts in the e-commerce space in order to further its goal to find equitable solutions for individuals damaged by counterfeiters online. While we recognize that the DMCA is not a cause of action, it is the most major hurdle to overcome when pursuing a copyright claim within the digital landscape.

Title II of the DMCA—also known as the Online Copyright Infringement Liability Limitation Act (OCILLA)--seeks to provide internet service providers and websites with more certainty regarding their risks for copyright infringement liability.[148] In order to benefit from safe harbor provisions, e-commerce websites must fulfill specific conditions for eligibility: (1) qualify as a service provider;[149] (2) implement and consistently enforce a policy that inform subscribers and account holders of a policy that provides for the termination of said subscribers' and account holders' accounts should they become repeat infringers; (3) accommodate "standard

[148] 1 McGrady on Social Media §2.01(2)(a) (2019).

[149] A service provider is "an entity offering the transmission, routing, or providing of connections for digital online communication between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as was sent or received." 17 U.S.C. §512(k)(1)(A). See also, *Corbis Corp. v. Amazon.com*, 351 F. Supp.2d 1090, 1100 (W.D. Wash, 2004) (stating that e-commerce platform Amazon.com fits within the definition of an online service provider).

technical measures" that are "used by copyright owners to identify or protect copyright works."[150]

After qualifying for safe harbor provisions, e-commerce platforms, in general, will not be liable for relief due to copyright infringement "by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider" so long as the provider: (1) does not have knowledge or awareness of the material or activity that using the material is infringing, or upon gaining knowledge or awareness acts "expeditiously to remove, or disable access to, the material," (2) does not receive a financial benefit directly attributable to the infringing activity if they have the right and ability to control such activity, and (3) upon notification of claimed infringement they respond expeditiously to remove or disable access to the allegedly infringing material.[151] In a nutshell, Title II of the DMCA creates a quid pro quo situation where copyright owners allegedly get expedited information and action against suspected infringements, while a service provider receives a safe harbor for that information.

The mentioned knowledge requirement looks to both a subjective and objective standard.[152] This standard for facts regarding the knowledge requirement is particularly demanding, and often requires specific knowledge of particular infringing activities.[153] Thus, while the DMCA and OCILLA force e-commerce platforms to maintain specific activity to remain immune from user copyright infringement lawsuits, it seems at first glance that it is unable to do anything in regards to the rampant counterfeiting issues at hand—instead it only acts as a post-mortem Band-Aid on infringement that has already occurred and may not even be discovered until damage has already been done.

A. Why Does the DMCA Matter in a Trademark Counterfeiting Context?

Counterfeiters commonly use actual images of goods in their attempt to pass their wares off as legitimate.[154] These images are the copyrighted intellectual property of the original brand

---

[150] 17 USCS §512(i)(1)-(2).
[151] *Id.*
[152] See *Viacom Int'l v. Youtube, Inc.*, 676 F. 3d 19, 31 (2d Cir. 2012); See also, §512(c)(1). The specific knowledge specification requires that the service provider: (1)"does not have actual knowledge that the material or an activity using the material on the system or network is infringing", (2)" in the absence of such actual knowledge, is not aware of the facts or circumstances from which infringing activity is apparent." See *id.* The second knowledge provision is often referred to as a "red flag" and deals with whether or not a provider would be subjectively aware of facts that would make a specific infringement "objectively obvious to a reasonable person." See *Viacom Int'l*, 676 F.3d at 31.
[153] See *id.*
[154] https://www.inta.org/TrademarkBasics/FactSheets/Pages/CounterfeitingNL.aspx; https://books.google.com/books?id=7SA6DwAAQBAJ&pg=PT194&lpg=PT194&dq=counterfeiters+use+image+of+actual+product&source=bl&ots=Nw2vWHds2Z&sig=ACfU3U07wgr_qbGiWYtmgGDoiRtpD6D0Sw&hl=en&sa

owners.[155] While this speaks to the internet-savvy skills of the modern counterfeiter, it also puts consumers at a high risk of being deceived by counterfeit product postings.[156] By using legitimate images that are sourced from the actual brand owner's product postings, customers must play a guessing game to figure out whether or not an e-commerce posting is legitimate or fake.[157] This is one of the major disadvantages to shopping on the online sphere.[158] Without the ability to inspect goods in person, they need to rely on the images provided to them online.[159] As a result, a counterfeiter's use of a legitimate brand photo of a good bolsters a fake posting that includes the same product a consumer may want but at a lower cost.[160]

Although the DMCA allows for a notice and takedown regime in cooperation with online service providers, a brand's inability to monitor every website in the world for infringing images leaves them with little choice but to try and hold websites accountable for the content being posted on their websites. In this, the very thing that is attempting to help intellectual property owners online, the DMCA, becomes their worst enemy when it comes to equitable relief from copyright infringement.

1. Application of DMCA to Impose Liability on E-commerce Platforms

The DMCA is a tool that brands can use to take down images belonging to them that are being appropriated in the sale of counterfeit goods. However, the application of the DMCA to an e-commerce counterfeiting issue seems like a tenuous solution at best. As stated before, these takedowns only occur as notices are submitted, and with e-commerce exponentially growing, there is only so much that a brand can do to protect its consumers this way. However, just as counterfeiters themselves have become more sophisticated in the sale of their wares, so too must brands become more creative in their fight to hold e-commerce platforms responsible for the rampant infringement on their platforms. Although e-commerce platforms have, as seen in recent case law, been able to fall into the safe harbor provisions of the DMCA, perhaps future amendments to the law might put it into a slightly different context and balance of liability in a similar way that we posited with secondary liability for trademark infringement.

=X&ved=2ahUKEwjspKfEl8vmAhUEAZ0JHShbAB4Q6AEwAHoECAsQAQ#v=onepage&q=counterfeiters%20use%20image%20of%20actual%20product&f=false; https://blog.redpoints.com/en/what-are-the-biggest-impacts-of-counterfeits-on-brands; https://www.jstor.org/stable/27919913?seq=1#metadata_info_tab_contents

[155] https://blog.redpoints.com/en/what-are-the-biggest-impacts-of-counterfeits-on-brands

[156] See *id.*

[157] *Id.*

[158] Thomas Holt, Adam Bossler, Kathryn Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction (2017), 228;

[159] *Id.*

[160] *Id.*

As stated previously, e-commerce platforms that qualify for DMCA safe harbor provisions must meet the following requirements to be free from liability: (1) not have knowledge or awareness of the material or activity that using the material is infringing, or upon gaining knowledge or awareness acts "expeditiously to remove, or disable access to, the material," (2) not receive a financial benefit directly attributable to the infringing activity if they have the right and ability to control such activity, and (3) upon notification of claimed infringement they respond expeditiously to remove or disable access to the allegedly infringing material.[161] This knowledge factor is the main hurdle that brands have to overcome - courts have lauded that control over third parties, and their infringing actions, is one of the major reasons why DMCA claims against internet platforms and websites fail.[162]

However, with new anti-counterfeiting initiatives, such as ProjectZero,[163] for example, e-commerce platforms are putting themselves in the precise position to exude control over a problem that they are aware exists. Created with the purpose of preventing counterfeiting on its platform, Amazon.com that third-party users are utilizing its e-commerce platform for the purpose of selling counterfeit goods.

With these new collaborative efforts with brands bolstered by technological advancements, e-commerce platforms are no longer ignorant of specific instances of counterfeiting on their sites, and subsequently are no longer ignorant of the specific instances of copyright infringement occurring on their platforms. This use of algorithmic, or artificial intelligence (AI) technology on e-commerce platforms opens a new door for brand owners. No longer do the knowledge factors of Title II's safe harbor provisions seem unattainable. However, even if the knowledge requirement is established due to changing technology on the internet, it still remains that a platform's response to notice and takedown requests can still leave them well within the boundaries of the DMCA safe harbor. However, no takedown system can be considered flawless. An e-commerce site could easily take "too long" to investigate the removal of a posting or could fail to remove every infringing post in a timely manner. Even the prioritization of some brands over others in the order to which counterfeits are taken off of their e-commerce platform could potentially be the cause of strife.

---

[161] 17 USCS §512(i)(1)-(2).

[162] See 2015 U.S. Dist. LEXIS 92890 at *23-24.

[163] Project Zero, created by Amazon.com for its brand retailers, is one of the major anti-counterfeiting programs that has caused new waves. https://brandservices.amazon.com/projectzero?tag=theverge02-20. The program boasts three major functions: (1) automated protections, (2) self-service counterfeit removal, and (3) product serialization. *Id.* The automated protections use Amazon.com's machine learning algorithm, fed with information about a brand, by the brand itself, to continuously scan listings to search for and remove suspected counterfeit products sold on its platform. *Id.* The self-service counterfeit removal system allows the brands themselves a hand in the process by allowing brands the ability to remove counterfeit listings from Amazon stores. *Id.* Data collected from these removals is then fed into the automated protections. *Id.*

As noted above in the secondary liability for trademark counterfeiting discussion, when e-commerce is viewed as a law disruptive technology, we can view emerging technologies in this context in order to put the caselaw and statutes into perspective as far as future copyright liability. Perhaps, liability can become more balanced and brands may finally be able to gain more equitable recourse within the scope of e-commerce and provide further incentives for e-commerce platforms to become inhabitable for counterfeiters. Although this theory suggests for some shared liability of e-commerce platforms for copyright infringement by third parties, the DMCA is a huge hurdle to overcome. And, as has been stated before, it is difficult to predict where the courts may land when it comes to dealing with law on the internet, with the past, or slowly creeping towards the future alongside the available technology.

VI. Criminal Liability: Aiding and Abetting, Trafficking, and RICO

Although traditional intellectual property law may be the most obvious path to try and gain retribution regarding the sale of counterfeits on e-commerce platforms, criminal law offers unique solutions that have been notoriously underutilized. Trafficking laws, aiding and abetting statutes and the Racketeer Influenced and Corrupt Organizations Act (RICO) may offer solutions on a criminal and federal level that can finally impose liability on rogue e-commerce platforms for turning the other cheek to the activity on their websites.

A. Aiding and Abetting

1. Statutes Applicable with Aiding and Abetting Counterfeiting

The application of criminal aiding and abetting to counterfeiting is hardly a new concept within the legal world. Within the language of 18 U.S.C.S §2320, the United States has named a criminal offense anyone who intentionally "traffics in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services," or "traffics in labels, patches, stickers. . . or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive."[164] Although this seems more in tune to the actions of counterfeit sellers themselves, the definition of the word "traffic" allows us to potentially broaden the scope of liability. There, the word traffic not only encompasses those who have created the counterfeit good, but those who "transport, transfer. . . for purposes of commercial advantage or private financial gain" or those who "import, export, obtain control of, or possess, with intent so to transport, [or] transfer."[165]

[164] 18 USCS §2320 (a)(1)-(2). Because this is a trademark issue by nature, the statute allows for all defenses and affirmative defenses that would otherwise be applicable in an action under the Lanham Act to be offered when under prosecution by this act. *Id*. at §2320(d).
[165] *Id*. at (f)(5).

Previous iterations of the same act, specifically the 2008 version, acknowledged the potential existence of aiders and abettors in connection with trademark infringement.[166]

Understandably, the duties given to U.S. Customs and Border Protection (USCBP) also include penalties for those who aid and abet counterfeiters.[167] Specifically, any person who "directs, assists financially or otherwise, or aids and abets the importation of merchandise for sale or public distribution that is seized [for bearing a counterfeit mark] shall be subject to a civil fine."[168]

Across the United States, multiple states have made reference to aiding and abetting laws in the penalties they place on the use of counterfeit trademarks. Specifically, North Carolina, South Carolina, Rhode Island, and Florida statutes call for the confiscation of any personal property that has been employed in the aiding or abetting of the crime of counterfeiting.[169] This same language is then repeated in the Stop Counterfeiting in Manufactured Goods Act (also known as the Protecting American Goods and Services Act).[170] Even American territories, such as Guam, have statutes that hold individuals liable for aiding and abetting in the trafficking of counterfeit goods.[171]

2. **Application of Aiding and Abetting to Marketplaces**

Although the courts have not yet applied aiding and abetting statutes to the e-commerce world, they have not been afraid to apply the standard to brick and mortar institutions.[172] In 2016, the 8th Circuit affirmed a district court decision holding that brick and mortar marketplaces, such as the flea market in the case, could be held accountable for the aiding and abetting of trafficking in counterfeit goods.[173]

---

[166] 2008 version of the act included the phrasing in section (3)(A) that "The court, in imposing sentence on a person convicted of an offense under this section, shall order, in addition to any other sentence imposed, that the person forfeit to the United States. . . (ii) any of the person's property used, or intended to be used, in any manner or part, to commit, facilitate, aid, or abet the commission of the offense." Although this language was later removed and replaced with a reference to §2323 (Forfeiture, destruction and restitution), the language in the section frames itself to be less, not more restrictive. Specifically, the forfeiture section has grown to expand the amount of goods seized to "any property used, or intended to be used, *in any manner or part* to commit or facilitate the commission of an offense. . . " (a)(1)(B) (emphasis added). For the purposes of §2320, this includes both criminal and civil forfeiture. §2323(a)-(b).

[167] 19 USCS §1526(f).

[168] *Id.* at §1526(f)(1).

[169] N.C. Gen. Stat. Section 80-11.1; S.C. Code Ann. § 39-15-1190; R.I. Gen. Laws Section 11-17-13; Fla. Stat. § 831.033

[170] 109 P.L. 181, 120 Stat. 285

[171] 9 GCA Section 47.40. "A person is guilty of aiding or abetting the trafficking of counterfeit goods who: (a) solicits a person to purchase counterfeit goods; or (b) knowingly and for the purpose of trafficking of counterfeit goods, transports any person into, out of or within Guam, or who procures or pays for the transportation any person into, out of or within Guam for the purpose of trafficking counterfeit goods." Id.

[172] United States v. Frison, 825 F.3d 437 (8th Cir. 2016).

[173] See *id.* at 444.

In *United States v. Frison*, Jack Frison, the owner of Frison Flea Market, challenged a conviction of aiding and abetting the trafficking of counterfeit goods.[174] Frison's market operated three days a week under his supervision, and Frison's income came from vendor rental fees, and admission charges to customers.[175] The rental fees allowed vendors certain privileges, such as the ability to leave their inventory in the brick and mortar marketplace while it was closed.[176] Among the other goods that were sold at the flea market, many of the vendors sold counterfeit clothing, footwear, purses, and accessories.[177] Naturally, the sale of counterfeit goods at the Frison Flea Market did not go unnoticed.[178] Frison and his market received warnings from police officers that he needed to prevent the sale of counterfeit goods because he was responsible for everything in his flea market, notices from the Record Industry Association of America warning off the sale of bootleg music, cease and desist notices from Coach, Inc. and Coach Services regarding the sale of counterfeit goods, complaints from the Better Business Bureau, and was the subject of warrants and seizures by the Department of Homeland Security, Immigration and Customs, and other federal officers.[179] However, these punitive measures did little to deter the sale of counterfeit goods in the Frison Flea Market.[180] In fact, the only major change was the Frison's implementation of a $500 fine to vendors who were caught selling counterfeit goods.[181]

Despite the evidence gathered against him, Frison argued on appeal that the statute as applied to him, aiding and abetting in the trafficking of counterfeit goods, was unconstitutionally vague, and therefore void.[182] Specifically, he claimed that he "did not have fair notice that his behavior was criminal; [and] it was unclear what he should have done to avoid liability."[183] Frison's main argument with regards to the notice, was that he did not have notice that a "passive landlord who [was] merely renting his property could be held responsible for the actions of his tenants." However, the court found that Frison was far from a passive landlord.[184] In fact, he was extremely active in his market, inducing fines on vendors, establishing his dominance and his position "in charge," among other things.[185] However, even if he had been a less active landlord,

---

[174] *Id.* at 438.
[175] Id. at 439. Frison's supervision was not constant, but he was typically present at the flea market during its "hours of operation." Id. The fee customers were charged was an entry fee of $1. Id.
[176] Id.
[177] Id.
[178] Id.
[179] Id. at 440.
[180] See id. at 439-440. The sale of counterfeit goods and warnings not to sell said goods occurred from June 2003 up until June 22, 2012 after which this case commenced. Id.
[181] Id. 439.
[182] Id. at 442.
[183] Id. Although not discussed in this article, Frison also argued that the statute was unconstitutionally vague as applied because "law enforcement enforced the statutes arbitrarily." Id.
[184] Id.
[185] Id.

the court believed that a person of ordinary intelligence would have realized that aiding and abetting individuals that were committing willful infringement or trafficking of counterfeit goods should have known that they would be held liable for the same illegal conduct.[186] If this was not enough, the court noted that Frison received multiple warnings and notices that his conduct as the owner and operator of the flea market was unlawful.[187]

Although Frison attempted to assert that he thought he did all he could do to comply with the law, posting signs telling vendors not to sell counterfeit goods and fining vendors that did, the court found this "lip service" to the law unconvincing.[188] The court looked instead to the facts that Frison did not evict violators from the premises, and the fact that Frison actually benefited from fining the vendors.[189] By failing to evict infringers and continuously fining them for their misbehavior, Frison indicated that he both knew the fake merchandise existed, and failed to shut it down, instead choosing to profit monetarily from their illegal activity.[190]

Looking at these facts, the court determined that Frison, and his brick-and-mortar flea market, was correctly convicted for aiding and abetting for the actions of the vendors in his market despite the arguments to the contrary.[191]

3. **Applying Brick and Mortar Laws to E-Commerce Platforms**

The similarities between Frison and the arguments of e-commerce platforms is plain, in a similar way that secondary trademark liability for a flea market owner can be analogized to an e-commerce platform. Using the crime triangle as discussed above, Frison stated that he was not responsible for the actions of the vendors that made use of his marketplace[192] but was found to be complicit in aiding and abetting. A similarity is found with e-commerce platforms claiming no responsibility for criminal activity on their sites. Additionally, e-commerce platforms, similar to *Frison*, take some sort of monetary benefit from the sales of counterfeit goods on their platforms, even if done unwittingly.[193]

It is easy to assert that not all of the factors that the court applied in *Frison* are relevant in the e-commerce space. First and foremost, e-commerce spaces typically attempt to comply with the law in order to avoid later, and more grand liability.[194] Additionally, e-commerce platforms

---

[186] Id.
[187] Id.
[188] Id. at 443.
[189] Id.
[190] See id.
[191] Id. at 444.
[192] Id. at 439.
[193] *Id.*
[194] *Id.*

will often shut down the accounts of individuals found to be selling counterfeit goods.[195] However, these differences may not transcend the overall concept purported by Frison: that marketplace owners should be held accountable for the illegal activity that occurs on its premises, especially when they have an active role in the maintenance of the marketplace and sufficient control over the vendors.[196] Just as the Frison court looked at an abundance of statutes collectively and in light of the conduct that occurred at the Frison flea market, so too should we look at an abundance of statutes in light of the conduct occurring online in the ecommerce space.[197]

The application of the crime triangle here is relevant. Specifically with regard to the three behaviors that we suggest above as e-commerce platforms can engage with sellers and consumers in ways that ensure they have an active role in the maintenance of the marketplace and sufficient control over vendors. If they fail to 1) take active steps to protect consumers on their sites, 2) engage in place management strategies that are designed to make their sites less conducive to counterfeit trade, and 3) remain aware and ahead of the ever-changing curve set by trademark counterfeiters[198] then these factors could potentially influence whether or not they are aiding and abetting.

B. RICO

Profits are one of the main motivators for counterfeiting, and these profits often aid further illicit activity such as additional counterfeiting, terrorism, gang activities and more.[199] However, counterfeiters are not the only ones profiting from the sale of counterfeiters.[200] E-commerce platforms also take a cut out of whatever is sold on their platforms.[201] The question stands whether or not e-commerce platforms could be held accountable for their gains from such illegal activity even once the illegal activity is discovered as stopped, or should be required, or encourage to give these proceeds to consumers or another group of victims of counterfeits.

The Racketeer Influenced and Corrupt Organizations Act was passed in 1970 for the purpose of combating organized crime within the United States.[202] This Act allowed for a shift in how the United States addressed mob related crimes - instead of only being able to charge

---

[195] *Id.*
[196] *See generally* United States v. Frison, 825 F.3d 437 (8th Cir. 2016).
[197] See id. at fn. 2.
[198] *See supra* 21.
[199] See https://www.unodc.org/e4j/en/organized-crime/module-3/key-issues/counterfeit-products-trafficking.html; See also, https://www.govinfo.gov/content/pkg/CHRG-109shrg21823/html/CHRG-109shrg21823.htm
[200] See https://sell.amazon.com/pricing.html; See also, https://pages.ebay.com/seller-center/get-started/seller-fees.html
[201] Id.
[202] https://www.nolo.com/legal-encyclopedia/content/rico-act.html

individual mob and gang members for their involvement in a crime, the government could hold entire organizations accountable for their actions.[203]

The RICO Act not only affects individuals involved in racketeering activity, but those indirectly involved or received money from the activities as well.[204] The language of the statute partially states that it is unlawful for any person who has received any income derived directly or indirectly from a pattern of racketeering activity, to use or invest the proceeds of such income in the operation of any enterprise which is engaged in, or the activities which effect, interstate or foreign commerce.[205] Counterfeiting is also a predicate act under the RICO statute. In a world where e-commerce platforms receive profits from the sale of counterfeits, and invest this money back into their own company, this language is particularly interesting.[206] Even more so, when the charge of aiding and abetting can be adapted to fit RICO charges. Although there have been no noted cases of an e-commerce website being charged under the RICO statute, if the factors above can be proven, it remains a possibility for a claim.

VII. Other Methods of Imposing Liability

Our final section will explore other peripheral possible methods of imposing liability on e-commerce platforms that to date have not been used and we do not believe offer strong cases, but are worth briefly exploring, namely negligence and common law trademark infringement .

A. Negligence Liability for E-Commerce Platforms

Cases dealing with the application of liability under a negligence standard are slim and disheartening at best in the realm of e-commerce platforms. In order for a platform to be held liable in the context of negligence regarding the sale of counterfeit goods, they would have to be willfully blind as to the sale of counterfeits on their platforms or storefronts. Most of the time, these sellers are only found to be negligent in regard to the sale of counterfeits on their platform and therefore are not held liable for such sales.

Further, there is no affirmative duty for platforms to take precautions against the sale of counterfeits in current state law, and the standards for contributory infringement do not impose any duty to seek out and prevent violations.[207] Without a duty imposed upon platforms, a

[203] https://www.justia.com/criminal/docs/rico/
[204] See 18 USCS § 1962
[205] See §1962(a)
[206] https://www.washingtonpost.com/technology/2019/11/14/how-amazons-quest-more-cheaper-products-has-resulted-flea-market-fakes/?arc404=true
[207] See e.g. Hard Rock Cafe, 955 F.2d at 1149 (holding that the standard for contributory liability does not impose a duty to seek or prevent violations); Hendrickson v. Ebay, Inc., 165 F.Supp. 2d 1082, 1095 (C.D. Cal 2001) (holding that e-commerce platforms do not have an affirmative duty to monitor their website for violations); Lockheed Martin Corp. v. Network Solutions, Inc., 175 F.R.D. 640, 646 (C.D. Cal 1997).

negligence claim by itself cannot be brought out against platforms for any damages done to consumers as a result of the sale of counterfeit goods on their platforms and storefronts. Therefore, while imposing tort liability may be possible, there first must be some plausible duty first established in some area of the law.

B. Common Law Trademark

Another consideration in the merging between intellectual property and e-commerce platforms are how to handle common law trademarks. In simplest terms, common law trademarks differ from other trademarks in that common law trademarks are not registered with the USPTO.[208] Practically speaking, however, common law trademarks are much more limited in terms of the actual geographic area the mark is protected in.[209] This geographic limitation has then begged the question: what, if any, protection do common law trademarks receive online?

To answer the question, an analysis of the original justifications for common law trademarks can prove useful. Common law trademarks are so ingrained in intellectual property law that the method of protection existed fifty years before the implementation of the Lanham Act.[210]

Section 43(a)(1)(A) of the Lanham Act[211] provides the legal framework for common law trademark, and the section has only expanded on the allowance of common law trademarks.[212] Initially, the Lanham Act language of "false designation of origin" and "false description or representation" were only meant to apply to representations about the product's origin.[213] The courts had a more liberal reading of this language however, and construed the language to include the source or sponsor of the product, instead of just representations about the product's origin.[214] Most courts considered actions for infringement of unregistered marks on false designation of origin of the marked products, because infringing a common law mark is likely to confuse a consumer about the source of the product.[215] Congress eventually codified that interpretation, and courts also interpreted 43(a) to cover titles of artistic works, elements of a celebrity's identity, and authorship credit, even though those are not technically trademarks.[216]

---

[208] *See* 15 USCS § 1125(a)(making no distinguishment between a registered mark and an unregistered mark in terms of ability to bring a civil action); *see also* Shontavia Johnson, T*rademark Territoriality In Cyberspace: An Internet Framework For Common-law Trademarks,* 29 Berkeley Tech. L.J. 1253, 1255 (2014)
[209] *See* Johnson, *supra* note 153.
[210] Margreth Barrett, *Finding Trademark Use: The Historical Foundation for Limiting Infringement Liability to Uses in the Manner of a Mark*, 43 Wake Forest L. Rev. 893, 902 (2008).
[211] Cited in note 153 as 15 USCS § 1125(a).
[212] Jane C. Ginsburg et. al., TRADEMARK AND UNFAIR COMPETITION LAW, 478 (6th ed., 2017).
[213] *Id.*
[214] *Id.*
[215] *Id.*
[216] *Id.*

Even with the expansion of the original interpretation of Section 43(a), common law trademarks still only provide the mark holder with a limited amount of rights. These rights are also focused around a geographic area, with the specific geographic area being determined by analyzing four "zones" sales, advertising reputation and expansion.[217]

Each of these zones has a separate analysis to determine the geographic scope held by a common law trademark. In order to determine the zone of actual market penetration, courts look for more than a de minimis amount of sales, also analyzing 1: the amount of sales of the product that bear the trademark in the region, 2: growth trends in the specific region, 3: the number of consumers purchasing the product as opposed to total number of consumers in the region and 4: the amount of advertising of the product in the region and 5: the market share of the trademarked good.[218] If the zone of market penetration is limited, the zone of reputation can be used and is meant to show where consumers recognize the product, and can extend further than the immediate geographic location of a storefront.[219] The zone of natural expansion is perhaps the most controversial element to determine the geographic scope of common law trademarks, and allows protection for a common law trademark where the trademark owner has articulable and concrete expansion efforts.[220]

1. Common Law Trademark and the Internet

The internet poses a number of issues when it comes to common law trademarks, and courts are yet to conclusively define the geographic scope of common law trademarks that are utilized on products sold on the internet. Though there has not been a definitive ruling, some courts, in dicta, have suggested that common law trademarks on the internet provide nationwide protection so long as there is an active internet presence.[221]

Recently, a firearm accessory company filed a complaint in federal district court for direct and contributory trademark infringement against an e-commerce platform; included was a claim for relief asserting "common-law trademark infringement and misappropriation of . . . goodwill . . . constitut[ing] unfair competition in violation of Virginia common law."[222] A major issue concerning the protection of common law trademarks mentioned in the complaint is the to-be-defendant's policy of acknowledging only federally registered trademarks in its brand owner support program.[223] Further, the plaintiff's complaint states that not only did the defendant

[217] Johnson, *supra* note 302 at 1259.
[218] *Id.*
[219] *Id.* at 1260
[220] *Id.* at 1261.
[221] *Id.* at 1280.
[222] Complaint for Trademark Counterfeiting, Trademark Infringement, Copyright Infringement, Patent Infringement, and Unfair Competition at 71, Maglula, Ltd. v. Amazon.com, Inc., (E.D. Va. 2019) (1:19CV01570),
[223] Id. at 2-3, 55-6.

"refuse[] to acknowledge . . . well established common law trademarks," the e-commerce platform "went as far as to accuse [plaintiff] of submitting 'inaccurate or invalid' reports."[224] The resolution of this case will provide valuable information for brand owners seeking to protect their common law trademark rights for products sold online. While it is widely acknowledged that federal trademark registration provides broad protections, common law trademark protections still exist to protect a brand's marks within a certain geographical region and brand owners should know to what extent they are able to rely on them for protection against counterfeiters. The court's ruling will impact future litigation where e-commerce defendants have allegedly infringed common law trademarks because of the nationwide reach of their sales activities.

VIII: Conclusion: Potential Way Forward

When looking to the way forward, we suggest that courts, policy makers and the legislature keep in mind that this problem of counterfeit sales by third-party sellers is changing rapidly and will continue to do so. As artificial intelligence continues to be used by brands, e-commerce platforms, service providers and even counterfeiters, the landscape will continue to change. We urge lawmakers and others to keep in mind where appropriate guardianship of the consumer and marks are and might be in the future according to the crime triangle and apply liability accordingly. While this will continue to shift because of technology that we do not currently have and cannot currently imagine, the general framework of the crime triangle and corresponding duties and liabilities to protect a consumer will apply.

[224] Id. at 51.