# Shop Safe Act Affirmative

## File Explanation

This is an affirmative about the trademarks part of the topic. A trademark is a recognizable sign, phrase, or symbol that distinguishes a company’s product from its competitors. The purpose of trademarks is to prevent consumer confusion over what products they are buying.

#### The problem with the status quo.

One of the primary purposes of trademark law is to prevent people from purchasing counterfeit goods by mistake. However, current trademark law makes it very difficult to stop online counterfeiting.

Let’s assume Walmart brick-and-mortar stores start selling iPhones, but they turn out to be counterfeit. While counterfeiting is a felony, Apple may not be able to find whoever supplied the fake iPhones to Walmart. Instead, Apple could sue Walmart for **contributory trademark infringement**. Walmart didn’t make the fake iPhones, but they have a legal responsibility (called “**contributory liability**”) to monitor the products they sell in their stores to make sure they are genuine products. Even if Walmart did not know that the specific counterfeit iPhones were fake, Apple would still prevail in a lawsuit if they can prove that Walmart’s monitoring policies were insufficient. Apple would argue that Walmart may not have known, but they should have known if their enforcement policies were better. The reason counterfeiting is very rare in a physical store like Walmart is that stores are **proactive** about making sure their products are genuine.

Now let’s assume that instead of the counterfeit iPhones being sold in Walmart’s physical stores, they’re instead sold by a third-party seller on Walmart.com. In this case, if Walmart claims they didn’t know the specific phones were counterfeit, they won’t face contributory liability. Federal courts have ruled that contributory trademark liability only applies to online marketplaces if they have specific knowledge of infringement and did not act. The specific decision that ruled this is called *Tiffany v. eBay*, which some of the evidence in this file references.

Apple can try to go after the online counterfeiter directly, but they may not even have information of who the third-party seller is or have a way to sue them if they are in another country. Instead, Apple’s only recourse is to police the online listings of goods themselves and then report any violations they find to Walmart. This is **reactive** enforcement, which has been compared to the game of “Whack-a-mole” – for every listing that Walmart takes down, more pop up in their place.

#### What does the affirmative argue?

This affirmative claims that Congress needs to pass a law called the **SHOP SAFE** **Act**, which would apply stronger contributory trademark liability to online marketplaces. It creates a duty for online platforms to proactively police their marketplaces for counterfeit goods, in the same way that brick-and-mortar stores do right now. If an online marketplace adopts proactive enforcement policies, then they would receive a “safe harbor” from liability. If the online platform fails to develop adequate prevention policies, they could face liability and be sued.

This functions in a way that is very similar to the **Digital Millennium Copyright Act**, which governs liability for online copyright infringement. If someone posts copyrighted material to YouTube without permission, there are automated algorithms that will detect and take down the material. Therefore, YouTube can’t be sued for copyright infringement, because they have prevention policies in place. This affirmative essentially creates a version of the DMCA for trademark law rather than copyright.

**\*If this 1ac is too long to read, there are a couple cards with asterisks at the beginning of them. You can easily skip these cards without losing too much.**

There are two advantages:

#### Advantage 1: Counterfeiting

The thesis of this argument is that online counterfeiting is a serious problem for national security. One of the authors, Patricia Campbell, argues that there is an increased trend of selling counterfeit electronics through e-commerce, and even actors like the Department of Defense, defense contractors, and electric power utilities are incorporating counterfeit electronics into replacement parts. This trend risks creating hardware vulnerabilities in electronics, in the power grid, and in military technology, including weapons. While this might sound implausible, in 2011 a US nuclear submarine base found that it had used 33 counterfeit semiconductors in replacement parts for US nuclear submarines. The affirmative solves this because passing the SHOP SAFE Act will apply trademark liability to online platforms, which will force them to be more proactive and adopt stronger prevention policies.

#### Advantage 2: Money Laundering

This advantage claims that the online trade in counterfeit products is contributing to global money laundering. The counterfeit trade is a more lucrative source of revenue for criminal networks than drugs and human trafficking. While there is a global effort to stop money laundering now, e-commerce is a loophole that allows bad actors to exploit – especially since the risk of detection is very low if online platforms aren’t required to track names, physical addresses, and IP addresses. The advantage claims that a lot of that revenue goes to fund global terrorist organizations. The affirmative plan solves because the type of proactive prevention policies that online marketplaces must adopt would include tracking identities and locations. It also just reduces the amount of money bad actors make if it reduces online counterfeiting.

#### Definitions

These provide background information to this affirmative. It is not essential that you memorize these, but they might help you answer cross examination questions.

**Brands** vs **Platforms** – a lot of evidence refers to the trademark owner selling the product (like Apple) as a “brand”, and refers to the online marketplace hosting third-party sellers (like eBay) as a “platform” for short.

**Contributory liability** – this is a form of secondary liability that holds a third party liable for counterfeiting if they knew about trademark infringement on their platform and did nothing to stop it. Contributory liability applies to trademark counterfeiting now, but it depends on the standard of knowledge that courts apply to determine whether an online platform ‘knew’ infringement was occurring.

**Specific knowledge** – also called “contemporary knowledge” or “actual knowledge”. This is the current standard for determining contributory trademark liability. In the 2nd Circuit case *Tiffany v. eBay* (2010), the court held that eBay’s liability for counterfeit Tiffany products sold on its site required eBay to remove counterfeit listings that were reported to it, but that eBay had no further obligation to police its website, because it lacked specific knowledge of other counterfeiters

 **Constructive knowledge** – also called “reason to know” – this is a standard for determining contributory liability developed in the case *Inwood v. Ives* (1982). *Ives* said that if a (brick and mortar) marketplace had reason to suspect counterfeiting was occurring, whether through multiple notices, widespread reports, or third-party assessments, and the marketplace did not take reasonable precautions, then that marketplace is contributorily liable even if did not know about a specific instance of counterfeiting. Essentially, constructive knowledge is a standard that says you “should have known” illegal activity was taking place, and the reason you didn’t know was that you were negligent.

**Safe harbor** – this means that if an online platform takes proactive enforcement measures, then they are no longer subject to liability. Most safe harbor provisions require specific steps determined by legislation (the Digital Millenium Copyright Act has a copyright safe harbor provision for online platforms based on notice and takedown, for example). SHOP SAFE includes a safe harbor if an online marketplace meets a list of conditions that are explained in the 1ac Dunn evidence on the counterfeiting advantage.

# 1AC

### 1AC - Plan

The United States federal government should significantly strengthen trademark protection by placing contributory liability on online platforms that have constructive knowledge of trademark infringement but fail to implement seller screening, preventative listing review, and enforcement policies.

### 1AC – Counterfeiting Advantage

#### Advantage 1 is counterfeiting

#### Online counterfeiting is skyrocketing – 70% of consumers have bought counterfeit goods through e-commerce.

Alex Tekip, 2023 – staff of MSU Today, “MSU survey: 7 in 10 consumers deceived into buying counterfeit products online” 10/19, <https://msutoday.msu.edu/news/2023/msu-survey-7-in-10-consumers-deceived-into-buying-counterfeit-products-online> //DH

Nearly seven in 10 people were deceived into buying counterfeit products online at least once in the past year, according to new research from Michigan State University.

The study was led by researchers in MSU’s College of Communication Arts and Sciences: Professor of Advertising Saleem Alhabash, Associate Professor of Advertising Anastasia Kononova, Professor of Retailing Patricia Huddleston, and graduate students Moldir Moldagaliyeva and Heijin Lee.

This research comes on the heels of two major anti-counterfeiting legislative actions:

The U.S. Congress passed the Integrity, Notification and Fairness in Online Retail Marketplaces, or INFORM Consumers Act, in June 2023. The INFORM Consumers Act is designed to increase transparency about third-party product sellers and, in turn, reduce the amount of fake and stolen goods sold online.

The Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce, or SHOP SAFE Act, was reintroduced to Congress in September 2023 after it did not go to a vote in 2020 and 2021. The SHOP SAFE Act incentivizes e-commerce platforms to vet sellers and proposes holding these platforms accountable for counterfeit products sold through third parties.

“Counterfeiting goes beyond a fake designer handbag,” said Alhabash. “Counterfeiters outsmart retailers, they figure out vulnerabilities in the supply chain and interrupt it. This causes retailers to lose money and, depending on the product, can pose a threat to the safety and well-being of consumers.”

Clothes and shoes — the most commonly purchased counterfeit items, according to the survey — might pose minimal threats, but even these products may contain harmful chemicals such as lead. Fake versions of items such as airbags and medication most likely do not meet government-determined safety standards, Alhabash said, and can therefore pose a health risk. That’s why he and his team believe it is important to understand shopper behavior, characteristics and motivations to devise effective strategies for educating consumers about the dangers of buying counterfeits online.

This research is the first U.S.-based global survey to provide the anti-counterfeiting and brand protection community — which includes brand owners, e-commerce platforms and law enforcement — with tools and insights to better communicate to consumers the dangers and risks of purchasing counterfeits.

Social media, e-commerce and third-party sellers

Counterfeit products were most commonly purchased via e-commerce websites (39%) and social media (39%). Of the consumers who bought counterfeits on social media, 68% did so on Facebook.

Following the COVID-19 pandemic and the exponential growth in e-commerce, online retail and social media platforms have become a hotbed for counterfeit products, especially as such platforms permit promotion of products by third-party sellers. Counterfeiters understand how the supply chain works, and they repeatedly use online platforms to promote and sell their products to consumers.

Though brand owners and consumers can report counterfeits sold on e-commerce platforms, these after-the-fact efforts, unfortunately, have not curbed the prevalence of illicit counterfeit sales online.

Kari Kammel, director of MSU’s Center for Anti-Counterfeiting and Product Protection, recently testified in the Senate’s SHOP SAFE Act hearings advocating for a balanced approach to regulating third-party sales on e-commerce platforms.

“A proactive requirement of e-commerce platforms that allows third-party sales and responsibility for ‘constructive knowledge’ of counterfeit sales will help balance the burden between intellectual property rights owners and platforms,” Kammel said.

#### If counterfeiting occurred in brick-and-mortar retail, stores would be liable for contributing to trademark infringement. This causes stores to proactively police for counterfeit goods. But online platforms have lower liability. This forces brand owners into reactive, Whack-A-Mole enforcement and increases counterfeiting

Christopher Coons, 2023 – US Senator from Delaware. Senate Judiciary Committee Hearing, “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” 10/3, Proquest Congressional, accessed via University of Michigan //DH

And counterfeit prescription drugs sold to consumers online are, at best, ineffective and at worst, in some cases deadly to those who purchase them. Now, if I unknowingly bought a fake laptop at my local Best Buy, up on Concord Pike, and it then caught fire in my home, BestBuy would be liable for the harm to me and liable to the brand owner for contributing to trademark infringement.

This framework for liability incentivizes brick and mortar stores to thoroughly and proactively vet their supply chains to keep counterfeit products out of consumers hands. Now, that same counterfeit battery bought online is met with a different liability framework. Platforms don't have the same proactive obligations.

In fact, they need not remove a listing until a brand owner tells the platform specifically that the listing is counterfeit. The weight, the onus for policing online counterfeits is principally on brands, not platforms. Under this structure, brand owners have to play a never ending game of Whac-A-Mole as they monitor a multiplying number of online marketplaces for counterfeit listings.

Platforms know they have a counterfeit problem. And many have undertaken laudable anti-counterfeiting efforts. But current efforts are neither effective nor sufficient because the problem hasn't gone away. In fact, it is dramatically increasing and that's why I was proud to reintroduce the SHOP SAFE Act last week with Senator Tillis, a bill that works to try and balance the rights of brand owners and the obligations of online platforms to intercept and stop the sale of harmful counterfeit goods.

The act opens platforms to liability if counterfeit goods affecting health and safety are sold on the platforms, the same liability brick and mortar retailers have been subject to for decades. It requires brand owners to provide platforms with notice of their trademarks and a critical point of contact. So platforms can proactively implement an articulated list of best practices to keep unsafe counterfeits out of consumers online shopping carts.

Those best practices include better vetting before goods are listed, quickly removing counterfeit listings, terminating repeat counterfeiters and requiring accurate images of the products sold. Platforms that follow best practices will have a safe harbor from liability. In other words, platforms taking -- making genuine and good faith efforts to clean up their sites have and should enjoy a liability shield.

#### \*Platforms are liable only if they have specific knowledge of trademark infringement and do nothing about it. This gives them incentives to avoid knowing about it, because they profit from counterfeit sales

Brian J. Winterfeldt, 2021 - Counsel to the Global Brand Owner and Consumer Protection Coalition. Comment submitted to the US Patent and Trademark Office, “RE: Secondary Trademark Infringement Liability in the E-Commerce Setting” 1/25, <https://www.regulations.gov/comment/PTO-T-2020-0035-0022> //DH

E-commerce platforms today are integrally involved in the commercial process – rather than mere conduits for buyers to connect with sellers, many e-commerce platforms actively facilitate sales by categorizing, optimizing, and promoting products and sellers, handling inventory and logistics, shipping, and processing financial transactions. These platforms facilitate access to the US marketplace and US consumers at a level that would otherwise generally be unavailable to international merchants, and which allows sellers within the US and abroad a level of anonymity that brick and mortar retailers in the US are simply not afforded. As a result, the current US legal regime applied to e-commerce platforms has enabled the circumvention of certain aspects of the usual commercial regulatory scheme, which has been unable to keep pace with rapid technological developments.

Currently under US law, online intermediaries are generally not liable for the products sold on their platforms by third parties unless they fail to act upon specific knowledge of particular infringements. Because e-commerce platforms have no affirmative duty to prevent or remedy infringement, there is a strong disincentive for those intermediaries to proactively stop the sale of counterfeits and other harmful products. On the contrary, e-commerce platforms have a strong financial incentive to allow these sales to proliferate, as they make their profit regardless of whether the articles sold are genuine or infringing. Furthermore, many direct infringers using e-commerce platforms are located outside the US, putting them beyond the jurisdiction of US courts and therefore leaving limited recourse to brand owners or consumers impacted by sales of counterfeit or other infringing products by such foreign sellers. Remedies at the border against the import of infringing goods, such as through the International Trade Commission or Customs and Border Protection, are often practically infeasible when attempting to stop the flow of small parcel shipments that are commonly used by international counterfeiters – especially where their products are intermingled with other supplies by e-commerce providers or shipped using the e-commerce providers’ own branded packaging.

Accordingly, there is a grave imbalance in terms of the risks and responsibilities as between brand owners, consumers, and online marketplaces. We strongly believe that changes to the US legal regime of secondary liability are needed to remedy these issues. In addition to this general input, please find our specific responses to the questions presented in the Federal Register notice below.

1. Is the doctrine of secondary infringement liability, as currently applied by the courts, an effective tool in addressing the problem of the online sale of counterfeit goods? If not, please identify the shortcomings in this approach to combatting counterfeits sold online, including whether the shortcomings are general to all goods and modes of e-commerce or whether they are specific to a particular type of goods or e-commerce.

The doctrine of secondary infringement liability as currently applied by the courts1 is not an adequate tool in addressing the problem of online sales of counterfeit goods. The current doctrine, as applied to the e-commerce setting, is not effective because: (1) proving specific knowledge is difficult for trademark owners and inconsistent across jurisdictions, and (2) the burden of online enforcement is disproportionately on trademark owners.

The time burden and financial cost to brand owners to meaningfully provide specific knowledge as to each and every instance of infringement across every e-commerce platform is prohibitively high. Even with unlimited resources, it would be impossible to constantly monitor for and identify each incident of infringement across all platforms, particularly for large brand owners with dozens or even hundreds of individual brands. The specific knowledge requirement encourages platforms to turn a blind eye toward monitoring their own ecosystems, to avoid liability based on specific knowledge generated through their own review. General awareness of infringement on the platform is not sufficient to trigger any platform obligations, and some courts have found that programs employed by certain platforms to promote infringing goods, the practice of co-mingling of counterfeit and genuine goods, and the fulfillment of goods by the platform itself, still fail to trigger secondary infringement liability.

As a result, nearly full responsibility for policing the vast online e-commerce ecosystem falls squarely on individual brand owners. This involves deploying complex technological solutions and human capital to trawl the multitude of e-commerce platforms, identify potential infringements and weed out false positives, and provide notice or pursue other enforcement action as to each individual incidence of infringement. For large brand owners, this involves a combination of automated and manual review of tens of thousands of listings per month. This is a substantial drain on brand owner resources, while e-commerce platforms are left to benefit from continued sales of infringing material. It is clear that market forces, standing alone, are not sufficient to change platform behaviors in this regard.

Some platforms are taking steps to try and mitigate infringement beyond the minimum notice and takedown approach. Our members are very grateful for such initiatives, but in our experience these are often designed to provide an appearance of credibility and utility while stopping short of meaningfully preventing infringement on a large scale. Thus, changes to the secondary liability legal regime are necessary to redistribute the burden of preventing and addressing counterfeiting and other infringement through e-commerce platforms, so there is greater responsibility-sharing among platforms along with brand owners to ultimately protect consumers.

#### E-commerce is driving the spread of counterfeit electronics, creating cyber-vulnerabilities in supply chains for the Department of Defense

Patricia E. Campbell, 2023 - Law School Professor and Director of the Intellectual Property Law Program at the University of Maryland Carey School of Law “Debugging the Trademark Laws: The Lanham Act and Counterfeit Microelectronics,” 31 TEX. INTELL. PROP. L.J. 211 (2023). Hein Online. Accessed via University of Michigan //DH

C. Counterfeiting is a Lucrative Proposition

Numerous explanations for the counterfeit electronics problem have been discussed. Profit has long been identified as the "primary incentive" for the sale of counterfeit parts.83 The internet and the rise of e-commerce platforms has made counterfeiting even more lucrative; "production costs are low, millions of potential customers are available online, transactions are convenient, and listing on well-branded e-commerce platforms provides an air of legitimacy."84 In addition, when the sellers of counterfeit goods are in another country, as is often the case, they are largely outside the jurisdiction of criminal prosecution by U.S. law enforcement and may be immune from civil liability to private parties. 85 Thus, the perceived risk is low.86

Further, the supply chain disruptions and chip shortages caused by the Covid-19 pandemic have only intensified the problem. Counterfeiters have "stepped up their game to swindle enterprises in dire need of the critical components."87 Reputable firms in need of chips have been enticed to order hard-to-find parts from risky sources, and they have received shipments that are improperly packaged, defective, or even nonoperational.88 According to the Wall Street Journal, "[t]he global chip shortage has created a gold mine for bad actors."8 9 Counterfeit semiconductors, including diodes, are being incorporated into mobile phones, tablets, and other privately used electronic devices, creating risks for consumers.90 Long manufacturing lead times for semiconductor chips have increased the willingness of distributors to go to the open market to obtain parts for customers in order to prevent manufacturing lines from sitting idle. 91

Government contractors and the DoD present a particularly attractive-and oftentimes willing-market for counterfeiters, largely due to the obsolescence of necessary replacement parts. 92 Unlike commercial products such as cellphones and laptop computers, defense systems are typically designed for long lifecycles. 93 Production of the parts contained in those systems will be discontinued when it is no longer cost-effective for the manufacturer, usually long before the systems themselves are taken out of service, leading to diminishing manufacturing sources and material shortages (DMSMS) issues. 94 When production ends, parts may no longer be available from the original component manufacturer, an authorized aftermarket manufacturer, or an authorized distributor. 95 If sufficient end-of-life purchases were not made, 96 the DoD and defense contractors may be forced to purchase replacement parts from outside the authorized supply chain, including from brokers and independent distributors. 97 The DoD estimated that as much as 15% of all spare and replacement parts for military electronics are determined to be counterfeit. 98 The military's emphasis on using the lowest cost suppliers rather than focusing on the quality of parts obtained is another contributing factor. 99

Economic gain is not the sole motive for dealing in counterfeit electronics. As noted above, malicious counterfeits are making their way into the supply chain. 100 As an increasing number of devices are connected to the Internet of Things (IoT), "the potential for extensive economic and health and safety losses due to deliberately corrupted components increases by orders of magnitude. 101

#### \*Supply chain vulnerability risks hardware sabotage causing catastrophic failure in critical infrastructure and DOD weapons systems

Patricia E. Campbell, 2023 - Law School Professor and Director of the Intellectual Property Law Program at the University of Maryland Carey School of Law “Debugging the Trademark Laws: The Lanham Act and Counterfeit Microelectronics,” 31 TEX. INTELL. PROP. L.J. 211 (2023). Hein Online. Accessed via University of Michigan //DH

More recently, clones and tampered parts with malicious insertions have become part of the counterfeiting problem, leading to national security concerns.68 Clones, or unauthorized reproductions of authentic parts, may be produced through reverse engineering, resulting in exact duplicates of the original part, or they may be form-fit-function equivalents (i.e., conforming products, but not exact duplicates) that are passed off as authentic products. 69 In either case, one concern is that the clone might function in ways that the original product did not, potentially leading to extremely dangerous results. For example, a timer could be inserted that would cause the chip to fail at a certain time, or it could be programmed to fail in response to certain stimuli .70

Tampered parts, on the other hand, are parts which have been intentionally modified for sabotage or malfunction.71 Tampered parts pose advanced threats to critical infrastructure and national security:

Parts of this category would likely be state sponsored by adversary countries and could have dangerous or catastrophic consequences for systems that incorporate them. Consequences include but are not limited to denial of service of a critical function of the system, side-channel attacks that enable loss of sensitive or critical information, premature or latent failure, or unauthorized access to proprietary data or system functionality. 72

It is somewhat unclear whether tampered microelectronics have already infiltrated the supply chain,73 or whether the current dangers associated with tampering are still limited to software residing on more complicated assemblies and equipment such as servers.74

The U.S. government recently acknowledged that it faces potentially catastrophic risks from all types of counterfeit electronic parts:

Counterfeits are not produced to meet higher-level quality standards required in mission critical applications and are a significant risk in causing failure to systems vital to an agency's mission. For weapons, space flight, aviation, and satellite systems, these failures can result in the [sic] death, severe injuries, and millions of dollars in system damage or loss. For example, if counterfeits are installed in a missile's guidance system, such missile may not function at all, may not proceed to an intended target, or may strike a completely unintended location resulting in catastrophic losses. Critical nonconforming and counterfeit items may cause failures in navigation or steering control systems, planes and flight control. Counterfeits can create "backdoors" into supposedly secure programmable devices which could be exploited to insert circuit functions to steal information and relay it to third parties or command or prevent the device from operating as designed. Defense, space, and aviation systems in particular must meet rigorous component specifications: failure of even a single one can be catastrophic causing serious problems and placing personnel and the public in harm's way.75

#### These supply chain vulnerabilities risk nuclear war through attacks on the power grid or attacks on weapons systems

Michael Klare, 2023 – Senior Visiting Fellow at the Arms Control Association. From 1985 to 2018, Dr. Klare served as the Five College Professor of Peace and World Security Studies, a joint appointment at Amherst, Hampshire, Mount Holyoke, and Smith Colleges and the University of Massachusetts, Amherst “Assessing the Dangers: Emerging Military Technologies and Nuclear (In)Stability” February, <https://www.armscontrol.org/sites/default/files/files/Reports/ACA_Report_EmergingTech_digital.pdf> //DH

**C3 refers to Command, Control and Communications systems**

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great-power crisis to paralyze the vital command, control, and communications (C3) capabilities of an adversary, many of which serve both nuclear and conventional forces. Given the heavy reliance placed by senior officers on reliable and extensive C3 systems to track enemy actions and oversee countermoves by their own forces, the incapacitation of these networks through cyberattacks at the very onset of battle would, presumably, convey an enormous advantage to the attacking side. In the “fog of war” that would naturally ensue from cyberattacks of this sort, the recipient of such an assault might anticipate more punishing follow-up kinetic attacks, possibly including a preemptive strike on its nuclear deterrent capabilities. Fearing the possible loss of those capabilities, the nation under assault might place its nuclear weapons on high alert and, in the worst case, launch them in response to ambiguous signs of attack. This might occur, for example, in a confrontation between NATO and Russian forces in eastern Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking, for example, of a possible confrontation in Europe, James N. Miller Jr. and Richard Fontaine of the Center for a New American Security wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If those early attacks succeeded, “it could result in [a] huge military and coercive advantage for the attacker.” This scenario might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical C3 infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities, and so choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.” 123

What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation: simply by their presence, they could sow doubts in the minds of adversary leaders regarding the reliability of their NC3 systems. “The introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” thereby undermining strategic stability, Page O. Stoutland and Samantha Pitts-Kiefer wrote in a 2018 paper for the Nuclear Threat Initiative. Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state might misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike.124

Compounding these dangers, in the view of many analysts, is the widespread integration of nuclear C3 with conventional command, control, and communications systems. For reasons of convenience and economy, the major powers have chosen to rely on the same early-warning and communications links to serve both their nuclear and conventional forces—a phenomenon described by James Acton of CEIP as “entanglement.” In the event of a great-power conflict, one side or the other might employ its cyberweapons to confuse or disable its adversary’s conventional C3 in the opening stages of a nonnuclear assault; but the recipient of such attacks, not knowing whether it is conventional or nuclear systems that are the intended targets, might fear it is the latter and so prepare for immediate nuclear operations, again risking early weapons use.125

Yet another pathway to escalation might arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure, rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. Russia, for example, is believed to have infiltrated the U.S. electrical grid, and it is widely assumed that the United States has done the same in Russia.126

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread harm and eventually leading one side or the other to initiate kinetic attacks on critical military targets, possibly initiating a spiral of escalation ending in nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, Miller and Fontaine argue, such attacks “could lead to major conflict and possibly nuclear war.”127

#### The plan solves by adopting a “constructive knowledge” standard for trademark infringement. This means online platforms have a duty to police if they should have known counterfeiting was occurring, even if they did not have knowledge of specific acts of infringement.

Patricia E. Campbell, 2023 - Law School Professor and Director of the Intellectual Property Law Program at the University of Maryland Carey School of Law “Debugging the Trademark Laws: The Lanham Act and Counterfeit Microelectronics,” 31 TEX. INTELL. PROP. L.J. 211 (2023). Hein Online. Accessed via University of Michigan //DH

Instead, Congress must enact legislation that more generally addresses the level of knowledge required for a finding of contributory infringement by any party that facilitates acts of counterfeiting and trademark infringement; it should not be limited to e-commerce platforms. The new legislation should overturn the Tiffany requirement (the de facto standard throughout the U.S.) whereby a service provider must have contemporary knowledge of which particular listings are infringing before contributory infringement can be found.418 Constructive knowledge of infringement should be sufficient to give rise to a duty to investigate and stop the infringing conduct.

In Luxottica Group, SPA v. Airport Mini Mall, LLC, the Eleventh Circuit recently affirmed a jury verdict finding defendants liable for contributory trademark infringement where they knowingly facilitated infringement by others. Luxottica and its subsidiary Oakley alleged that the defendants operated a shopping mall in Georgia containing approximately 130 booths leased to vendors, many of which sold counterfeit products including the plaintiff's sunglasses. 4 19 Despite three law enforcement raids, two letters from Luxottica, and a meeting with local police, the defendants took no steps to determine which tenants were selling counterfeit sunglasses or to evict the infringing tenants.420 The district court found the defendants liable for contributory infringement and awarded $1.9 million in damages, and the Eleventh Circuit affirmed. The court determined that contributory infringement could be found where "the defendant ([a]) supplies a product to the direct infringer whom it 'knows' is directly infringing (actual knowledge); or ([b]) supplies a 'product' to a direct infringer whom it 'has reason to know' is directly infringing (constructive knowledge)." 42 1

The Luxottica court explained that constructive knowledge can be demonstrated in several ways. Willful blindness is only one form of constructive knowledge for contributory trademark infringement.422 The defendants argued that under Tiffany, they could only be liable for contributory infringement if Luxottica provided them with notice of which particular vendors were selling counterfeit products, but the court disagreed. It found that Tiffany did not categorically shift the burden onto trademark owners to provide notice to defendants. 423 Instead, both "actual [and] constructive knowledge of the direct infringers' identities could arise from many sources, including steps the defendants could have taken to investigate . . infringement ... after being put on notice ... that [unidentified vendors] may have been selling counterfeit Luxottica products." 424 The court concluded the trial evidence was sufficient to prove the defendants had at least constructive knowledge of specific instances of infringement, since Luxottica's letters might have prompted a reasonable landlord to conduct at least a cursory inspection. 425 In addition, evidence of serious and widespread infringement (in this case, three law enforcement raids) made it far more likely defendants knew about the infringement. 426 Following Luxottica, even the Second Circuit has agreed that actual knowledge of a specific infringer is not required in all cases.427 A defendant may be willfully blind to particular transactions or to the identities of infringers, and a defendant may be liable for contributory infringement despite not knowing the identity of a specific vendor who was selling counterfeit goods.428

The Tiffany standard for contributory liability-requiring contemporary knowledge of which particular listings are infringing-improperly allows ecommerce platforms to insulate themselves from liability. Online marketplaces organize their operations in such a way as to avoid contemporary knowledge and then essentially suggest that they are too large to know which listings are infringing, all the while profiting from every sale by their sellers. 429 The burden is disproportionately placed on brand owners to continually screen platforms, seek out listings that are potentially counterfeit, and send takedown notices to the platforms. 430 It has been repeatedly described as a game of "whack-a-mole." 431 Further, by the time the infringing listings are removed, the items may have already been sold, and new listings may have appeared. That is out of touch with today's world. 432 It has led to a flood of counterfeit products, including counterfeit microelectronics, being sold on the internet, and the result is lost sales by original manufacturers, damage to brands, and threats to public health and safety.

The Lanham Act should be amended to specifically recognize contributory liability for anyone who knowingly facilitates direct infringement by a third party. That should include an online marketplace that "continues to supply its [service] to one whom it knows or has reason to know is engaging in trademark infringement." 33 "Reason to know" (i.e., constructive knowledge) of infringing activity should be context-dependent and could be demonstrated in multiple ways, including sample purchases that were identified as counterfeit, unusually large numbers of listings for an item, unexpectedly low prices, suspicious images, law enforcement raids, and other indicators. Requiring actual knowledge of specific infringing acts is not the correct standard. Imposing liability when an intermediary has constructive knowledge that infringing activity is occurring will redistribute the burden and force e-commerce platforms to bear partial responsibility for identifying and curtailing that activity. It could also encourage electronic parts manufacturers to pursue civil actions against online purchasing platforms hosting vendors of counterfeit parts.

#### The plan’s requirements of proactive enforcement creates a safe harbor from liability for any platform that complies. This substantially reduces counterfeiting

Hayley Dunn, 2021 - Maryland licensed attorney who holds a J.D., cum laude, from the Catholic University of America, Columbus School of Law. At time of writing, served as a judicial law clerk to the Honorable Laura S. Ripken of the Court of Special Appeals of Maryland. “What's in Your Box? Removing the Tiffany Standard of Knowledge in Online Marketplaces,” 29 Cath. U. J. L. & Tech 91 (2021). Available at: <https://scholarship.law.edu/jlt/vol29/iss2/6> //DH **italics in original**

Although the cause of action in the proposed statute above addresses all products, there is proposed legislation that speaks directly to products in online marketplaces that implicate health and safety. On March 2, 2020, the House Committee on the Judiciary introduced the Stopping Harmful Offers on Platforms by Screening Against Fakes in E-commerce Act of 2020 (SHOP SAFE Act of 2020).284 The SHOP SAFE Act would hold online marketplaces “contributorily liable for infringement by a third party seller” when the seller’s infringement “implicate[s] health and safety,” unless the online marketplace takes a series of measures.285 The measures fall into three categories: seller screening, preventative listing review, and enforcement.286

The Act requires online marketplaces to verify the identity of sellers with reliable documentation, such as a government identification.287 Additionally, online marketplaces must ensure the seller is available for service of process in the United States.288 Online marketplaces must require sellers to attest to the authenticity of their listings; to provide their contact information, identification, geographic location; and to use images they own or have permission to use.289 These provisions would help curb the anonymity of third party selling, which makes suing a seller for trademark infringement near impossible in online marketplaces.290

The proposed legislation also requires online marketplaces to use “proactive technological measures” to screen goods before displaying them to the public in order to ensure that there are no trademark infringements.291 This would place an affirmative obligation on online marketplaces to actively police their websites, rather than solely rely on individual complaints of infringement.292

Online marketplaces have enforcement responsibilities under the Act.293 First, they must have a “program to expeditiously disable or remove from the platform” a reported infringement by an individual.294 All major online marketplaces already have such systems in place, although the particular procedures in each vary.295 The individual reporting, coupled with the online marketplace’s proactive preventative measures, may help decrease the prevalence of counterfeit goods.296 Second, when an online marketplace takes down three separate listings from an individual seller, they must ban the seller from the website and ensure the seller cannot re-enter the online market under an alias.297 This provision works to curb the common problem of suspended sellers constantly creating new accounts to relist their counterfeit products.

The Act takes a significant step towards curbing the detrimental effects of counterfeit products. The most significant change from the status quo is the seller verification process and mandate to consent to U.S. jurisdiction. Furthermore, the requirement for online marketplaces to proactively police their websites for infringements *prior* to a listing going live for consumers may dramatically decrease infringements. However, the “technological measures” for websites to take are undefined, and the review of these processes for compliance is unknown. Additionally, under the Act, contributory liability is limited to counterfeit goods “that implicate health and safety,” which excludes a large amount of goods—such as Tiffany jewelry—the very goods that began the battle for online contributory trademark infringement over fifteen years ago.298 The SHOP SAFE Act is a monumental step forward for addressing online marketplace counterfeits and protecting consumers and rights holders.299 The Act was placed on hold given the COVID-19 pandemic and would need to be re-introduced in the new congressional session. Ironically, the pandemic has emphasized the critical need for this legislation now more than ever given counterfeit PPE.300 While it is limited in scope and has undefined terms, the Act may pave the way for broader legislation that could protect trademark owners and consumers alike.

### 1AC – Money Laundering Advantage

#### Advantage 2 is money laundering

#### E-commerce counterfeiting is the largest criminal enterprise in the world and the US is the largest market

Kari Kammel, 2023 - Director of the Center for Anti-Counterfeiting and Product Protection (“the A-CAPP Center) at Michigan State University. Statement to the US Senate Committee on the Judiciary, IP Subcommittee, “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” <https://www.judiciary.senate.gov/imo/media/doc/2023-10-03_-_testimony_-_kammel.pdf> //DH

While trademark counterfeiting has been around for many years, the scope of the problem has changed dramatically with the advent of online shopping. The sale of goods in online marketplaces, both licit and illicit goods, has grown exponentially in the past decade;3 and particularly since the onset of COVID-19, consumers have increasingly shopped online.4

The United States leads the world in total e-commerce sales and business to business sales, and is second in the world in business to consumer sales.5 With virtual storefronts and easy online transactions, online marketplaces give businesses of all sizes the opportunity to achieve global profits and reach previously inaccessible consumers, and also give consumers access to products delivered to their door that they might not be able to find in local markets.

However, counterfeiters also take advantage of the opportunity online marketplaces provide them and rely on the brands’ goodwill and reputation to create counterfeit products to reach often unwitting consumers. The sale of counterfeit goods remains low risk to the counterfeit sellers-much lower risk than selling in a brick-and-mortar venue. Counterfeit items previously sold in flea markets and on the street or in bodegas are now sold in volume on online marketplaces, social media pages, apps, and the dark web.6

The volume of counterfeits is staggering but also difficult to measure for a variety of reasons. First, it is an illicit activity that is often focused on deception. Second, the most accurate data we have is from seizure data. The U.S. Customs and Border Protection’s Intellectual Property Rights Seizure Statistics report for the 2021 fiscal year reported that CBP had 102,490 seizures with an estimated manufacturer’s suggested retail price (MSRP) of over $3.3 billion.7 The size of the problem is often calculated based on seizure data, or takedown data, which does not fully reflect the universe of counterfeit goods.8 Third, data sharing between brands, platforms, law enforcement and academia has always been a struggle. However, despite these limitations, estimates of counterfeiting profits globally by Global Financial Integrity state that it is financially the largest criminal enterprise in the world, approximately $923 billion to $1.13 trillion a year—a higher amount than either drugs ($426-652 billion) or human trafficking ($150.2 billion).9 Financially, counterfeit goods impact national economies; counterfeit and pirated goods in international trade have been estimated to amount to as much as USD 464 billion in 2019, or 2.5% of world trade that year.10

#### Transaction laundering through e-commerce is undermining anti-money laundering enforcement

Eray Arda Akartuna et al, 2023 - Department of Security and Crime Science, University College London “The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review” Security Journal (2023) 36:615-650, <https://link.springer.com/content/pdf/10.1057/s41284-022-00356-z.pdf> //DH

**ML = Money Laundering, TL = Transaction Laundering**

Transaction laundering

Transaction laundering (TL) is similar to digital invoice manipulation. However, it can be considered an 'offshoot trend' for numerous reasons. TL involves diverting illicit (often Dark Web) transactions (such as for drugs or firearms) through a front company with a merchant account, thus allowing them to be invoiced as transactions for legitimate goods/services (Chattopadhyay 2018). Upon agreeing a price for illicit drugs on the Dark Web, for example, a buyer would be rerouted to a legitimate looking e-commerce site where they would make an 'order' for innocent-looking items that do not actually exist (such as books or clothes), which would in fact be payment for the illicit goods/services agreed. Oblivious payment service providers then process and thus inadvertently launder these funds.

TL can involve setting up a front business or using a 'pass-through' business willing to offer its merchant account for illicit use (Trulioo and PYMNTS.com 2020b). Having passed the often extensive onboarding procedures for acquiring a merchant account, these businesses are in high demand by criminals who do not have the capabilities to fool payment service providers and pass the necessary checks to obtain one themselves. An example of a TL scheme, disguised through an e-bookstore, is shown in Fig. 6.

TL poses serious dangers that are less evident than other trends. Firstly, TL typically enlists a willing criminal entity to process transactions, rather than a legitimate service or mobile app. Therefore, a crucial node of possible detection, i.e. internal fraud departments, is lost. Secondly, TL effectively merges the predicate offence (such as illegal drug distribution) and the laundering of its proceeds into one transaction. Illicit funds are essentially laundered as they are generated. Finally, the relevant stakeholders or risk characteristics for TL are substantially vague, as virtually any online site with e-commerce capabilities is at risk.

Due to its elusiveness, TL has been referred to as the 'least enforced' form of contemporary ML (Teicher 2018b), and as a 'huge financial blindspot' (Kaminska 2017). TL-related technological developments are worrying. For example, with some payment service providers now accepting cryptocurrency payments, TL can now occur in the decentralised DLT ecosystem with even less detection possibilities.

#### E-commerce counterfeiting is fueling terrorism, organized crime and global kleptocracies

David Luna, 2021 – founder and executive director of ICAIE, CEO of Luna Global Networks & Convergence Strategies LLC, and a former U.S. diplomat and national security official with over 20 years of federal service. “Why We Must Confront the Growing Threat to National Security Posed by Illicit Economies and Cesspools of Corruption and Organized Crime” <https://www.linkedin.com/pulse/why-we-must-confront-growing-threat-national-security-david-m-> // DH

Illicit economies are not harmless and can have tremendous human, economic, societal and security costs and consequences.

Illicit economies come with vulnerabilities to peace and security — including corruption, violence, chaos, organized crime, terrorist financing and instability. Illicit economies are the lifeblood of today’s bad actors, enabling kleptocrats to loot their countries, criminal organizations to co-opt states and export violence and terrorist groups to finance their attacks against our societies.

Illicit economies are pervasive threats that undermine democracy, corrode the rule of law, fuel impunity, imperil effective implementation of national sustainability and economic development strategies, contribute to human rights abuses and enflame violent conflicts.

Across today’s global threat environment, criminals and bad actors exploit natural disasters, human misery and market shocks for illicit enrichment.

The lucrative criminal activities enabling and fueling the multitrillion-dollar illicit economies include the smuggling and trafficking of narcotics, opioids, weapons, humans, counterfeit and pirated goods; illegal tobacco and alcohol products; illegally harvested timber, wildlife and fish; pillaged oil, diamonds, gold, natural resources and precious minerals; and other contraband commodities. Such contraband and illicit goods are sold on our main streets, on social media, in online marketplaces and on the dark web every minute of every day. The United Nations has estimated that the dirty money laundered annually from such criminal activities constitutes up to 5 percent of global gross domestic product, or $4 trillion.

The International Coalition Against Illicit Economies recognizes that illicit economies and crime convergence are threat multipliers that ripple across borders and imperil supply chain security, market integrity, democratic freedoms and institutions and systems of open, free and just societies.

In Mexico and Central America, for example, organized crime infiltrated the government at every level, and has diversified into other sectors such as agriculture, mining and transportation. Criminals also control strategic and critical infrastructure such as the country’s major ports. In recent years, the Jalisco New Generation Cartel has killed judges, police officers, politicians and thousands of civilians. Gangs like MS-13 and the Mexican cartels also remain a significant threat across the United States.

The significant market penetration of the Latin cartels has resulted in illicit economies that have corrupted and destabilized Mexico’s justice system and rule of law, and threaten regional stability. Their reach is now global, expanding to other regions of the world like Africa, Europe, and the Asia-Pacific.

China’s involvement in the expansion of illicit economies — including the booming trade in fraudulent consumer goods, money laundering/trade-based money laundering and the corruptive and malign influence of the Chinese Communist Party — continues to harm American national interests, our economy and competitiveness and the health and safety of our citizens.

In Africa, authoritarian governments, ungoverned spaces and conflicts have created the perfect storm for criminals and terrorist groups to expand their illicit trafficking and smuggling operations. The lucrative business of illicit trade has also been militarized in some areas, bribing complicit government officials to shield illicit enterprises from scrutiny and coercing soldiers to protect the illicit markets.

In other parts of the world – from Southeast Asia to the Caucasus – ruthless corrupt leaders and malign actors are similarly engaging in criminality and undermining global security, financing criminalized markets and creating illicit economies.

According to Euromonitor, while COVID-19 has brought economic malaise to most sectors, the illicit economy continues to accelerate, especially across the digital world. E-commerce platforms and online marketplaces are generating tremendous prosperity for scammers, fraudsters, counterfeiters and other predatory criminals that are raking in tens of billions of dollars selling fake pharmaceuticals and vaccines, personal protective equipment, counterfeit apparel and footwear, copyrighted electronics knock-offs and other illicit goods. Recent Organisation for Economic Co-operation and Development estimates put sales of fake goods and pirated products globally at $464 billion per year, with the International Trademark Association projecting that such illicit trade could reach up to $2.3 trillion by 2022.

These illicit economies divert revenue from legitimate market drivers such as businesses and governments and impair the ability of communities to make the investments necessary to stimulate economic growth, especially during these hard economic times. Revenue that could be used to build roads to facilitate commerce, hospitals to fight pandemic outbreaks and diseases, homes to raise and protect families or schools to educate children and future leaders, is instead lost to criminals’ greed crimes.

But this goes beyond just economic harm. Illicit economies incur a significant negative social cost, and in some cases, help to foment market instability, enslave our human capital, pillage our natural world and endanger national efforts to implement sustainable development goals.

#### \*Kleptocracies are threat multipliers that increase terrorism and global conflict

David M. Luna, 2023 - founder and executive director of the International Coalition Against Illicit Economies, and a former U.S. diplomat and national security official with over 20 years of federal service. S4D Working Group on Kleptocracy and Illicit Finance Dialogue “Dialogue II: Investigating and Prosecuting Kleptocrats and Complicit Enablers,” Final Report, 3/2, <https://traccc.gmu.edu/wp-content/uploads/2023/03/S4D-WG-Kleptocracy-and-Illicit-Finance-Dialogue-2023-FINAL-REPORT-2-MARCH-2023.pdf>

In numerous parts of the world, kleptocrats continue to “use political power to appropriate the wealth of their nation”.2 Such great illicit wealth through corruption and criminality acts as a threat multiplier and is financing an array of conflicts, violence, market chaos, and global instability. Kleptocracy remains a pervasive threat to democracy, corroding the rule of law, fueling impunity, imperiling effective implementation of national sustainability, undermining poverty alleviation and economic development strategies, contributing to human rights abuses, and enflaming insecurity in many regions.

“When government officials abuse public power for private gain, they do more than simply appropriate illicit wealth. Corruption robs citizens of equal access to vital services, denying the right to quality healthcare, public safety, and education. It degrades the business environment, subverts economic opportunity, and exacerbates inequality. It often contributes to human rights violations and abuses, and can drive migration. As a fundamental threat to the rule of law, corruption hollows out institutions, corrodes public trust, and fuels popular cynicism toward effective, accountable governance.”3

According to Oxford Dictionary, kleptocracy is defined as the “rule of thieves”, or a “government by people who use their power to steal their country resources.” Across today’s geo-security landscapes, kleptocrats, tyrants, autocrats - and their enablers - exploit every opportunity to leverage power, and to enrich themselves through corruption, fraud, embezzlement, illicit trade, money laundering, and other forms of crime.

In a complex, more dangerous world, and with democratic backsliding in some corners, kleptocracy has been increasing around the world and “most countries are failing to stop corruption “:4

“As global peace has been deteriorating for 15 years, corruption has been both a key cause and result of this.”

As they embark on such criminality, in too many places around the world, kleptocracies further weaponize corruption, and contribute to increased inequality, insecurity, and instability. In democracies where kleptocracy takes hold, unjust power systems enable economies to spiral downwards into failed states, conflict zones, or terrorist- or criminally-controlled ungoverned spaces.

“… in too many places around the world, kleptocracies further weaponize corruption, and contribute to increased inequality, insecurity, and instability.”

For example, the current unjust war in Ukraine sheds greater light on how President Putin, Kremlin leaders, and oligarchs have not only pillaged Russia’s natural resources, but have used such wealth to finance other conflicts in Syria, Crimea, and malign influence in Central African Republic, Mali, Eritrea, and other African states through their mercenary group, the Wagner Group. Recent sanctions related to Russia’s invasion of Ukraine by the United States, the European Union (EU), and other countries, have targeted the assets of Russian kleptocrats including fine real estate, sports teams, hotels, private yachts, jets, and other luxury possessions, as well as their numerous banking accounts.

Professional gatekeepers and enablers have helped kleptocrats and corrupt officials to hide their assets and launder them across financial safe havens around the world through anonymous shell companies, opaque investments, and other legal mechanisms. Often, kleptocrats will work with enablers through offshore banking with shell companies or trusts that contain valuable real estate or other assets. These professional facilitators and enablers include bankers, lawyers, accountants, wealth managers, art dealers, investment advisors, real estate agents, trust creators, company incorporators, gold and diamond traders, money laundering firms, and other service-based providers.

Thus, power and illicit wealth are the lifeblood of today’s kleptocrats, enabling autocrats to loot their countries of staggering amounts of wealth, co-opt democracy, foment violence, undermine liberty, and curtail the freedoms of their people. They also help to corrode the rule of law, fuel impunity for criminals, imperil effective implementation of national sustainability and economic development strategies, contribute to human rights abuses, and enflame violent conflicts.

Corrosive capital, dark money, and illicit finance--particularly when related to authoritarian states--pose direct threats to democracies, societal stability, market security, and the global financial system. This is especially true when autocrats engage in illicit activities with criminal oligarchies, state-sponsored criminal groups, complicit enablers, and other threat networks to launder dirty money to finance malign actions that destabilize the national interests of Western powers, the stability of nation-states, world order, and the security of the international system.5

When corrupt ruling elites, their families, and business associates conspire with criminals, they manipulate weak governance structures to erode judicial independence and quash anticorruption investigations and the rule of law so that democracy cannot take hold.

Increasingly, autocrats and kleptocrats borrow from each other’s practices to sustain their power and illicit behaviors, provide an alternative governance model, and destabilize Western norms and values. These are existential threats to democracies. In large part due to the extraordinary efforts of investigative journalists, civil society groups, the G7, INTERPOL, and efforts by law enforcement and financial intelligence units, and exposés such as the Panama, Paradise, and Pandora Papers, we are more informed of the breadth and scale of brazen kleptocrats’ thievery. For example, we have learned of hundreds of billions of dollars that were stolen in Angola, Democratic Republic of the Congo, Equatorial Guinea, Haiti, Hungary, Indonesia, Malaysia, Nigeria, Nicaragua, Peru, Philippines, Russia, Venezuela, Ukraine, and many other countries. An interesting point among these kleptocracies is not only how often many of them will do business with one another, but how collectively they have also helped to create a community of enablers across secrecy havens, financial safe havens, and banking centers (e.g., New York City, Dubai, London, Hong Kong, Sydney, etc.).

#### Terrorism risks are growing rapidly, and risk nuclear use

National Academies of Sciences, Engineering, and Medicine. 2024. Nuclear Terrorism: Assessment of U.S. Strategies to Prevent, Counter, and Respond to Weapons of Mass Destruction. June, <https://nap.nationalacademies.org/catalog/27215/nuclear-terrorism-assessment-of-us-strategies-to-prevent-counter-and> //DH

**IND = Improvised Nuclear Device, RDD = Radiological dispersal device, RED = Radiological explosive device**

NEW DYNAMICS IN NUCLEAR TERRORISM POSE NEW RISKS

The committee does not foresee an imminent nuclear terrorist attack with a nuclear weapon or an IND Nevertheless, the number and types of groups who may be motivated to use INDs, RDDs, or REDs is likely growing (Earnhardt, Hyatt, and Roth 2021). While some nonstate actors may be deterred by the near-certainty of attribution and retribution, others including millenarian groups such as ISIS and U.S.-based accelerationist groups, actively court retaliation to spark a wider war or to realize apocalyptic beliefs.

Nuclear weapons, weapons usable fissile materials, and nuclear weapons design expertise are almost entirely controlled by state actors. This means that in order for a terrorist organization to carry out a nuclear attack with either a nuclear weapon or an improvised nuclear device, they would need the complicity of a state, the failure of the state’s controls, or the failure of the state itself. As the national security and intelligence communities shift focus from terrorism to great power competition, there is danger that there will be less capability and capacity for early detection and for mobilizing a timely counter-terrorism response to a non-state actor that obtains a nuclear weapon or weapons usable fissile materials.

Importantly terrorism is not exclusively an international threat or domestic threat but increasingly is a transnational one (Hoffman and Ware 2023). A particularly troubling development is the existence of U.S.-based accelerationist groups who have been deliberately recruiting U.S. military personnel. Additionally, there are disturbing and growing U.S. domestic links with mercenary and terrorist groups across international borders.

Another worrisome development with respect to terrorism is the extent to which technical information can be obtained online and this could encourage groups to seek nuclear material. . Additionally, extremists are utilizing social media to fuel radicalization and extreme partisanship, as well as to propagate dis- and misinformation, and sow mistrust of government institutions and authoritative information. Social media is serving as a powerful organizational tool for terrorist groups, facilitating an increase in international connectivity among domestic and foreign terrorist organizations.

The risk of nuclear terrorism must also be evaluated in the context of changing norms associated with nuclear weapons and civil nuclear power. There have been cyberattacks on operating nuclear power plants in India, Japan, and South Korea. Russia has demonstrated a willingness to defy international norms, not only by attacking and occupying Ukraine’s operating civilian nuclear power plants, but also by employing proxies with a history of war crimes, deploying operatives to attack and poison individuals with advanced nerve agents and radiological substances, and threatening to use nuclear weapons.

In sum, managing the threat of nuclear and radiological terrorism will be challenged by the continued prevalence of groups operating both domestically and overseas who are motivated to carry out these kinds of attacks. State actors could potentially collaborate with terrorist groups providing them the capability to conduct such attacks. As this threat landscape continues to evolve, the pressure of other national security challenges associated with great power competition along with resource constraints will make it difficult for the national defense and intelligence communities to sustain current levels of effort for managing the nuclear terrorism risk.

#### Plan solves. Contributory liability plus safe harbor requirements force platforms to crack down on trade-based money laundering and close loopholes in the anti-money laundering regime

Ron Teicher, 2021 - founder and Chief Executive Officer of EverCompliant, a financial services company dedicated to fighting transaction laundering. “More than Online Product Safety, the SHOP SAFE Act Highlights the Risk of Counterfeit Transactions” 3/25, <https://www.linkedin.com/pulse/more-than-online-product-safety-shop-safe-act-risk-ron-teicher?trk=read_related_article-card_title> //DH

The SHOP SAFE Act “incentivizes e-commerce platforms to adopt best practices designed to limit the sale of counterfeit products that pose a risk to consumer health and safety,” according to the House Committee’s press release.

Projected to reach an aggregate value of $1.9 trillion by 2022 – excluding digital piracy proceeds – according to a 2016 report authored by European financial consultants Frontier Economics, the global counterfeit market has increasingly migrated online, right alongside the modern consumer.

In the U.S., e-commerce sales are projected to reach $794.5 billion this year on the heels of the COVID-19 pandemic, according to marketing research firm eMarkerter. Year-over-year, that represents a 32.4% increase from 2019, almost double the 18% that e-Marketer originally forecasted before the pandemic. Knockoff products have stealthily followed the broader trend.

To address the problem, the House Judiciary bill mandates liability for trademark infringement for hosting third-party sellers, unless compromised e-commerce platforms take 10 prescribed steps to prevent the sale of counterfeit goods on their virtual storefronts.

Additionally, the bill encourages platforms to “establish best practices such as vetting sellers to ensure their legitimacy, removing counterfeit listings, and removing sellers who repeatedly sell counterfeits,” according to the press release.

The bill also creates a legal impetus for online markets to take essential steps to “prevent the continued sale of counterfeits by the third-party seller.” Beyond obvious risks to consumer safety, with a particular focus on fake medical goods that have disrupted hospital procurement during COVID, online knockoffs also threaten the integrity of the global banking system.

For financial institutions (FIs) that provide banking services to online platforms, the SHOP SAFE Act has thus heightened anti-money-laundering (AML) and counter-terrorism-financing (CTF) risks. In effect, this bill has cast a light on the digital ‘last hop’ of the trade-based-money-laundering (TBML) cycle, where criminals cash-out online. And not all knockoff consumers are unwitting.

But prior to clarifying how these cyber-enabled, illicit-financing mechanisms work, it’s important to highlight the geopolitical undercurrents and problem regions that have allowed the counterfeiting threat to proliferate.

Genesis of the Bill

This legislation came on the heels of outgoing President Donald Trump’s Executive Order titled “Ensuring Safe & Lawful E-Commerce for US Consumers, Businesses, Government Supply Chains, and Intellectual Property Rights”.

A Department of Homeland Security report published last January to accompany the online counterfeiting EO addresses this growing pattern. “E-commerce has contributed to a shift in the sale of counterfeit goods in the United States, with consumers increasingly purchasing goods online and counterfeiters producing a wider variety of goods that may be sold on websites alongside authentic products,” says the DHS report.

As such, the DHS report says that the growing presence of knockoffs online presents a threat on a multitude of different levels. “Illicit goods trafficked to American consumers by ecommerce platforms and online third-party marketplaces threaten public health and safety, as well as national security,” says the DHS report.

The report also notes that the counterfeit threat “impacts American innovation and erodes the competitiveness of U.S. manufacturers and workers.” Circling back to the theme of illicit finance, however, knockoffs inherently increase FIs’ exposure to rapidly proliferating and largely hidden transaction-laundering (TL) risks.

Counterfeit Transactions and the AML Angle

Electronic Money Laundering, known as Transaction Laundering, is the digital evolution of money laundering and has become one of the biggest challenges facing the Anti-Money Laundering (AML) regime today. Transaction Laundering occurs when an undisclosed business uses an approved merchant’s payment credentials to process payments for another undisclosed store selling unknown products and services.

Beyond defrauding and potentially harming consumers by selling fake or harmful goods, online sellers who willfully deal in counterfeit products may also be engaged in laundering funds by falsifying the nature of goods being sold.

From an AML standpoint, consider an attack vector where a local drug distribution ring uses proceeds from narcotics sales to purchase Chinese counterfeit goods at below-market value and then sell the knockoff merchandise online at a huge mark-up as if they were legitimate. Without heightened due diligence, tax investigators would just mark reported income as the proceeds from e-commerce.

In traditional brick-and-mortar storefronts, this trade-based typology has already proven to be a popular narco-laundering mechanism in Colombia. Highlighting this scheme is the 2016 extradition of Colombian national Jhon Jairo Hincapie-Ramirez to the U.S.

Hincapie-Ramirez allegedly played a significant role in an international money-laundering conspiracy known as the Guangzhou Enterprise. The suspect and his co-conspirators were accused by the Department of Justice of shipping counterfeit goods of Chinese origin “around the world to launder over $5 billion” for Mexican and Colombian cartels, according to the 2015 indictment.

Preferred Method of Terrorism Financing

More frightening is the sale of counterfeit products online to finance terror attacks. The “infringement of intellectual property is becoming the favorite method of financing for terrorists,” said Interpol’s then-Secretary General Ronald K. Noble in 2003.

More recently, counterfeiting was the primary funding stream for the tragic 2015 jihadist attack on satirical French publication Charlie Hebdo. Proceeds from knockoff sales on e-commerce sites helped the French-Algerian Kouachi brothers procure the weapons used to murder 12 people and injure 11 others at the media outlet’s headquarters.

Also, in 2017, the Federal Bureau of Investigation reported that the Sunni terrorist group ISIS was executing fake transactions on the e-commerce platform eBay to funnel money to a U.S.-based operative.

Given the risk, and the increasing ease through which threat actors can conceal their illicit activity through proliferating e-commerce flows, the SHOP SAFE Act is essential to safeguard 21st Century financial integrity and national security.

The bill is a sorely needed enforcement tool to hold platforms like Amazon, which accounts for 50 percent of all U.S. retail e-commerce volume – and half of which is generated by third-party sellers – accountable for ghost-laundering risks.

As trade-based laundering becomes increasingly cyber-enabled via the last hop of e-commerce transaction chains, threat actors will continue to exploit regulatory loopholes until stronger laws are enacted and enforced. The SHOP SAFE Act is still under review by the House Judiciary Committee.

#### Liability and due diligence requirements that establish safe harbors create global standards for enforcement

Cindy Braddon, 2024 – Head of Communications and Public Policy at the Transnational Alliance to Combat Illicit Trade “Legislation and cross agency, cross border, public/private sector cooperation and enforcement is critical to stopping trade in counterfeits” 1/8, <https://www.tracit.org/tracit-talking-points> //DH

The surge in online shopping brought on by the pandemic has stayed with us. Now we can buy anything, anywhere and it will arrive almost immediately, which is perfect for a society that more and more demands instant gratification. As with every good thing, however, criminals figure out ways to profit by exploiting weaknesses on online platforms and the consumers that shop there. Selling and profiting on counterfeits in an online environment – where there is lax oversight and a focus on facilitating sales without the same due diligence requirements in place for brick-and-mortar stores – has become a significant consumer protection problem that must be addressed immediately.

The Transnational Alliance to Combat Illicit Trade (TRACIT), a US-based independent multinational business association, is focused on stopping counterfeit and illicit goods across ten industries by addressing all forms in which they are traded.

Our experience is that brand owners are committed to protecting their intellectual property and their brands and invest significant time and resources into working with ecommerce and social media platform, employing technologies and bringing legal enforcement actions aimed at eliminating counterfeits that potentially harm with products that do not meet regulatory and safety standards.

Fortunately, Congress passed the INFORM Consumers Act last year. This is a crucial, albeit small step along the path to ensure that consumers have a safe and secure online shopping experience. For the first time, online marketplaces will have to conduct some basic due diligence to better vet their third-party sellers and disclose key information about the sellers to consumers. Also, importantly, platforms must have an easy-to-use portal on each product listing for consumers to report suspicious activity. The Federal Trade Commission is enforcing the law and stiff fines are available for violations.

We need to go further to incentivize online marketplaces by creating liability if they do not implement certain best practices.

When a platform involved with the transaction guides, encourages, and controls every step of the interaction between buyer and a merchant; when it actively promotes, controls, consummates, and guarantees the transaction, that platform is far more than an internet venue that connects purchasers and merchants. It is now facilitating the sale of counterfeits and must take responsibility for its role. For the reason, the liability provisions of the SHOP SAFE Act of 2023 are the essential next step in responsible public policy to protect consumers.

Currently ecommerce and social media platforms are telling us they are regularly removing thousands and thousands of fraudulent products listings. Now is the time for standardized and enforceable best practices across online marketplaces to insure they stop the bad actors from ever listing their counterfeit products in their stores from the get-go, and bar counterfeiters from accessing their platforms after repeatedly violating their terms.

The SHOP SAFE Act of 2023 does just that. The bill makes online marketplaces more accountable for implementing key best practices. It provides a safe harbor from liability if platforms proactively screen against fakes and counterfeits; promptly remove counterfeit listings; enforce their policies; communicate with brands and law enforcement; and ban counterfeiters from hopping back on their platforms. Voluntary and inconsistent practices are not working. Let’s take the next step to better protect our consumers, our economic and national security. Let’s work together to bar repeat offenders from ever being able to sell in their marketplaces again. Let’s pass SHOP SAFE in the US and make it a global standard.

# Case extensions

## Counterfeiting Advantage

### They Say: “Counterfeiting Exaggerated”

#### Counterfeiting through e-commerce is expanding rapidly – data from Homeland Security support this

Daniel Shapiro, 2024 - Senior Vice President, Brand Relationships and Strategic Partnerships, Red Points. Testimony before the U.S.- China Economic and Security Review Commission. Hearing on Consumer Products from China: Safety, Regulations, and Supply Chains. 2/29, <https://www.uscc.gov/sites/default/files/2024-03/Daniel_Shapiro_Testimony.pdf> //DH

Quantifying the issue of counterfeit goods in the U.S.

As mentioned above, the issue of counterfeiting has undergone a rapid evolution beyond the traditional confines of street corners and flea markets.

As of 2018, counterfeiting ranked as the largest criminal enterprise globally, with sales of counterfeit and pirated goods totaling an estimated $1.7 trillion to $4.5 trillion annually, surpassing the revenue from both drugs and human trafficking7.

This significant increase is mirrored in data collected by the U.S. Department of Homeland Security (DHS). Between 2000 and 2018, DHS reported a tenfold increase in the seizure of infringing goods at U.S. borders, with annual seizures growing from 3,244 to 33,8108. Even more telling is the domestic value of these seized items based on the manufacturer's suggested retail price (MSRP) of the legitimate goods, which reached the staggering amount of $1.4 billion in 20189.

The expected growth of e-commerce amplifies concerns that the extent of this problem could escalate further, particularly if current practices continue without significant changes.

#### Online counterfeiting is a unique vector – retail counterfeiting is less of a threat

Austin Church, 2023 – J.D. Candidate, Boston University School of Law “INCORPORATING A DEPOSIT MECHANISM INTO THE DIGITAL MILLENNIUM COPYRIGHT ACT TO FIGHT ONLINE COUNTERFEITING IN E-COMMERCE” BOSTON UNIVERSITY LAW REVIEW [Vol.103:935, Hein Online. Accessed via University of Michigan //DH

The unique circumstances surrounding counterfeits on Online Marketplaces make online counterfeiting more likely.73 The Department of Homeland Security identified four factors that increase the likelihood of counterfeiters going online: (1) “Lower Startup and Production Costs,” (2) “Lower Marketing Costs,” (3) “Lower Distribution Costs,” and (4) “Consumer Attitudes and Perceptions.”74 Online counterfeiters have lower startup costs because online storefronts are much easier and cheaper to create than traditional brick and mortar stores, especially given the Online Marketplaces’ incentives to increase the accessibility to new sellers.75 Lower startup costs also make it harder to eliminate counterfeiters because of the ease of creating alternative stores or accounts.76 Online counterfeiters reap much of the benefit of lower production costs—increasing profit margins and the ability to undercut legitimate options— that most counterfeiters achieve.77

Online counterfeiters are also able to leverage lower marketing costs through stealing online promotional materials and by using the algorithms of Online Marketplaces and social media to funnel traffic to their fraudulent goods.78 The anonymity given to online sellers also makes it easier for them to use the same stolen promotional materials in other accounts, further driving down marketing costs.79 This ability to use cheap promotional materials across accounts also makes it easier for online counterfeiters to run multiple counterfeiting accounts simultaneously.80

Online counterfeiters are also able to leverage the user-to-user sales format of Online Marketplaces to better facilitate sales of counterfeit goods.81 Unlike with traditional counterfeiting, where goods (especially foreign ones) are shipped en masse to distribution centers, many online sales are sent by mail to the user directly.82 Large shipments typically get more inspection compared to air parcels.83 In light of these realities, online counterfeiters are increasingly shifting to distributing counterfeit items through air parcel delivery to great success.84

Consumer respect and trust for many Online Marketplaces also assist online counterfeiters.85 Online Marketplaces typically lack the red flags that consumers often associate with counterfeit goods, leading to an implicit trust in the legitimacy of the listings they encounter on Online Marketplaces.86 Some red flags for the presence of counterfeit goods are “suspicious location of the seller, poor quality packaging, or discount pricing.”87 The first two of those examples do not apply to online sales at all and the discount pricing can be shifted from a red flag to an inducement of counterfeit sales. This can happen because consumers who trust the platform may see discounted prices as a way to save or as a benefit of shopping online, not as an indication that the goods are counterfeit. Online counterfeiters are also able to effectively disguise their listings to look legitimate, leading to third-party sales on Online Marketplaces comprising 39% of all unwitting purchases of counterfeited goods.88

### 1AR: They Say: “INFORM Act Solves”

#### INFORM fails – it’s easily circumvented

Austin Church, 2023 – J.D. Candidate, Boston University School of Law “INCORPORATING A DEPOSIT MECHANISM INTO THE DIGITAL MILLENNIUM COPYRIGHT ACT TO FIGHT ONLINE COUNTERFEITING IN E-COMMERCE” BOSTON UNIVERSITY LAW REVIEW [Vol.103:935, Hein Online. Accessed via University of Michigan //DH

The INFORM Consumers Act is similar to the SANTA Act, but it broadens the scope of protection from toy sellers to all high-volume sellers.150 One issue with this law is that online counterfeiters can evade its reach by creating multiple low-volume accounts, therefore never triggering the enhanced scrutiny reserved for high-volume retailers. The INFORM Consumers Act requires some verification documents and use of such documents may reduce this problem.151 However, the reliance on verification documents is troubling because the INFORM Consumers Act does not provide much detail on whether Online Marketplaces have an obligation to ensure the documents are authentic.152 A further weakness of the INFORM Consumers Act is that it suspends sellers who do not comply with the Act until they comply; this allows noncompliant sellers to simply create new accounts and continue their activities.153

### They Say: “Status quo Solves”

#### There is overwhelming noncompliance – most policies are window dresing

Dr. David Shepherd, et al, 2023 – Senior Lecturer, School of Criminology and Criminal Justice, University of Portsmouth, United Kingdom. “PRACTICES USED BY ONLINE MARKETPLACES TO TACKLE THE TRADE IN COUNTERFEITS” World Intellectual Property Organization Advisory Committee on Enforcement, 11/24,

<https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_16/wipo_ace_16_11.pdf> //DH

The study finds that just eight of the 50 sampled marketplaces have coherent anti-counterfeiting strategies in place and all eight passed the compliance test. Four of these marketplaces are generalists, which sell a wide range of products, and their anti-counterfeiting strategies are based on a wide range of administrative controls. The other four are specialists and their control strategies are based on inspecting and verifying the authenticity of products.

The other 42 marketplaces do not have coherent strategies in place and 60 per cent failed the compliance test. Some are indifferent to the counterfeit problem. Others are simply engaged in window-dressing, that is their actions fall short of the values and intentions proclaimed in their policies. The social media sector is notably deficient in delivering on its own policies. The investment in anti-counterfeiting strategies falls well short of that required to serve the sector’s business model.

#### The majority of enforcement is reactive, and even the supposedly proactive ones don’t implement it well enough

Dr. David Shepherd, et al, 2023 – Senior Lecturer, School of Criminology and Criminal Justice, University of Portsmouth, United Kingdom. “PRACTICES USED BY ONLINE MARKETPLACES TO TACKLE THE TRADE IN COUNTERFEITS” World Intellectual Property Organization Advisory Committee on Enforcement, 11/24,

<https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_16/wipo_ace_16_11.pdf> //DH

57. Surprisingly few platforms claim to monitor their platforms (34 per cent), which triangulates with the views of brand participants that the controls of most platforms are reactive in responding to reports of counterfeits rather than proactive in their surveillance. The absence of proactive monitoring on some platforms may be due to naivety. Participant K had observed an acute lack of awareness in one classified ads business which emerged as a genuine shock when it was confronted with the scale of counterfeits on its platform. Most of those who do monitor their platforms also publish transparency reports (22 per cent). These provide statistics about the number of reports by rights holders, requests for information and interventions in the reporting period.

58. A small number (18 per cent) claim they use machine learning or artificial intelligence for monitoring purposes. However, according to Participant H, the sheer scale of the number of sellers and transactions means that even the AI systems on his platform are currently restricted to sampling rather than 100 per cent continuous monitoring. Furthermore, his platform is finding that traditional word and image searches are becoming less effective because counterfeiters are learning how to disguise their fake products. Consequently, Participant H is increasingly using AI to monitor trends in sellers’ behaviors. The system flags changes in volumes, values and product types for further investigation.

### They Say: “Cyber Attacks Won’t Escalate”

#### Even with limited damage, cyber attacks increase public pressure for escalation

Ryan Shandler et al, 2023 - Assistant Professor of Political Science at the Georgia Tech School of Cybersecurity & Privacy. Prior to joining SCP he was a postdoctoral fellow at the University of Oxford with Nuffield College“Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis” Journal of Global Security Studies, Volume 8, Issue 1, March 2023, <https://academic.oup.com/jogss/article/8/1/ogac042/6988925> //DH

In this paper, we suggest that the foremost threat of cyberattacks is not necessarily their first-order consequences—such as the degradation of physical systems, data theft, or loss of access. While these outcomes remain a cause for concern, the fixation on direct effects obscures the more insidious consequences of long-term psychological harm and societal damage. This perspective acknowledges the human dimension of cyberattacks that target individual well-being, morale, and vulnerability. For many cyber perpetrators, ranging from terrorists to state-sponsored hackers and criminal organizations, the primary objective of attacks is to evoke anxiety and terror, and disseminate misinformation among the public. In other words, these are nonphysical aims whose efficacy cannot be simply measured by weighing rubble, counting bodies, or tallying lost funds. Viewing a ransomware attack on a hospital network as minor or unsuccessful, simply because it caused minimal physical destruction and failed to attain a ransom, ignores the extensive psychological and societal damage it can leave in its wake (Shandler and Gomez 2022). Through this lens, the severity of cyber-threats can and should also be measured by the level of psychological distress. We remove from the definition of distress transient or minor emotional responses such as unease or discomfort, and focus our attention on acute psychological distress, including visceral anxiety, enduring anger, and heightened threat perception (Canetti 2017; Byrne et al. 2022).

Currently, there is no consensus whether cyberattacks cause sufficient individual-level harm to constitute a grave threat. Some argue that the bulk of cyberattacks constitute only minor irritants (Lindsay 2013; Gartzke and Lindsay 2015), while other researchers insist that even low-level cyberattacks can levy severe psychological and political consequences (Gross, Canetti, and Vashdi 2016; Canetti et al. 2017). Addressing this dilemma, this paper employs an internal meta-analysis that reviews a series of experimental studies simulating exposure to cyberattacks. An internal meta-analysis is a powerful analytical tool that aggregates and analyzes a pooled collection of experiments conducted by a single researcher or group of researchers. This technique allows us to exploit heightened statistical power to provide precise statistical estimates of treatment effects, and incorporate studies conducted with different population groups at different points of time. We analyze the full gamut of studies conducted by the authors—including null and unpublished findings—to provide accurate, transparent, and conclusive evidence about the individual-level consequences of exposure to cyberattacks. In all, we aggregate and meta-analyze findings from eighteen experimental studies conducted between 2015 and 2021. Over the course of these studies, we exposed 6,020 unique respondents in three countries to simulated cyberattacks and conventional attacks, before measuring the psychological distress that ensued. All studies mimicked how people are exposed to real-world cyberattacks, while maintaining strict ethical standards to ensure participants’ well-being.

Our aggregate findings confirm that cyberattacks cause equally high levels of psychological distress as conventional terrorism and political violence. This finding challenges international and domestic security norms and practices in several ways. First, psychological suffering elicited by cyberattacks might now be sufficient to constitute an armed attack as defined by international law. If this were the case, cyberattacks could trigger the right of armed self-defense in response to attacks that until now have been perceived as limited strikes. At the same time, the newly perceptible psychological harms of cyber-conflict may weigh on calculations of proportionality and so constrain cyber operations. Second, we consider how the extreme psychological distress experienced by the public creates a groundswell of support for military retaliation, thus generating a political tailwind in support of escalation. In this way, we unveil an indirect route by which cyber operations influence foreign policy decision-making.

#### The risk is high – actors are targeting hardware vulnerabilities to cause catastrophic damage

Nazak Nikakhtar, 2024 - Former Assistant Secretary for Industry & Analysis, Under Secretary for Industry & Security U.S. Department of Commerce. Partner, International Trade, National Security Practice Chair, Wiley Rein LLP. Statement to the US-China Economic and Security Review Commission, “Current and Emerging Technologies in U.S.-China Economic and National Security Competition” 2/1, <https://www.uscc.gov/sites/default/files/2024-02/February_1_2024_Hearing_Transcript.pdf> //DH

For several years, Members of Congress, executive agencies, and third-party organizations have been sounding the alarm on the potential risks caused by Chinese components and hardware embedded into U.S. energy grid. In testimony before the Senate Energy and Natural Resources Committee, Director of CESAR (the Department of Energy’s (“DOE”) Office of Cybersecurity, Energy Security, and Emergency Response) Puesh Kumar, pointed to reports from the Director of National Intelligence (“DNI”) and emphasized that cyber actors are targeting U.S. energy infrastructure, and they are posing serious threats to national security.73 Further, the 2023 Annual Threat assessment from DNI identified China as representing “the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks [and that] China’s cyber pursuits and its industry’s export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland.”74

Today, outsider actors are capable of exploiting hardware vulnerabilities in U.S. systems to destroy physical components of the U.S. electric grid.75 The attacks could originate from hardware within the grid itself, or the transmission of malicious code to the grid from external hardware devices, such as electric vehicles (“EV”) charging stations, large data and power storage devices, or telecommunication equipment scattered nationwide. Large attacks on the U.S. electric grid, should they occur, will have devastating impact on the United States population – leaving masses without access to electricity and heat and will cause critical service systems such as hospitals, emergency services, utility providers (water/sewer, gas), and military installations incapable of performing essential tasks.76 Attacks on military utility installations have been a particular area of concern as hostile nations could utilize preemptive blackouts to limit U.S. defensive and responsive capabilities.

Moreover, power plants and petrochemical refineries and facilities may similarly be rendered inoperable due to cyber intrusions.77 And nuclear generation facilities, in particular, pose a risk for catastrophic destruction should outside interference induce a radiological release.78 These are merely a few examples of the range of risks that exist today. These risks become all the more dangerous when coordinated cyberattacks simultaneously cripple multiple power sources across broad geographic regions.

### They Say: “Power Grids Are Resilient”

#### IoT and smart grid adoption is increasing grid vulnerabilities

Roya Gordon, 2024 – cybersecurity professional who serves as an executive industry consultant for Operational Technology (OT) cybersecurity at Hexagon’s Asset Lifecycle Intelligence division“The Internet of Things and Increasing Threats to the Electric Grid” Security Technology, February 2024, <https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2024/february/Internet-of-Things-Increasing-Threats-Electric-Grid/> //DH

**IoT = Internet of Things**

As IoT devices become more integrated into the power grid, the risk of cyberattacks increases. A coordinated attack could manipulate energy flows, cause cascading failures, disrupt power to critical infrastructure, and damage the grid infrastructure. This highlights the need for increased security measures to ensure the safety and stability of the power grid.

One major vulnerability is weak authentication and encryption. Insufficient authentication mechanisms and encryption protocols can leave IoT devices and communication channels vulnerable to unauthorized access. According to an article from CSO online, more than “90 percent of data transactions on IoT devices are unencrypted.”

Let’s look at the lack of security standardization in smart meters as an example. Although the Advanced Metering Infrastructure (AMI) has brought significant benefits, such as energy consumption and billing transparency between utilities and customers, it has also introduced new cybersecurity risks. Security researchers recently discovered a vulnerability in Schneider smart meters that transmits clear text credentials that, if intercepted, could allow an attacker to use the credentials to access smart meters, modify data, or launch a DDOS attack.

IoT devices within a smart grid can also be susceptible to ransomware and malware infections. While there isn’t evidence of smart grid-specific IoT malware yet, threat actors have proven sophisticated enough to develop OT/ICS specific malware like BlackEnergy and Industroyer2, which were responsible for the attack on Ukraine’s power grid in 2015 and 2016. WIRED also reported that in 2019, the hackers behind the 2017 Triton malware probed at least 20 U.S. electric power companies.

As cities continue to take on the “smart grid” concept, threat actors will only continue to find new ways of exploiting vulnerabilities and launching cyberattacks via vulnerable devices used in the power grid.

#### Resilience isn’t possible when attacks cause physical damage to the grid

Joe Weiss, 2020 – Managing Partner at Applied Control Solutions, LLC and Emeritus Managing Director ISA99 ICS Cyber Security “A critical look at the CSIS Report “Dismissing Cyber Catastrophe”” 8/31, <https://www.controlglobal.com/home/blog/11295544/information-technology> //DH

Claim: They are harder to damage through cyberattack than they look, given the growing (albeit incomplete) attention to cybersecurity; and experience shows that people compensate for damage and quickly repair or rebuild.

My response: This is true when there is no equipment damage such as occurred with the 2003 Northeast Outage. However, this is not true when long-lead equipment such as transformers, generators, or large motors are damaged or destroyed. I also question whether there actually is growing concern about control system (not OT network) cyber security as can been from the responses to the DOE Request for Information with respect to the Presidential Executive Order 13920.

### They Say: “Cooperation Turn”

#### Brands’ self-interest maintains cooperation after liability

Stephen Lamar, 2023 - American Apparel & Footwear Association President and CEO. “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” 10/3, Proquest Congressional, accessed via University of Michigan //DH

STEPHEN LAMAR: I think if -- if SHOP SAFE were to become law, I think you would still have very, very robust brand platform collaboration and cooperation. That's been going on for a number of years. That will continue to go on regardless of the shifting of the liabilities. Because it's in the brand's own interest to continue to make sure that their platform partners are educated.

At the same time, the platforms need to avail themselves of the public information that's out there. For example, trademarks are filed with the Patent and Trademark Office, which is what the legislation talks about. So, you know, relying on a US government body that is the central repository of trademarks in the United States, I don't think it's a difficult ask.

#### Platforms won’t cooperate if they’re shielded from liability

Austin Church, 2023 – J.D. Candidate, Boston University School of Law “INCORPORATING A DEPOSIT MECHANISM INTO THE DIGITAL MILLENNIUM COPYRIGHT ACT TO FIGHT ONLINE COUNTERFEITING IN E-COMMERCE” BOSTON UNIVERSITY LAW REVIEW [Vol.103:935, Hein Online. Accessed via University of Michigan //DH

Courts recently grappled with the issue of contributory trademark liability for e-retailers in Tiffany (NJ) Inc. v. eBay Inc.41 In Tiffany, luxury jewelry brand Tiffany sued eBay for not doing enough to keep fake Tiffany goods from being sold on its platform (Tiffany did not list any of its goods on eBay’s platform).42 eBay did establish anticounterfeiting measures, including an antifraud program and its Verified Rights Owner Program, to allow potentially infringing items to be removed by eBay.43 Despite the measures taken by eBay, Tiffany alleged contributory trademark infringement because eBay was unable to catch all instances of counterfeit Tiffany articles and argued that eBay’s general knowledge of counterfeit Tiffany goods on its site was sufficient to attach liability to eBay.44

Ultimately, the Second Circuit rejected Tiffany’s general knowledge argument and found that contributory trademark infringement requires a higher quantum of knowledge.45 In other words, a platform’s general knowledge that third parties are selling counterfeit goods is not enough to attach liability; the platform must have knowledge of specific infringing listings or listings that will infringe in the future.46 The court in Tiffany looked at the actions eBay took to reduce infringement and the takedown of known infringing articles as the basis for its determination that there was no specific knowledge.47 This knowledge requirement is similar to the standard for contributory copyright liability under the Digital Millennium Copyright Act (“DMCA”).48 Therefore, Tiffany effectively created a safe harbor for e-retail platforms that is similar to the storage safe harbor under the DMCA in the copyright sphere.

Courts have since explored the contours of the Tiffany safe harbor. In BMW of North America, LLC v. Rocco,49 the United States District Court for the Central District of California refused to extend the safe harbor to capture resellers.50 There, plaintiff BMW sued defendant Adam Rocco, an internet reseller who listed and sold counterfeit BMW parts.51 The court did not extend the Tiffany safe harbor to Rocco because, unlike eBay in Tiffany, Rocco was able to inspect the counterfeit goods before selling them and was therefore not a venue merely facilitating the sale of goods.52 A key aspect of this analysis is that courts should give an e-retail platform extensive leeway only when its knowledge base is limited and gathering information would be unduly burdensome.53 However, this framework incentivizes e-retailers to know less in order to make falling into the safe harbor more likely. That, coupled with the financial incentives of having counterfeit goods on their platforms (revenue from sales of counterfeit goods), creates a perverse incentive for e-retailers to take the minimum steps to fall within the generous safe harbor while still allowing counterfeits to exist out of sight and out of mind.54 Other courts have also continued to fine tune the requirements initially set forth in Tiffany.55 Currently, the Tiffany safe harbor protects many e-retailers, and—perhaps as a result— many sellers list and sell counterfeit goods online.56

### 1AR: Cooperation Low Now

#### Anti-counterfeiting cooperation is low now

Helena Rother, 2023 - senior associate, Communications and Research, at the International Trademark Association “Evaluating corporate anti-counterfeiting efforts after the pandemic” World Trademark Review, 9/29,

<https://www.worldtrademarkreview.com/guide/anti-counterfeiting-and-online-brand-enforcement/2023/article/evaluating-corporate-anti-counterfeiting-efforts-after-the-pandemic> //DH

The data suggests that in-house legal teams work closely with law enforcement and government/legislative bodies. However, collaboration with brand owners in their same industry, brand owners in other industries, logistics/freight organisations, and payment and search engines is lacking. Just over half of all respondents said their organisation collaborates with other brand owners in anti-counterfeiting matters either frequently or very frequently, while a further two-fifths collaborate less often. In addition, more than one third of respondents reported no collaboration with brand owners in other industries.

A similar proportion said they do not collaborate with logistics/freight organisations and payment providers. Moreover, information about whether and to what extent in-house legal teams are collaborating with other stakeholders to fight counterfeiting remains low. Survey respondents expressed a high degree of uncertainty about whether they collaborated with various stakeholders. Reasons given for not collaborating include a lack of access to people in charge of anti-counterfeiting activities and lack of awareness about opportunities for collaboration.

## Money Laundering Advantage

### They Say: “Anti Money Laundering Fails”

#### Improving AML enforcement empirically improves institutional quality in developing countries

Folorunsho M. Ajide and Titus Ayobami Ojeyinka, 2023 – “Benefit or burden? An exploratory analysis of the impact of anti-money laundering regulations on sustainable development in developing economies” Sustainable Development, 10/17, Wiley Online Library, Accessed via University of Michigan //DH

**ML = Money Laundering, AML = Anti Money Laundering, SDI = Sustainable Development Indicator**

Table 4 presents the results of the Driscoll-Kraay, Prais-Winsten estimate difference GMM (D-GMM) and IV-GMM estimators. The coefficients show that AML regulations promote sustainable development in developing countries. A 1% increase in AML improves SDI by 12%. The D-GMM results also show there is a 5% increase in SDI for one unit improvement in anti-money laundering regulations. These results are consistent with the related studies that show that AML regulation promotes economic growth and encourages inflow of foreign investors because it increases investors' confidence in an economy (Ofoeda, Agbloyor, & Abor, 2022a; Ofoeda, Agbloyor, & Abor, 2022b; Ofoeda, Agbloyor, & Abor, 2022d; Ofoeda, Agbloyor, Abor, & Achampong, 2022). Anti-money laundering activities ensure quality of life and improve overall wellbeing. The impact of AML regulations is very crucial in restating confidence and trust in the financial market system and sustaining the economy in general. Studies prove beyond doubt that better regulations should grow the economic system for sustainability (Djankov et al., 2006). An effective AML regulation is expected to improve economic, social and environmental sustainability in developing countries. The results of this study also support the view of Porta et al. (1998), who state that legal systems and effective regulations would discourage asymmetric information and motivate transparent transactions, thereby fostering customer confidence and trust for sustainable growth and development.

The coefficients of institutional quality (IQ) and income per capita (LGDPPC) are positive and significant in relation to sustainable development. The results suggest that a 1% increase in quality of institution promotes sustainable development by 3.1%. Likewise, a percentage change in income increases sustainable development by 5.6% in developing nations. Human capital (SCH) has a positive impact on sustainable development at 1% significance level. This is in line with the submission of Koirala and Pradhan (2019). Furthermore, Ajide et al. (2023) and Osinubi et al. (2023) confirm that income per capita and human capita proxied by year of schooling improve the achievement of sustainable development in Africa and Middle East nations. Education provides the capacity for individuals to become economically useful as it equips individuals with necessary skills for economic empowerment, thereby increasing the possibility of achieving economic and social sustainability (Obanya, 2009). Institutional quality reduces environmental degradations and it is the ‘rule of the game’ for social interactions which promote justice and equity among economic agents (Torras & Boyce, 1998). The study of Ali et al. (2019) further suggests that quality of institution is very important for sustainable growth and development, while the findings of Akhbari and Nejati (2019) are conflicting. Furthermore, Osabuohien et al. (2014) find that the quality of institutions has a potential for environmental sustainability. The coefficients of FDI and trade openness have negative impacts on sustainable development. This supports the previous findings on the pollution haven analysis. FDI produces negative environmental externalities due to the lax regulations in developing nations (Abid et al., 2015; Carullo et al., 2013).

#### AML regulations build institutional quality and lower corruption

Folorunsho M. Ajide and Titus Ayobami Ojeyinka, 2023 – “Benefit or burden? An exploratory analysis of the impact of anti-money laundering regulations on sustainable development in developing economies” Sustainable Development, 10/17, Wiley Online Library, Accessed via University of Michigan //DH

**ML = Money Laundering, AML = Anti Money Laundering, SDI = Sustainable Development Indicator**

From the policy and practical perspective, this study offers some insights for policymakers seeking to improve and implement anti-money laundering regulations in business practices, and for the economy as a whole. The findings of this paper reinforce that AML regulation is favorable towards the achievement of sustainable development in least developed nations. Therefore, to combat and control the level of money laundering, developing nations must set up and enforce AML framework. AML regulation fosters the effectiveness of institutions and financial development towards sustainable development. It also guarantees financial transparency, standards and promotes public accountability. AML regulations strengthen the legal system and reduce the level of corruption common to most developing countries. Second, the study reveals that AML regulation stimulates sustainable development for developing countries. On this note, it becomes appropriate for policymakers to effectively implement the AML regulations and ensure compliance. Financial regulators and authorities should ensure that the AML framework is entrenched in their supervisory roles, and is cost-effective.

### They Say: “Alternate Causality – Shell Companies”

#### Their evidence is mostly about real estate and the United States is cracking down on that now

Luc Cohen and Chris Prentice, 2023 - \*Reports on the New York federal courts and \*\* reports on financial crimes, with a focus on securities enforcement matters. “US set to unveil long-awaited crackdown on real estate money laundering” Reuters, 8/10, <https://www.reuters.com/world/us/us-set-unveil-long-awaited-crackdown-real-estate-money-laundering-2023-08-10/> //DH

The U.S. Treasury Department will soon propose a rule that would effectively end anonymous luxury-home purchases, closing a loophole that the agency says allows corrupt oligarchs, terrorists and other criminals to hide ill-gotten gains.

The long-awaited rule is expected to require that real estate professionals such as title insurers report the identities of the beneficial owners of companies buying real estate in cash to the Treasury's Financial Crimes Enforcement Network (FinCEN).

FinCEN is slated to propose the rule sometime this month, according to its regulatory agenda, though the timeline could slip, said two people briefed on the developments. Anti-corruption advocates and lawmakers have been pushing for the rule, which will replace the current patchwork reporting system.

Criminals have for decades anonymously hidden ill-gotten gains in real estate, Treasury Secretary Janet Yellen said in March, adding that as much as $2.3 billion was laundered through U.S. real estate between 2015 and 2020.

"That's why FinCEN is taking this important step to put something officially on the books that would root out money laundering through the sector once and for all," said Erica Hanichak, government affairs director of advocacy group the FACT Coalition.

#### The global fight against financial secrecy is improving

Joseph Foti et al, 2024 – Chief Research Officer - Open Government Partnership at the Brookings Institution “A better anti-corruption machine: Breakthroughs needed to fight illicit finance and protect democracy” 6/17, <https://www.brookings.edu/articles/a-better-anti-corruption-machine-breakthroughs-needed-to-fight-illicit-finance-and-protect-democracy/> //DH

But the global fight against this financial secrecy has also been growing. A keystone of the battle has been increasing transparency about the people who ultimately own or control companies and other entities, referred to as “beneficial owners.” The last decade has seen notable progress: Over 80 countries now maintain beneficial ownership registers, collecting data that was once obscure and making it more accessible and transparent.

### They Say: “No Nuclear Terrorism”

#### Risks are increasing, both in groups seeking nukes and the ability to access materials

National Academies of Sciences, Engineering, and Medicine. 2024. Nuclear Terrorism: Assessment of U.S. Strategies to Prevent, Counter, and Respond to Weapons of Mass Destruction. June, <https://nap.nationalacademies.org/catalog/27215/nuclear-terrorism-assessment-of-us-strategies-to-prevent-counter-and> //DH

Fifteen years have passed since the WMD Commission’s report was completed, and there has been no known terrorist acquisition of a nuclear weapon, improvised nuclear device or radiological dispersal device. Still, Al Qaeda showed interest in nuclear terrorism to include conducting inert-material implosion testing in Afghanistan, undertaking efforts to steal materials and recruit scientists (Albright 2010; Mowatt-Larssen 2020, 2010). On August 4, 2014, the Doel 4 nuclear power plant in Belgium was shut down automatically as a result of an act of sabotage by an unidentified organization. Notwithstanding the many changes in the international security environment, the risk of nuclear terrorism remains significant.

With the demise of the Soviet Union, the U.S. government instituted very effective cooperative programs with the Russian Federation to dismantle Soviet weapons and weapon infrastructure and improve the security of components and materials of concern. Programs (among them U.S.-FSU science cooperation, the DOE Nuclear Cities Initiative, the U.S. Civilian Research and Development Foundation, and the “Lab to Lab” program) also were established to engage Soviet weapon scientists in non-weapon work, with the intent of reducing the potential their skills might be procured by nefarious entities (National Research Council 1996; Rotblatt 1998). In addition, the United States and Russia completed the “Megatons to Megawatts” program, which eliminated 500 metric tons of HEU by blending it down to low-enriched uranium fuel for civilian nuclear reactors.

Much has changed in the strategic environment since these successful programs were put in place, especially with respect to Russia’s relationship with the United States. Today there are other nuclear-armed states that could experience instability and governance challenges that would potentially result in a loss of control of nuclear weapons, fissile materials, or expertise. Possible examples include economic collapse in Pakistan or the fall of the Kim regime in North Korea. As the breakup of the Soviet Union demonstrated, such events can be sudden and difficult to predict.

Among the disturbing changes to the global security landscape is that terrorist organizations have proliferated, with a growing number of terrorists movements operating globally and transnationally. Political polarization within the United States is also on the rise with “home grown” extremist groups developing new capabilities and working together for shared goals. This will be discussed in more detail in Chapter 3. New technologies, such as remotely piloted and autonomous air, ground, and sea vehicles; digital fire-control systems for small arms; and machine learning algorithms that enable image recognition and empower deep fakes and other forms of misinformation, disinformation, and mal-information (MDM) have provided terrorist groups with new capabilities.

#### Terrorist recruitment of US military personnel increases the likelihood of nuclear acquisition

National Academies of Sciences, Engineering, and Medicine. 2024. Nuclear Terrorism: Assessment of U.S. Strategies to Prevent, Counter, and Respond to Weapons of Mass Destruction. June, <https://nap.nationalacademies.org/catalog/27215/nuclear-terrorism-assessment-of-us-strategies-to-prevent-counter-and> //DH

FINDING 3-4: Examples of new types of millenarian groups - the type of terrorist group most likely to ignore anti-nuclear norms – are emerging. There is also increasing evidence that extreme-right wing accelerationist groups are recruiting U.S. military personnel. If those personnel have insider knowledge about or access to nuclear facilities, materials, or intelligence, they may be in a position to compromise current U.S. nuclear security safeguards.

Millenarianism is the belief that after a major cataclysm, society will be dramatically changed or “cleansed”. For secular millenarians, the kind of fundamental change they are pursuing arises by taking actions that have the potential to generate a political crisis to include sparking revolution. For example, there are contemporary domestic accelerationists who are actively seeking to incite a “second revolutionary war” in the United States. Since religious millenarians often believe that a savior or Messiah appear following a period of tribulation, they seek to participate in bringing on the cataclysmic events that will cleanse the world in preparation for the Messiah. The threat of retaliation would presumably not deter these kinds of millenarian groups from extreme acts of violence to include nuclear or radiological devices, as they believe that cataclysmic events presage positive transformative change in society and in themselves. These are groups that want, not a seat at the table, but to blow up the table (Lemann 2001; National Commission on Terrorism 1998).

Examples of millenarian groups that have sought to acquire nuclear materials or weapons include not only al Qaeda and ISIS, but also the group Atomwaffen. According to an investigation by Propublica, authorities discovered an aspirational plan to blow up a nuclear facility over 40 miles from Miami (Thompson, Winston, and Hanrahan 2018a). The group’s name means “nuclear weapons” in German. Atomwaffen was formally disbanded in 2020 (Gais 2023), but it has evolved into a brand rather than a specific terrorist group (Lewis and Newhouse 2023) (Shadnia et al., 2022). Members of the coalition associated with the Atomwaffen brand in the United States seek to incite a race war and overthrow the federal government.

Particularly troubling is Atomwaffen’s recruitment of military or US government personnel. Notably, the group’s founder and leader, Brandon Russell, was arrested after authorities found homemade fuses, Geiger counters, and explosive and radiological materials in his garage. He had been serving in the 53rd Brigade Special Troops Battalion of Florida’s Army National Guard at the time of his arrest (Goldwasser 2021). He was described by a former roommate as “obsessed with nuclear weapons” (Fleer 2020). After his 2021 release from prison, Russell was indicted, in 2023, for allegedly planning to disable the power grid in Maryland (Weiner, et al., 2023). Josh Beckett, who served in the army from 2011-2015 as a combat engineer, trained Atomwaffen members in firearms and hand-to-hand combat and offered to construct weapons for the group (Thompson, et al., 2018b). Naval aviation machinist mate’s apprentice David Cole Tarkington was found to be a prolific Attomwaffen recruiter (Villarreal 2020).

### They Say: “Safe Harbors Fail”

#### It's not hard to qualify for a safe harbor – they just have to proactively enforce. Platforms have the ability to do this now – they just choose not to

Arielle Percival, 2021 - J.D., University of the Pacific, McGeorge School of Law, “Social Networks, Counterfeit, and Contributory Trademark Infringement: Are Social Media Giants Still Protected Ten Years after Tiffany?”, 52 U. PAC. L. REV. 877 (2021). Hein Online, accessed via University of Michigan //DH

**OSP = Online Service Provider**

Ten years post-Tiffany, technology has significantly progressed. 222 Data analysis and user-experience driven algorithms are the central pillars of companies within a particular category of OSPs-social media platforms. 223 A technology company can leverage its data to eliminate spam accounts and eradicate manufactured news stories proactively; yet the belief remains that an OSP does not have "knowledge" until it receives reports of infringing material.22

OSPs have successfully argued they do not have "actual knowledge" without notice of specific infringing content despite having the necessary data.225 Despite this position, OSPs can filter and eliminate spam and hate comments without notification from users. 226 Some OSPs use facial recognition to flag and suggest photos in which the user may appear to that individual user. 227 The average consumer often does not know the power of data. 228 But, as the power of data demystifies, a gap in the Tiffany standard for holding OSPs liable for contributory trademark infringement presents itself.229

Externally, the full extent of all the data points, the amount of data, or how large social media companies collect and store information will likely remain unknown. 230 What these companies choose to reveal determines much of what society knows today, and what they currently disclose is subject to change at any time at their discretion. 231 Additionally, the data they collect is more than what a user perceives, since the data is a combination of raw data and metadata. 232 For example, consider Twitter-a social media platform allowing users to communicate via short character-limited posts called "tweets." 233 When a user posts a tweet, the post creates a record. 234 Just 4% of the record is the text in the tweet itself, while the remaining 96% of the record is additional data related to the tweet that the user may not observe, including how the tweet is stored. 2 1 Understanding the extent and power of social media data is a complex endeavor.23 6 The lack of academic research regarding social media data highlights the tasks' complexity while also contributing to the haze surrounding the extent of a social media company's "knowledge":

In recent years, the explosion of social media platforms and the public collection of social data has brought forth a growing desire and need for research capabilities in the realm of social media and social data analytics. Research on this scale, however, requires a high level of computational and data-science expertise, limiting the researchers who are capable of undertaking social media data-driven research to those with significant computational expertise or those who have access to such experts as part of their research team.237

The limited research using social media data also makes clear that a mere possession of data does not always provide a solution to individuals. 238 Often, a person or computer needs to analyze the data before a company can use the data in any meaningful way. 239 If data does require analysis to reveal its usefulness, then that requirement supports the OSPs' argument that they only have generalized knowledge because they do not necessarily have a particular data record of counterfeit goods.240 This concept of "having" versus "knowing" aligns with other areas of law as well that distinguish possession of information from knowledge of information.241

On the other hand, OSPs analyze countless amounts of data to inform and run their businesses. 242 Some ways OSPs use the data is by evaluating user behavior within the application to determine how the applications present ads to each user, performing internal research for future business and technical development, personalizing their product offerings, and more.243 Thus far, OSPs have hid behind a veil of ignorance. 244 However, because OSPs already use data which could identify counterfeit sellers (e.g., location, behavior, Internet Protocol address of the specific user, etc.) to make internal business decisions, and since those business decisions are made by an employee within the company, OSPs should meet the knowledge requirement for contributory trademark infringement. 241

Although the technology likely exists for OSPs to easily and quickly identify and eradicate counterfeit items from their websites and applications, the central question is what liability the law should impose on an OSP versus what liability it can impose on OSPs.246 An OSP would argue it has no affirmative duty to investigate and police trademark infringing items. 247 The duty to enforce one's mark lies with the owner of the mark.248 Also, OSPs argue that they are unable to decipher the difference between counterfeit listings or postings and legitimate, non-infringing postings. 249 If one accepts that OSPs cannot accurately differentiate between legitimate and non-legitimate content unless the IP owner specifically identifies infringement, then requiring OSPs to take a more proactive role in eradicating counterfeit will require technological development. 250

Writing the code to perform actions within an application is not a free endeavor; all technological developments come with a cost. 251 To illustrate, Business Insider reported that Pinterest, a social media site dedicated to sharing photo-forward content, will spend $750 million on Amazon Web Services ("AWS") between May 2017 and July 2023.252 AWS is a cloud-based server system that many social media sites like Pinterest-and at one time Instagramuse to host most of the website's software and applications. 23 Before switching to Facebook's server center, Instagram-also a photo-focused social media siteused thousands of machines at AWS to run its application. 254 Considering Instagram has a higher number of users than Pinterest, with one billion active users as of January 2020 compared to Pinterest's 322 million active users, the cost to run an application like Instagram and store its data is far greater. 25 5 Also, not all the costs are solely monetary. 256 Every time a website implements a new feature or runs a new data query, the developer must ensure the update does not adversely impact the website's overall performance or a user's experience. 25 7

An IP owner would argue that because of OSPs' infrastructure, they must take a more proactive position in combatting the sale of counterfeit goods.258 OSPs have direct control over the infringing content and can "pull the plug" on the listings anytime. 25 9 From a moral perspective, since OSPs benefit financially-at least indirectly by incorporating counterfeit sellers' user data into their business decisions and directly through potential ad sales-OSPs should actively monitor for counterfeit listings. 260 Additionally, as the source of the data, OSPs are in a better position than third parties to identify efficient and effective methods to pinpoint counterfeit goods.261

The dichotomous wishes of these two constituents, IP owners and OSPs, led to the DMCA's safe harbor provisions. 262 The goal was to offer protection for OSPs and to ensure the internet continued to improve, while at the same time addressing the concern of copyright holders due to the sudden increase of copyright infringement online. 263 However, unlike copyright protection, trademarks act as a form of consumer protection, and thus it is even more necessary to enact similar legislation. 264

#### They use monitoring tech all the time, for other purposes

Stephen Lamar, 2023 - American Apparel & Footwear Association President and CEO. “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” Answers to Senators’ questions, 11/7, https://www.judiciary.senate.gov/imo/media/doc/2023-10-03\_-\_qfr\_responses\_-\_lamar.pdf //DH

• As we discussed during the hearing, technological solutions are available now. Most platforms are now making extensive use of data and algorithms for business purposes: to adjust the price of items based on demand (dynamic pricing) or to suggest the most relevant product to a buyer when there are multiple sellers for a similar product or to dynamically change the order or relevance of listings. This same technology could be put to good use in the fight against illegal content to remove illegal products once they have been posted, but also, more efficiently, to prevent such products from being posted on their platforms in the first place. Platforms are much better equipped to act efficiently against illegal goods than any other stakeholder.

# Information Sharing Counterplan Answers

### 2AC – Information Sharing Counterplan

#### 1. Solvency deficit – platforms won’t cooperate because they financially benefit from counterfeiting sales. That’s our 1ac Winterfeldt evidence

#### 2. Bad information turn – Reactive enforcement generates incomplete and inaccurate information – sharing it just means draining enforcement resources

Steve Pasierb, 2021 – President & CEO of the Toy Association. Written Statement submitted to the House Judiciary Committee. THE SHOP SAFE ACT: STEMMING THE RISING TIDE OF UNSAFE COUNTERFEIT PRODUCTS ONLINE, House Hearing, 5/27/01

<https://www.govinfo.gov/content/pkg/CHRG-117hhrg45396/pdf/CHRG-117hhrg45396.pdf> //DH

1.The Burden of Enforcement is Disproportionately Reactive and Placed on the Rights Holder

Currently, online marketplaces lack an effective, proactive, transparent process for screening sellers or products that are offered by sellers. Instead, under the current legal regime, the burden of enforcement disproportionately relies on rights holders and consumers to police and report infringement. The current system places no responsibility on the seller or the marketplace and instead requires that rights holders scour online marketplaces and investigate, report, and prove infringement to the marketplace before counterfeit items are removed. This causes delay, allows sales of counterfeits to unsuspecting consumers, and puts the responsibility and expense on brand owners. This problem is compounded because marketplace processes vary, forcing rights holders to constantly navigate different, and often changing, marketplace enforcement procedures. This process removes the initial burden from the seller and without basis further gives the sellers the benefit of the doubt, to the detriment of rights holders and consumers.

a. Reactive Measures Will Never Keep up with Counterfeiters and Proactive Screening Must be the First Line of Defense

While online marketplaces continue to grow and provide benefits to legitimate companies looking to more easily reach consumers, by not adequately screening sellers or products, these same marketplaces allow bad actors and sellers to prosper. Without proactive approaches, bad actors remain a step ahead and continue to flourish. Without seller screening, sellers can provide inaccurate or fake information, making it impossible for online marketplaces to track and suspend bad actors, or for rights holders, law enforcement, or consumers, to enforce their rights. Importantly, there is no amount of resources rights holders can expend to adequately neutralize bad actors if marketplace approaches are disproportionately reactive in nature.

Proactive procedures must be the first line of defense. Every marketplace must implement a proactive system to verify whether a product being sold on its platform is counterfeit and whether it meets regulations such as labeling requirements and consumer product safety regulations. While marketplaces do not act as traditional brick-and-mortar retailers that curate goods to sell to consumers, this should not absolve the online marketplace from all responsibility for the goods from which they profit.

Some marketplaces have argued that thorough verification is not possible because of the volume of sellers or products on their marketplaces. This volume of sellers and products is not inevitable though; rather, it is a business decision that online marketplaces themselves make. If a marketplace is unable to verify the identity of its sellers or products because of the high volume, that is a result of its own creation.

b. Marketplace Brand Protection Programs are Inconsistent

Many online marketplaces tout their brand protection programs and investments made. Some marketplaces claim to have expanded the ability to implement different filters and rule systems to proactively block counterfeits and some online marketplaces have begun offering more robust collaborative programs for rights holders to more easily report and submit enforcement claims.

Unfortunately, to date, it appears that these have had little impact on counterfeiters. In part, this may be because they are inconsistently applied, and they remain largely reactive. Toy Association member experience is that certain tools are only made available to brands that have registered for particular marketplace enforcement programs that may have onerous terms; some are only available at a cost to the brand owner; and some may only be available to accepted brands after application to the marketplace. Further, they are not uniform across marketplaces.

Another hinderance is that marketplace shipping practices can create further enforcement challenges. At least one marketplace that fulfills third party orders will ship product from the warehouse closest to the consumer, regardless of whether it is the seller from which the consumer ordered. If shipped from a seller that is different than the one from which the consumer purchased, this creates another layer of obfuscation, removes consumer choice, and hinders seller identification, investigation, verification, and enforcement.

c. A Lack of Transparency and Verification of Seller Identity Undermines Enforcement

Transparency of seller information remains inadequate, resulting in a lack of information available to consumers making purchasing decisions, and to rights holders and law enforcement attempting to track and enforce against counterfeiters. Some online marketplaces are beginning to increase access to seller information, such as through brand owner programs. However, access is often inconsistent across marketplaces, providing a variety of different information depending on the program.

Further, even when marketplaces do offer such information that is necessary for subsequent enforcement actions, it is often incomplete or incorrect due to inadequate preliminary verification. Without complete or verified information, rights holders cannot take the necessary next steps and are often forced to expend time and valuable resources chasing dead ends.

#### 3. Permutation – do both. Increasing information sharing and contributory liability provides stronger incentives for cooperation.

#### 4. Criminal prosecution fails – they can’t prove the third-party seller knew the mark was counterfeit

John H. Zacharia and Kari Kammel, 2020 - John H. Zacharia is former Assistant Deputy Chief for Litigation for the Computer Crime and Intellectual Property Section of the United States Department of Justice’s Criminal Division. Kari Kammel is the Assistant Director of Education and Outreach at the Center for AntiCounterfeiting and Product Protection at Michigan State University. “HOW CONGRESS PROPOSES TO PROTECT CONSUMERS FROM ONLINE COUNTERFEITS: The Good, the Bad, and the Ugly” September,

<https://a-capp.msu.edu/wp-content/uploads/2020/09/How-Congress-Proposes-to-Protect-Consumers-From-Online-Counterfeits.pdf> //DH

For its part, Amazon made a series of new announcements in its efforts to combat counterfeits sold on its platform. For instance, on January 13, 2020, and perhaps in anticipation of the DHS Report’s release less than two weeks later, Amazon announced though an anonymous source that, going forward, it “will report a merchant’s name, company name, product and contact information to authorities, after it confirms a business was selling fakes, closes the seller’s account, and the account holder does not make a successful appeal via Amazon’s typical processes.”78 This effort may produce an impressive number of referrals to law enforcement, but it may not be a good measure of its effectiveness for one simple reason: evidence of counterfeiting alone is not a federal crime. Federal law generally authorizes criminal prosecutions only against those who intentionally traffic in goods and knowingly use a counterfeit mark.79 Recent initiatives with the National Intellectual Property Rights Coordination Center, part of the U.S. Department of Homeland Security, have been coordinated to discuss data sharing with federal law enforcement.80 However, flooding law enforcement with information about thousands of third-party sellers without any evidence that the seller knew the mark was counterfeit will probably be an empty exercise that will lead to few new federal criminal trademark counterfeiting prosecutions.

### 1AR – Platforms Won’t Cooperate

#### Info-sharing fails - empirically

Matt Priest, 2018 - President & CEO Footwear Distributors and Retailers of America. FDRA Response to Senate Finance Committee Letter on Counterfeiting Investigation, 6/29, <https://www.iacc.org/wp-content/uploads/The-Fight-Against-Fakes_SenateFinanceCommitteeReport_2019.pdf> //DH

U.S. footwear companies are involved in various programs and activities internationally to address shortfalls in this area: awareness campaigns; domain name seizures; collaboration on investigations and actions against vendors active on social media, through websites, or selling platforms; and participation in the Memorandum of Understanding lead by the European Commission, which aims to facilitate collaboration between brands and several major selling platforms.

While these actions are important in helping to combat online sales of counterfeits, their impact has been limited for a number of reasons: platforms do not willingly and fully share the information they have regarding counterfeiters, law enforcement agencies have difficulties prioritizing the targets for which their action would have the biggest disruptive impact, brands do not have the capacity to easily identify targets or the most visible and active counterfeiters, and it remains very difficult for brands to identify counterfeits offered online without assistance from the platforms that have background information regarding their vendors (brands do not have access to this information). Some FDRA companies have also been unable to effectively engage with foreign countries, because they have been unable to locate the originating source of the counterfeit product.

#### Platforms don’t collect enough seller information to share because current liability is too weak

John H. Zacharia and Kari Kammel, 2020 - John H. Zacharia is former Assistant Deputy Chief for Litigation for the Computer Crime and Intellectual Property Section of the United States Department of Justice’s Criminal Division. Kari Kammel is the Assistant Director of Education and Outreach at the Center for AntiCounterfeiting and Product Protection at Michigan State University. “HOW CONGRESS PROPOSES TO PROTECT CONSUMERS FROM ONLINE COUNTERFEITS: The Good, the Bad, and the Ugly” September,

<https://a-capp.msu.edu/wp-content/uploads/2020/09/How-Congress-Proposes-to-Protect-Consumers-From-Online-Counterfeits.pdf> //DH

By the same token, third-party sellers’ use of e-commerce platforms in this way comes with obvious risks to consumers. Unlike when it sells its own branded products, e-commerce platforms cede control to third-party sellers to decide which products to sell, the means of shipping those products, and even pricing. Thus, although e-commerce platforms will typically prohibit third-party sellers from trafficking in illegal products, a counterfeiter can easily circumvent this prohibition by making the counterfeit product appear genuine. Furthermore, e-commerce platforms may not collect sufficient information to identify third-party sellers – making it harder (and in some cases impossible) for customers or brand owners to pursue third-party counterfeiters or those selling counterfeits online. And when ecommerce platforms neither store nor ship the third-party sellers’ products, they are effectively choosing to be blindfolded from seeing whether the products sold by third parties are genuine, or even seeing third-party sellers’ real identities.

### 1AR – Criminal Enforcement Fails

#### Cooperation for criminal enforcement fails. Civil liability is more effective at shutting down counterfeiting networks

Rebecca Dunlevy, 2012 -JD, Fordham University Law. “Internet Immunity: The Limits of Contributory Trademark Infringement Against Online Service Providers,” 22 Fordham Intell. Prop. Media & Ent. L.J. 927 (2015). Available at: https://ir.lawnet.fordham.edu/iplj/vol22/iss4/6 //DH

These criminal penalties have been largely ineffective in eliminating the wide-scale infringement of consumer goods because U.S. laws do not impose significant penalties for infringement45 and the producers of infringing goods are generally located outside the United States.46 Where the operation includes a storefront or offers goods in-person, the individual sellers of counterfeit goods are often illegal immigrants working in informal trafficking rings with ties to producers or organized crime outside the United States.47 The arrest of individual sellers has a limited impact on the importation of counterfeit goods because the individual sellers are generally replaceable due to their illegal status.48 In addition, trafficking rings can easily utilize mainstream shipping methods to move large quantities of infringing product into the U.S. or other developed countries‘ markets.49

Furthermore, even when offenders are arrested they are generally not punished to the full extent that the intellectual property laws allow. The Obama Administration‘s White Paper on Intellectual Property Enforcement Legislative Recommendations (“White Paper”)50 recommended an increase in the sentencing range for intellectual property crimes (less than half of those convicted received prison sentences) and for recidivist intellectual property crime offenders.51 The White Paper noted that intellectual property crimes were light on punishment despite the high profit margins associated with trademark infringement, providing the incentive to sell counterfeit goods, and the relationship of counterfeiting activity to organized crime.52 It is not yet clear if the implementation of these recommendations will impact the counterfeit market.

The meaningful enforcement of criminal counterfeiting laws and civil trademark infringement suits continues to be a challenge for both law enforcement and trademark owners. Trademark owners, unlike law enforcement, are able to use a wider variety of civil tactics to shut down counterfeiting rings. By pursuing those who facilitate direct infringement under theories of secondary liability, brand owners can make the provision of counterfeit goods to consumers significantly more difficult and costly for counterfeiters and associated parties.

# Circular Economy DA Answers

### 2AC – Circular Economy DA

#### 1. Non-unique – the circular economy is decreasing

Rachel Meidl, 2023 – Fellow in Energy and Sustainability at the Baker Institute. “Closing the Loop on the World’s Fastest-growing Waste Stream: Electronics” 6/14,

<https://www.bakerinstitute.org/research/closing-loop-worlds-fastest-growing-waste-stream-electronics> //DH

A circular economy is most effective when working symbiotically across supply chains to create value. However, a strong waste-centric and “end-of-pipe” narrative limits the vast social, economic, and environmental opportunities that newer circular models can offer, such as dematerialization and greater resource optimization. These economic opportunities are far broader and more diverse than those focusing solely on end-of-life activities, especially in an ideal circular economy where products and processes are designed to avoid the creation of waste in the first place. But the current global economy is only 8.6% circular and trending down from previous years.[29] Absent a shift in policies, business and consumer behaviors, and innovation, the amount of e-waste alone could more than double by 2050,[30] driving society further away from realizing a circular economy.

#### 2. No link – the safe harbor limits trademark bullying

Sally Feingold et al, 2015 - counsel for Etsy, Inc “IN THE MATTER OF DEVELOPMENT OF THE JOINT STRATEGIC PLAN FOR INTELLECTUAL PROPERTY ENFORCEMENT. COMMENTS OF ETSY, FOURSQUARE, KICKSTARTER, MEETUP, AND SHAPEWAYS” 10/16, <https://extfiles.etsy.com/advocacy/Etsy_IPEC_Comment.pdf> //DH

**OSP = Online Service Provider**

Where They Exist Safe Harbors Provide a Check Against Over-Enforcement

When they are in place, OSP safe harbors help protect against over-enforcement by allowing users to push back against problematic takedown requests. First, users do not need permission or agreement from OSPs protected by safe harbors before challenging an infringement claim viewed as illegitimate. Second, removing the OSP from the decision-making process facilitates user pushback against abusive claims. These challenges can lead to public litigation, bringing edge cases into the public discussion.

Key to understanding the value of safe harbors is recognizing the differing viewpoints of OSPs and their users. OSPs - Commenters included - must consider the best interests of their entire user base when evaluating a request to take down an individual item. Within that rubric, it is often rational to comply with a marginal, but colorable, request for any individual item to be taken down in order to protect the larger viability of the entirety of the user base and avoid costly litigation over a single item.

This is even truer for smaller OSPs who may be unable to afford legal fees required to consider the merits of the claim. Faced with threats of an expensive lawsuit due to an allegation of infringement, and devoid of the protection granted by a safe harbor, startups and small OSPs have more incentive to err on the side of over-accommodation - even at the expense of an individual user's free speech and legitimate activity.

Individual users have a significantly different perspective. What is a single piece of content among many for a service provider may be the user's livelihood. In those cases, the user's motivation to challenge over-enforcement is much greater than the OSP's. If OSPs had the security of safe harbor protections, OSPs would not need to hinder users from pushing back against rightsholder claims simply to avoid getting involved.

#### 3. No link – reputational harm and sanctions limit trademark bullying.

Jason Vogel and Jeremy A. Schachter, 2013 - Partner, Kilpatrick, Townsend & Stockton and Associate, Kilpatrick, Townsend & Stockton “HOW ETHICS RULES CAN BE USED TO ADDRESS TRADEMARK BULLYING” The Trademark Reporter, v.103, n2, <https://ktslaw.com/~/media/Files/articles/2013/vol103_no2_a3.ashx> //DH

The study, which was conducted by the USPTO, analyzed current trademark enforcement as well as the impact of such enforcement on the marketplace. It evaluated the scope of trademark rights and litigation. As for trademark bullying at the pre-litigation stage, it found that empirical evidence was lacking and solicited public comment to determine its impact. It sought feedback from trademark owners and practitioners “regarding their experience with litigation tactics, especially those involving an attempt to enforce trademark rights beyond a reasonable interpretation of the scope of the owner’s rights.”18 One prompt used by the USPTO in soliciting comment included the following:

Please describe situations where you have been involved in receiving a cease-and-desist letter. Anecdotal information might include, but is not limited to, a description of whether the letter resulted in the small business ceasing its use of one or more marks, or whether the sender of the cease-and-desist letter withdrew or abandoned its demands against the small business owner.19

This prompt was clearly meant to determine the impact of trademark bullying at the demand letter stage. Comments were received from several stakeholders groups such as the International Trademark Association (INTA), the American Intellectual Property Law Association (AIPLA), and the Intellectual Property Owner’s Association (IPO).20

For its part, INTA responded that regulation was not the answer and that education would be a better solution. It deemed the remedies available at law for overly aggressive assertions of trademark rights as sufficient, and cited the availability of sanctions, attorney’s fees, declaratory judgments, and reprimands from state bars. Further, it regarded cease and desist letters as important tools—whether overly aggressive or not—to enable parties to enter into a negotiation or alternative dispute resolution, thereby preventing the burden of litigation for either party.

The AIPLA largely echoed the sentiments of INTA. It pointed out how existing trademark law does not merely permit mark owners to be aggressive, it requires them to be. It cited Judge Leval’s discussion regarding Procter & Gamble after it lost a trademark suit. “Procter & Gamble cannot be faulted for zealously protecting [its] trademark interest. Indeed, the trademark law not only encourages but requires one to be vigilant on pain of losing exclusive rights.”21 AIPLA also discussed the notion that small businesses have the David & Goliath angle on their side, which enables them to rally public support in their favor and publicly shame a large, overly aggressive mark owner. If effective, this strategy would be available at even the demand letter stage.

#### 4. No impact - Existing circularity is circular greenwashing – it has no environmental benefit

Steve Harris et al, 2021 - IVL Swedish Environmental Research Institute, Life Cycle Management “Circularity for circularity's sake? Scoping review of assessment methods for environmental performance in the circular economy.” Sustainable Production and Consumption Volume 26, April 2021, Pages 172-186, <https://www.sciencedirect.com/science/article/pii/S2352550920305236> //DH

Recently there has been a rise in circularity indicators (at both product and macro-level) with Saidani (2018) reviewing 55 indicators and Parchomenko (2019) reviewing 63 indicators. Many of these measure material or value re-circulation, apparently as a proxy for environmental impact (Elia et al., 2017; European Commission, 2019; Saidani et al., 2019). Such measurements arguably risk driving action based on increased circularity and not necessarily on improved environmental performance – leading to what we refer to as “circularity” for circularity's sake. Moreover, there is currently limited evidence that company-level actions (e.g. developing product-service systems) and products designed for increased circularity (e.g. increasing longevity or recyclability) have increased environmental performance, particularly from a macro- perspective (Tukker, 2015).

In accordance, Esty and Porter (1998) (pg. 40) referring to industrial ecology, note that “The belief in the perfection of the circle can be taken too far. Even when company gains and social benefits are summed, the costs of closing some loops may exceed the benefits.” There is also a risk of “circular [green]washing”, reminiscent of the so-called “green-washing” that emerged in the 1990’s (Welford, 1997), where a company uses inaccurate information for marketing purposes.

#### 5. No impact – the environment is resilient

Jessica Weinkle, 2024 – Associate Professor in the Department of Public and International Affairs at the University of North Carolina Wilmington. She holds a doctorate in Environmental Studies from the University of Colorado Boulder. “How Planetary Boundaries Captured Science, Health, and Finance” Breakthrough Institute, 6/14, <https://thebreakthrough.org/journal/no-20-spring-2024/how-planetary-boundaries-captured-science-health-and-finance> //DH

The Planetary Boundaries enterprise

On the surface, Planetary Boundaries and its various derivatives seem scientific. They appear in notable scientifically-oriented journal outlets like Nature and Science, and they tend to involve lots of complicated calculations and formulas.

The framework posits nine thresholds under which “humanity can operate safely.” These range from climate change to ocean acidification to rates of biodiversity loss. If any of the boundaries (or perhaps some of the boundaries) are transgressed (for some unknown amount of time) the earth will no longer be safe (at some unknown point in the future).

There is some logic here, but the framework is inherently arbitrary. It conflates regional and global scales, which artificially constrains policy options and presents in technocratic form a moral philosophy for social and economic development. Planetary boundaries embed the ideas of tipping points, tipping elements, and tipping cascades, which also suffer from muddle; indeed, there is “no rapidly approaching planetary cliff.”

The idea of Planetary Boundaries first appeared in 2009 in the journalEcology & Society as a “proof of concept paper.” The paper’s lead author, Johan Rockström, had joint association with the Stockholm Resilience Center at Stockholm University and the Stockholm Environment Institute (SEI) supported by the Swedish government.

### 1AR: Nonunique - Circular Economy Decreasing

#### Newest research shows circularity trends are declining

Circle Economy Foundation, 2024 - We are a global impact organisation with an international team of experts based in Amsterdam. Report created in collaboration with Deloitte, a consulting firm. “The Circularity Gap Report: 2024” <https://drive.google.com/file/d/15droT_mBFK6Kkd1aO5kPzYFUqLdul2qM/view> //DH

Despite the circular economy entering the mainstream, global circularity is still in decline.

Over the past five years, the volume of discussions, debates, and articles addressing this topic has almost tripled, reflecting a heightened awareness and interest in circularity.1 However, the vast majority of extracted materials entering the economy are virgin, with the share of secondary materials declining steadily since the Circularity Gap Report began measuring it: from 9.1% in 2018 to 7.2% just five years later in 2023. Meanwhile, the total amount of materials consumed by the global economy continues to rise: in just the past six years alone we have consumed over half a trillion tonnes of materials—nearly as much as the entirety of the 20th century. These statistics display the cold, hard truth: despite the circular economy reaching ‘megatrend’ status, lofty speeches and targets are not yet translating into on-the-ground actions and measurable impacts. Without bold, urgent action to shift to a circular economy, we'll miss out on achieving broader social and environmental goals—ranging from emissions reductions to boosting the use of secondary materials—putting industries and governments at risk of sleepwalking into circular washing and missing out on much-needed impact.

#### Too many barriers exist for a circular transition

David Sehyeon Baek, 2023 - investment, fundraising and cybersecurity specialist at CGS-CIMB Singapore and NPCore Korea. “The Circular Economy Can't Save Us, But We Haven't Even Gotten Started” 8/18, <https://www.linkedin.com/pulse/circular-economy-cant-save-us-we-havent-even-gotten-started-baek-#:~:text=Reduce%20and%20Reuse%20are%20more%20effective%20as%20they%20prevent%20waste,circular%20without%20genuinely%20integrating%20sustainability>. //DH

The global economy remains wasteful, linear, and excessively dependent on fossil fuels. Despite the rise of the circular economy concept, over 90% of resources end up as waste, accelerating both pollution and climate change.

Challenges of Shifting to a Circular Economy: Transitioning from a linear to a circular system is complex. Replacing the “take, make, dispose” model requires a collective effort, rethinking consumerism, and reshaping supply chains to design out waste and enhance product longevity.

Insights from Sustainability Week Asia: Only 8.6% of the world's economy is circular, and the majority of resources don't return to production cycles. The emissions from single-use plastics in 2021 were massive, equal to all GHG emissions from the UK. Supply chain inefficiencies contribute significantly to waste and emissions.

The Difficulties in Achieving a Truly Circular Economy: Current economic and regulatory frameworks favor linear models, making circularity challenging. A circular approach requires coordination along the entire value chain, involving different stakeholders, including industry competitors, policymakers, and consumers.

The Shortcomings of Recycling: Recycling, especially of plastics, hasn't scaled up at the rate needed to match consumption growth. Various challenges like the cost of collection, sorting, contamination of materials, and the affordability of virgin plastic hinder effective recycling. Major brands like Coca-Cola are finding it hard to source recycled plastic at feasible costs.

Broader Implications of Failing to Adopt a Circular Model: Not embracing a circular economy can negatively affect businesses due to lost opportunities to retrieve valuable raw materials and potential regulatory pressures. Europe is leading the way with forthcoming circular economy standards.

It is true that the circular economy concept holds promise for a sustainable future. However, its actual implementation is riddled with complexities and challenges. There's a strong need for collective action, regulatory support, and behavioral shifts to make significant progress towards this goal.

Implementing Circular Economy Is Not So Simple

Despite being far removed from major metropolitan areas, even Arctic sea ice contains microplastics, indicating that pollution is now omnipresent in the world's oceans. Humanity produces around 1.3 billion tons of trash annually, which is leading to environmental and geopolitical challenges. The current economy is largely linear, focusing on production and disposal rather than reuse and recycling.

Consumer Expectations for Convenience: The modern lifestyle, heavily reliant on disposable, single-use plastics, has made the zero-waste lifestyle seem challenging and distant.

Regulatory Barriers: Some government regulations inadvertently promote wastefulness. For instance, misunderstanding expiration dates on food products leads to unnecessary waste.

Insufficient Waste Infrastructure: Especially in developing nations, a lack of proper waste management systems contributes significantly to plastic pollution in natural environments.

Inadequate Recycling Technology: Current recycling methods often degrade the quality of plastics. Advanced technologies are required to recycle plastics without compromising their quality.

Unsustainable Business Models: The global rise in the middle class implies increased consumption. Companies need to reinvent their production and distribution methods to accommodate this growth without overburdening the environment.

### 1AR: No Link: Safe Harbor

#### Trademark protection with safe harbors are the vital internal link to the platform economy

Sonia K Katyal & Leah Chan Grinvald, 2018 - \*Chancellor's Professor of Law; Co-Director, Berkeley Center for Law and Technology, University of California, Berkeley AND \*\*Associate Dean for Academic Affairs and Professor of Law, Suffolk University Law School. “PLATFORM LAW AND THE BRAND ENTERPRISE” BERKELEY TECHNOLOGY LAW JOURNAL [Vol. 32:1135, <https://scholars.law.unlv.edu/cgi/viewcontent.cgi?params=/context/facpub/article/2394/&path_info=Platform_Law_and_the_Brand_Enterprise.pdf> //DH

Central to these questions remains the ubiquity of the brand enterprise, which affects nearly every layer of platform architecture. Trademarks are central to the success of the platform economy, but few commentators have really delved into the question of how trademark law both governs and is governed by - the emergence of these new economies. Thus, this Article lays out a spectrum of trademark interactivity, identifying the emergence of two central forms of platform entrepreneurship, and then analyzes how the design and architecture of these new forms ushers in new challenges and opportunities for the modernization of trademark law altogether.

Trademark law plays a central, determinative role in the success or failure of the platform enterprise. At the broadest level, in Part II, this Article argues that the platform economy facilitates the emergence of what is called "macrobrands" - the rise of platform economies whose sole source of capital inheres in the value of the brand itself - the Airbnbs, Ubers, and eBays of the world.23 At the narrowest level, Part III argues that the platform economy, with its empowerment of the individual, has also facilitated a parallel emergence of the "microbrand" - the rise of discrete, small enterprises made up of individual businesses, each of whom have a strong interest in utilizing the basic principles of branding and trademark protection.

Indeed, this Article views the platform economy as a central opportunity to modernize existing trademark law to accord with the challenges of these new business models. As shown in Part II and Part III, the interaction between macrobrands and microbrands challenges trademark law to evolve to address the new issues presented by platform economies. At the same time, however, our existing frameworks are capacious enough to meet the challenges platforms pose, underscoring the wisdom of the basic, bedrock trademark principles in the process. In Part IV, we outline a host of suggestions to modernize, rather than displace, trademark law for the digital economy. While change can occur by legislation or voluntary measures, this Article focuses specifically on the formation of statutory safe harbors and the modification of the standards for infringement in common law. As this Article shows, these changes can both protect and encourage the vibrancy of the platform economy in an age of legal uncertainty.

#### It's only the lack of a safe harbor causes over-enforcement

Sonia K Katyal & Leah Chan Grinvald, 2018 - \*Chancellor's Professor of Law; Co-Director, Berkeley Center for Law and Technology, University of California, Berkeley AND \*\*Associate Dean for Academic Affairs and Professor of Law, Suffolk University Law School. “PLATFORM LAW AND THE BRAND ENTERPRISE” BERKELEY TECHNOLOGY LAW JOURNAL [Vol. 32:1135, <https://scholars.law.unlv.edu/cgi/viewcontent.cgi?params=/context/facpub/article/2394/&path_info=Platform_Law_and_the_Brand_Enterprise.pdf> //DH

**ISP = Internet Service Provider**

According to Stacey Dogan, existing trademark frameworks unwittingly encourage aggressive behavior through two central mechanisms.155 The first involves the oft-mentioned trope that trademark owners must police their marks.156 The existing lack of clarity regarding trademark owner's duty to police can lead to overenforcement, lending further strength to the perception that "stronger" marks receive more protection, and "weaker" marks get less. As Dogan explains, although trademark owners are required to take certain steps to enforce their marks, the confusion regarding the required level of notice to prospective defendants encourages them to take an "object first, analyze later" approach.1 57 As a result, many trademark owners take an approach that objects to all third party uses of their marks, even when confusion does not result.158 Dogan concludes, therefore, that many cases of trademark bullying involves value maximizing choices-trademark owners object, not because they risk "losing their marks if they fail to object, but because their rights will be more valuable if their objection succeeds."159

Consider dilution protections, as one example. Even though the strongest, most famous marks carry the least risk of losing their distinctiveness, the law's existing framework directs courts to consider the extent to which a mark holder engages in "substantially exclusive use of the mark," thereby indirectly encouraging trademark holders to overpolice their marks to satisfy this standard.160 Similar concerns regarding exclusivity also carry over into the standard for infringement, as well. This leads trademark owners to police their marks for anything remotely appearing similar, as a function of preserving the value of a mark, rather than guarding against a true risk of confusion. 161

These harms become even more apparent when we turn to the architecture of platforms. Due to the absence of trademark safe harbors, ISPs cannot institute a counter notice procedure for solely trademark-related claims; and as a result, users do not have the ability to challenge the notification and keep their work online.162 Etsy, for example, has observed that its number of trademark-related takedown notices is greater than the copyright-related ones that it has received.163 It offers examples of the notices it has faced: one involving a graphic designer using the trademarked name of a television show on a set of custom party invitations; an artist using a trademarked cartoon character in a humorous oil painting; or a small business owner who repackages food packaging into purses and liquor bottles into drinking cups.' 64 Even though each of these instances might be the subject of strong arguments for non-infringing uses, each of them was the subject of a takedown notice. 165

Because of the absence of clear safe harbors in the ISP context with respect to trademark law, commentators have argued that many ISPs will not challenge trademark requests in order to avoid becoming embroiled in costly litigation.166 As a recent filing by Etsy and other platforms concluded, "[t]he result is that a trademark claim - even one built on a weak foundation - can be an effective way to permanently quash the speech or economic activity of others." 67 In such cases, because of the complexity of trademark law, and the David vs. Goliath status of the user vs. the trademark owner, respectively, ISPs may not even provide the user with an opportunity to challenge the assertion of infringement.168 Here, small businesses, individual entrepreneurs, and ordinary creators might be most affected by such notices, simply because they lack the resources and channels to challenge their targeting. 169 And smaller ISPs, since they may be unable to afford the legal resources required to investigate a claim, may err on the side of over-accommodation as a result.170 Over the long term, these abusive practices can have the effect of actually undermining support for intellectual property altogether. As Etsy and others have noted, "[a] steady stream of examples of abuse can reduce the legitimacy of rightsholders as a whole in the eyes of the public, thus reducing public support for enforcement even in legitimate cases of infringement." 171

### 1AR: No Link: Reputational Harm

#### The possibility of reputational harm reduces bullying incentives

Patricia E. Campbell, 2023 - Law School Professor and Director of the Intellectual Property Law Program at the University of Maryland Carey School of Law “Debugging the Trademark Laws: The Lanham Act and Counterfeit Microelectronics,” 31 TEX. INTELL. PROP. L.J. 211 (2023). Hein Online. Accessed via University of Michigan //DH

Relying on cease-and-desist letters may result in unintended negative consequences, however. If a parts manufacturer sends a cease-and-desist letter to an accused counterfeiter, it may lose any right to obtain an ex parte seizure order from the court, thereby forfeiting one of the valuable tools provided by Lanham Act.368 Sending a cease-and-desist letter could also result in the commencement of a declaratory judgment action by the prospective defendant, potentially in a district where the manufacturer would prefer not to litigate, or it could result in the goods or the counterfeiter disappearing from the jurisdiction.369 The recipient of an aggressive demand letter may also use social media to post the letter and subject the trademark owner to public scorn.370 “Being perceived as a trademark bully does not help the brand’s reputation.”371

#### Shaming limits trademark bullying

Michael J. Choi, 2019 - J.D., University of San Francisco School of Law. ARTICLE: The Likelihood of Exclusion: Economic Disparity in the United States Trademark System. Journal of the Patent and Trademark Office Society, 100, 599 Nexis Uni //DH

Shaming is an effective method to fight trademark bullies because it is a cost-effective alternative to litigation. 172 Small businesses may lack the benefits of legal counsel and financial resources to defend themselves, 173 but shaming is available to anyone with a credible business and an Internet connection. 174 Because of today's social media prevalence, trademark shaming is often a viable option. 175 A business can mobilize the community "simply through 'tweeting' about receiving the cease-and-desist letter." 176 Social media ensures that if the particular bullying is egregious enough, media outlets will report the story. 177

A 2014 trademark dispute between bicycle behemoth Specialized Bicycle Components Inc. and small Canadian bicycle shop Roubaix illustrates this phenomenon. 178 The Internet immediately rushed to Roubaix's aid when it received a cease and desist letter from Specialized. 179 The merits of the infringement claim were irrelevant, as "support for [Roubaix] was so overwhelming, and condemnation of Specialized so swift." 180 Specialized was quick to withdraw its cease and desist letter and issue an apology. 181 This story demonstrates the importance of a shamer's credibility in a community, since the Internet would not have mobilized unless Roubaix was a hard-working and respectable business.

### 1AR: No Impact: Circular Greenwashing

#### Circularity has no environmental impact – it expands consumption overall

Elizabeth L. Cline, 2020 – journalist. “Will the Circular Economy Save the Planet?” Sierra Magazine, 12/23, <https://www.sierraclub.org/sierra/2021-1-january-february/feature/will-circular-economy-save-planet> //DH

To begin with, it's important to note that the business community is promoting circular economy projects involving resale, rental, and even more-durable design to entrepreneurs as an additional revenue stream. A 2016 McKinsey & Company report on circularity frames it as an opportunity to expand markets to a new customer group without cannibalizing existing sales. It estimates that the European economy could unlock about $2 trillion from new circular economy businesses like electronics refurbishment and textile-to-textile recycling and simply from the "increased spending fueled by lower prices" associated with shared and secondhand products. Likewise, the business consulting firm Accenture promises a staggering $4.5 trillion windfall from investing in new circular economy businesses, including those that focus on advanced recycling technology, innovative new recyclable materials, sharing platforms (like ride or home sharing), or subscription models (like fashion-rental website Rent the Runway). Russell concedes that most big businesses that are exploring circularity aren't doing so at the expense of their main revenue streams. "These companies are not abandoning their make-new-products strategy," she says.

What that means is that in fashion and elsewhere, the circular economy is not replacing the linear economy; it's merely running parallel to it. In other words, circularity is being positioned as a way to drive new growth, not necessarily as a way to cut down on the use of raw materials. There's no evidence that any of the large brands embracing circularity are actually using fewer virgin resources overall. The fashion industry is a case in point: It still manufactures an estimated 100 billion garments annually, enough for every human on the planet to buy something new to wear every month. Total production of virgin textiles—whether polyester, cotton, or rayon—hit historic highs in 2019.

#### Circular washing increases consumption

Elizabeth L. Cline, 2020 – journalist. “Will the Circular Economy Save the Planet?” Sierra Magazine, 12/23, <https://www.sierraclub.org/sierra/2021-1-january-february/feature/will-circular-economy-save-planet> //DH

What's more, by emphasizing reuse and recycling—rather than reducing production—the circular economy runs the risk of becoming a red herring, enabling companies to increase their environmental impact while appearing greener to the public. The circular economy is essentially riding on decades of public conditioning that has us convinced that reuse and recycling are always good for the planet, but that's not the case. "We've tried [reuse and recycling] over and over again, and it just hasn't worked," says Roland Geyer, a professor in industrial ecology and pollution prevention at the University of California at Santa Barbara and a critic of the circular economy.

The economics and difficulty of recycling complex consumer goods like electronics, cars, and furniture mean that wide-scale refurbishment and recycling of most products remain elusive. But even if industry were to overcome these barriers and finally scale up recycling, virgin-resource consumption still might not decrease. This is partly because recycling itself requires water, energy, and chemicals. It is far from a zero-impact process. In the case of recycling textiles, energy is needed to spin old fibers into new material, then chemicals are required to dye and finish that material into garments, and more energy is needed to ship them to retail stores. A 2018 Quantis report on the fashion industry found that scaling up to clothing made from 34 percent recycled materials would only cut carbon emissions across the industry by a mere 5 percent.

In fact, designing products so they're made to be recycled and reused could drive up overall consumption of virgin resources. In a 2017 paper, Geyer and environmental science and management expert Trevor Zink explain how the circular economy could be initiating a rebound effect. Besides creating new and separate markets for cheap secondhand products that don't replace new products, it could dramatically increase the supply of recycled materials. This would put them in competition with virgin materials, driving the price of both down and the consumption of both up.

Steel, for example, is the most widely recycled material, and yet consumption of primary steel has doubled in the past 20 years. Because the total consumption of resources is growing by about 3 percent every year, it's difficult to make every new thing out of old things, which means recycled material will always be in competition with virgin material. "The whole point, the only point, of reusing and recycling is so we make less new stuff," says Geyer. "And that's just not happening."