# Shop Safe Act Negative

## File Explanation

This file contains responses to the Shop Safe Act affirmative.

#### Counterfeiting Advantage Answers

The negative can argue that many of the claims made by the 1ac is false: online counterfeiting is not a huge problem, that most counterfeiting occurs in physical markets, not online markets, and that the impact claims about cyber-attacks on the military and the power grid are greatly exaggerated. The negative also has a cooperation turn that says that putting liability on online platforms reduces their incentive to cooperate against counterfeiting now. The turn assumes that platforms are doing a lot to try to stop counterfeiting, but that liability means they’ll decrease their efforts to only comply with the bare minimum of what the law requires.

#### Money Laundering Advantage Answers

The negative can also challenge the central claims of this advantage. The strongest argument is the claim that current anti-money laundering efforts fail. The affirmative might reduce online counterfeiting, but money laundering occurs in many different areas that the affirmative does not affect. The negative can also say that the impact to terrorism is greatly exaggerated. Finally, they can contest the claim that the plan harmonizes a global approach to anti-money laundering. The argument is that the safe harbor provision in the SHOP SAFE Act is so expensive to meet that it will disrupt e-commerce altogether, rather than create stronger enforcement.

#### Circular Economy Disadvantage

This disadvantage claims the SHOP SAFE Act will harm small online platforms – startups and secondary resale markets – that are developing innovative methods to build and market products, especially second-hand products. It claims that the economy is in the midst of a transition to becoming more ‘circular’ – in other words, there’s a growing market for reusing, recycling, refurbishing, or upcycling (modifying) products, and that this transition will reduce consumption of new resources, reducing the environmental footprint of US consumerism.

It claims that the plan’s imposition of liability on online platforms will be abused by trademark owners, who will try to file lawsuits against perfectly legitimate online platforms because they want to shut down re-sale markets that compete with the trademark owners’ products. Abusive enforcement is called “trademark bullying.” The idea is that if online resale platforms fail, then the circular economy transition fails as well. The impact is environmental damage from consumption – the greater amount of new resources we consume, the greater the likelihood of more pollution and eventual environmental collapse.

#### Information Sharing Counterplan

This counterplan claims that instead of imposing trademark liability on online platforms, the Congress should just increase counterfeiting enforcement through other channels. Primarily, this means that Customs and Border Protection, the law enforcement agency in charge of stopping imported counterfeit products, should work directly with both trademark owners (“brands”) and online platforms, to share information about best practices, to work on developing new or improved detection technology, and work cooperatively to develop cost-effective proactive enforcement.

The net benefit is all three disadvantages turned out in the packet, as well as the Circular Economy DA. All of these arguments say “strengthening trademark protection is bad.” The counterplan strengthens anti-counterfeiting enforcement, but it does not strengthen trademark protection.

# Case

## Counterfeiting Advantage Answers

### 1NC – Counterfeiting Advantage Answers

#### 1. Counterfeiting is exaggerated and their statistics include physical sales

Matthew Schruers, 2023 - President Computer & Communications Industry Association “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

MATTHEW SCHRUERS: We're just talking about the scale of the problem. And I would note that all of these statistics that we're looking at are by their own terms, wildly inflated relative to the problem that we're talking about. First of all, many of them are the upper range and so we get a site of between X and Y. And Y is the top figure and then Y becomes the figure, so. We need to realize that -- that the outer bound is not the median figure.

Secondly, most of these figures apply and include copyright piracy, patent infringement. And -- and I'll be the first to acknowledge that infringement in foreign markets that have weak rule of law is a serious policy problem. That is not the problem that -- that we're talking about here. This bill is not going to do anything about pirated software in China.

It's not going to prevent patent infringement. It's -- it's not going to prevent the sale of -- a physical sale of a bootleg handbag on the street of Moscow, right? This is just about regulating online platforms. And those numbers are wildly over inclusive based on what we're talking about here. So I think we have to take these numbers with many grains of salt.

#### 2. Status quo voluntary enforcement solves now

Matt Schruers, 2023 - President Computer & Communications Industry Association. Written Statement submitted to the Senate Judiciary Committee, “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” Senate Hearing, 10/3, <https://www.judiciary.senate.gov/imo/media/doc/2023-10-03_-_testimony_-_schruers.pdf> //DH

b. Services Are Already Combating Counterfeits

The digital sector shares the sponsors' goals of preventing unsafe counterfeit products from spreading online. Responsible services invest significant resources in protecting users from illegal or unsafe goods, enforcing their terms of service and existing law to combat unsafe products and protect consumers online. Many online intermediaries engage with brand owners extensively and have established programs that encourage information sharing to enable the identification of and enforcement against counterfeit and infringing goods.4 Industry also works with law enforcement to find and hold bad actors accountable and protect consumers.

Some major e-commerce providers voluntarily provide legal tools for trademark or brand owners. These brand registration programs allow the service to better utilize automated tools to identify and remove confirmed counterfeit products. Through enrollment, brand owners provide relevant information to the service about their products that better enables the service to proactively address counterfeits, and to streamline brand owners’ reporting process. In enforcing their strict prohibitions against counterfeiting, in many cases services will take more extensive action than merely removing content that is specifically reported to them, and are exploring ways to remove additional suspected counterfeit content on a proactive basis, with some already doing so 99% of the time.5 Some sites voluntarily publish data in their recurring transparency reports that detail removals on counterfeit goods, in addition to takedowns related to trademark claims.6

#### 3. Cyber-attacks won’t escalate to nuclear war – history demonstrates restraint

Erica Lonergan and Shawn Lonergan, 2023 - Erica D. Lonergan is an assistant professor at the Army Cyber Institute at the US Military Academy at West Point and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Shawn W. Lonergan is a US Army Reserve officer assigned to 75th Innovation Command and a senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers. Escalation Dynamics in Cyberspace, google books, p. 6 //DH

Rather than dangerous escalatory spirals that threaten to spill over into kinetic conflict, even the most heated interactions between rivals in cyberspace are characterized by limited, tit-for-tat retaliations that are often separated by significant periods of time and that remain far below any conflict or armed attack threshold. Indeed, in a survey of cyber incidents and responses between 2000 and 2014, Brandon Valeriano et al. find that "rivals tend to respond only to lower-level [cyber] incidents and the response tends to check the intrusion as opposed to seek escalation dominance. The majority of cyber escalation episodes are at a low severity threshold and are nonescalatory."20 Similarly, Sarah Kreps and Jacquelyn Schneider conduct an original experiment to test different logics of cyber escalation and find that cyber attacks "create a threshold that restrains the escalation of conflict."21 Specifically, they find that Americans are less likely to support using kinetic force to respond to a cyber attack, even when the effects of the latter are comparable to other types of kinetic attacks.22

Even the most destructive cyber attack in history, NotPetya, launched by Russia in the spring of 2017 (reportedly using a leaked National Security Agency tool, EternalBlue), did not cause escalation. NotPetya wreaked $10 billion worth of damage across the globe, including to large multinational companies such as Maersk, Merck, and FedEx.23 If cyber operations are likely to cause escalation, NotPetya would be a prime contender, not only because of the extent of the damage inflicted, but also because it was carried out by a longstanding adversary of the nations it affected, which included some of the most powerful states in cyberspace.

Yet, the response on the part of the countries affected by NotPetya was rather restrained. In February 2018—nearly a year after the attack, seven allied nations (the United States, United Kingdom, Denmark, Lithuania, Estonia, Canada, and Australia) issued official statements attributing the NotPetya cyber attack to Russia.24 Concurrent with the coordinated attribution, Rob Joyce, then the White House cybersecurity czar, threatened other ambiguous consequences in remarks delivered at the Munich Security Conference in Germany. Joyce warned that the United States would "work on the international stage to impose consequences. Russia has to understand that they have to behave responsibly on the international stage ... So we're going to see levers the U.S. government can do to impose those costs."25 However, it took nearly a year for allied governments to organize a public, diplomatic attribution effort. The only observable costs that were imposed on Russia were sanctions targeting a limited number of individuals associated with the NotPetya attack as well as with the 2016 U.S. Presidential election interference and cyber penetration of the U.S. power grid.26 Of course, it's possible that there were additional, covert measures taken to impose costs on Russia. But if so, there was no demonstrable effect on any escalation dynamic with Russia.

#### 4. Power grids are resilient – and natural disasters prove there’s no impact

Tom Johansmeyer, 2024 - POLIR Ph.D. candidate at the University of Kent, Canterbury “Why Natural Catastrophes Will Always Be Worse Than Cyber Catastrophes” <https://warontherocks.com/2024/04/why-natural-catastrophes-will-always-be-worse-than-cyber-catastrophes/> //DH

When it comes to disaster, reach is far less important than physical impact. Lewis noted that mass physical damage from cyber events hasn’t been realized, and the contrary is observably true for natural disasters. Reversibility is an important and often overlooked aspect of physical impact, as it defines the longevity of damage. Small-arms damage, for example, is generally reversible, while nuclear attacks are not. Cyber attacks have been demonstrably reversible, given their transitory nature. U.S. institutions and communities have become quite adept at reversing the damage from natural disasters, but their widespread physical impact makes the process much slower and labor-intensive than remediation after cyber attacks. A comparison of two events makes this clear.

In 2015, a cyber attack on the power grid affected 230,000 people in Ukraine. Due to what has often been characterized as an act of cyber war (a questionable use of that expression at best), the lights were out for as long as six hours. This came as part of a wave of cyber attacks on the grid in 2015 and 2016, none of which had any further meaningful impact. The 2015 cyber attack-induced blackout tends to be seen as the “success story” for offensive cyber against power grids, even despite the lack of sustained impact. Natural catastrophes, on the other hand, have had no trouble depriving millions of people of access to electricity for days at a time. One of the most interesting cases for closer study, though, is Hurricane Ida.

Hurricane Ida challenges the belief that natural catastrophes, due to geographical constraint, are limited in their potential impacts. First, the storm was hardly limited by geography. It made landfall in Louisiana and ultimately affected more than a dozen states directly or indirectly before leaving the northeastern United States in its wake. The overall economic loss from the storm exceeded $65 billion, according to Munich Re NatCatSERVICE. Yet, you don’t need to view the storm as a whole to understand the challenges associated with reversibility.

Let’s go back to Louisiana, where 1.1 million people went without power for more than a week. Compared to the 2015 cyber attack in Ukraine, the depth and breadth of the outage is incredible. However, the week-long outage should be seen as brief, given the effort required to bring the lights back. Hurricane Ida “destroyed more than 22,000 power poles, 26,000 spans of wire and 5,261 transformers — that’s more poles damaged or destroyed than hurricanes Katrina, Zeta and Delta combined.” Cyber catastrophes could thus be seen as more geographically constrained than natural catastrophes, when viewed from the perspective of remediation efforts. The need to engage directly with what has been damaged is far more concentrated. The relative speed and ease with which cyber catastrophe damage can be reversed appears to have created an upper limit for economic effect, while the need to go out and fix broken equipment after a natural disaster necessarily takes more time, people, and expense.

#### 5. Cooperation turn - contributory liability undermines cooperation between brands and platforms, which increases counterfeiting

Jonathan Berroya, 2021 - Senior Vice President and General Counsel, Internet Association. Testimony before the Subcommittee On Courts, Intellectual Property, and The Internet Judiciary Committee U.S. House of Representatives. The SHOP SAFE Act: Stemming the Rising Tide of Unsafe Counterfeit Products Online. 5/27, <https://docs.house.gov/meetings/JU/JU03/20210527/112713/HHRG-117-JU03-Wstate-BerroyaJ-20210527.pdf> //DH

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

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

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

### Extend: “Counterfeiting Exaggerated”

#### Affirmative statistics are prior to the passage of the INFORM Act and include non-trademark forms of counterfeiting

Matt Schruers, 2023 - President Computer & Communications Industry Association. Written Statement submitted to the Senate Judiciary Committee, “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” Senate Hearing, 10/3, <https://www.judiciary.senate.gov/imo/media/doc/2023-10-03_-_testimony_-_schruers.pdf> //DH

Fighting counterfeits is a shared mission and we advise Congress to regulate the retail market in its totality, including e-commerce, traditional brick-and-mortar, and small businesses, using a coherent regulatory approach that applies to everyone. However, American small businesses should not be expected to shoulder a disproportionate burden. Instead, the regulatory approach should also be proportional to the scale, and the scale of the problem is far from clear. A popular figure that is frequently invoked ($500 billion) is a four-year-old, worst-case scenario that sweeps in estimated copyright and patent infringement and precedes recent legislation, and is thus not useful for this policy discussion.

II. SHOP SAFE Is Not Needed

a. Give INFORM Time to Work

Like SHOP SAFE, INFORM aimed to reduce the sale of counterfeit, stolen, and dangerous consumer products with updated transparency requirements and verification of third-party sellers online along with contact information for consumers. INFORM was designed to help build more trust online by providing consumers additional transparency about third-party sellers online and because CCIA supports this goal we endorsed INFORM.

This law went into effect only three months ago on June 27, 2023. The recently reintroduced SHOP SAFE contains largely the same provisions that were proposed before INFORM passed. The 117th Congress simultaneously debated both bills and Congress ultimately reached consensus around INFORM, with broad cross-sectoral support from the private sector.

Advocacy for the newly reintroduced SHOP SAFE advances the same pre-INFORM figures, lacking any learnings or conclusions about the impact of INFORM. Rather than relying on outdated numbers, Congress should obtain updated information that takes into account this newly enacted and implemented law before rushing to pass new legislation that could destroy many legitimate small businesses operating online.

The best course of action is to allow INFORM time to work. We need to see and understand its impact in the real world to judge if additional legislative responses or course corrections are required.

#### The INFORM Act is reducing counterfeiting now- it just needs time

Matt Schruers, 2023 - President Computer & Communications Industry Association. Responses to questions from Senator Tillis. “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” Senate Hearing, 10/3, <https://www.judiciary.senate.gov/imo/media/doc/2023-10-03_-_qfr_responses_-_schruers.pdf> //DH

Online marketplaces and sellers have invested significant time and resources to implement the INFORM Consumers Act. It will take time to understand how INFORM impacts both marketplaces and especially small and medium-sized sellers. Lawmakers should give INFORM time to work before pushing legislation that is more burdensome and harmful to online sellers. Because of INFORM, covered “online marketplaces” have placed additional identification, verification, and disclosure requirements on sellers. This will help prevent bad actors from selling through online marketplaces and give stakeholders improved tools against repeat offenders. In addition, INFORM will help boost collaboration between digital services, industry stakeholders across the online ecosystem, and with law enforcement. INFORM will also help protect small business sellers who are running legitimate businesses online by helping to weed out bad actors and give consumers more confidence online.

#### Most counterfeiting occurs in physical marketplaces, not online

Jonathan Berroya, 2021 - Senior Vice President and General Counsel, Internet Association. Testimony before the Subcommittee On Courts, Intellectual Property, and The Internet Judiciary Committee U.S. House of Representatives. The SHOP SAFE Act: Stemming the Rising Tide of Unsafe Counterfeit Products Online. 5/27, <https://docs.house.gov/meetings/JU/JU03/20210527/112713/HHRG-117-JU03-Wstate-BerroyaJ-20210527.pdf> //DH

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

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

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

### Extend: “Status Quo Solves”

#### Online platforms are incorporating new technology to detect counterfeiting now

Krista Chavez, 2024 – Senior Communications Manager at NetChoice “4 Ways Retailers Combat Counterfeiting” 5/9, <https://netchoice.org/4-ways-retailers-combat-counterfeiting> //DH

But retailers are working hard to counter these trends and protect their customers. Here’s four ways how:

Using AI to Spot Fakes

Retail marketplaces are deploying AI algorithms to recognize features like logo placement and trademarks that distinguish genuine products from counterfeit ones. When marketplaces can partner directly with rightsholders to identify key markers, it makes these AI algorithms even more powerful. AI programs also flag sellers who engage in counterfeiting. Some retail platforms use third-party software, like Corsearch, to help them find counterfeit goods. eBay purchased 3PM Shield, a provider of AI marketplace tools, to “enhance its ability to address suspicious or harmful seller behavior, and potentially problematic items.”

In 2023, Amazon identified and removed seven million counterfeit items from the supply chain. And the sneaker resale platform StockX stopped nearly $30 million of fake sneakers from trading on the platform.

At the same time, many luxury retailers like Mulberry and Prada are investing in digital IDs for their products to make identifying counterfeits easier. And LVMH and Cartier, along with others, have created the Aura Blockchain Consortium, which offers a certificate that guarantees the authenticity of luxury products.

Creating Databases of Bad Actors

The U.S. Department of Justice has created a database to track pharmaceutical, electronic and food counterfeiting crimes with open-source information. But retailers are also taking measures into their own hands. Etsy, for example, added a portal to report alleged copyright violations.

Retailers can flag bad actors in the supply chain by avoiding unknown manufacturers who seem overly eager to do business – stick with reputable manufacturers instead. Ship times can also be a red flag; counterfeit products, particularly those involved in drop shipping schemes, typically take much longer to ship than reputable retailers.

Taking Legal Action

Companies also aggressively pursue counterfeit goods manufacturers and sellers. In 2023, Bulgari sued several online stores for selling ‘Bvlgari’ products. The suit says the defendants sell counterfeit merchandise at e-commerce stores that are difficult to distinguish from the company’s official online presence. In 2022, Crocs won a default judgment against a footwear maker accused of selling counterfeit versions of Crocs’ signature plastic clogs.

Amazon’s Counterfeit Crimes Unit (CCU) detects, investigates and removes counterfeit items from the site and identifies bad actors as targets for prosecution all over the world. Since its launch in 2020, the unit has pursued more than 21,000 bad actors through litigation and criminal referrals to law enforcement, according to its 2024 Brand Protection Report.

In addition to the disposal of counterfeit products, in 2023, Amazon collaborated with brands and Chinese law enforcement, which led to more than 50 successful raid actions against manufacturers, suppliers, or upstream distributors of counterfeit products. This collaboration resulted in numerous criminal convictions.

Educating Consumers

Retailers are taking measures to: 1) help consumers identify potential counterfeit goods; and 2) educate consumers on the risks of purchasing counterfeit products. This includes engaging with media outlets, utilizing social media and creating reports, like Etsy’s transparency report.

According to IncoPro, millennials ages 25 to 34 are most at risk for these scams, being much more likely to buy fake goods unknowingly (41%) than those over 55 (18%). But education can help. According to Michigan State University, “the higher consumers’ awareness of the severity of counterfeit risks, the less likely they are to purchase counterfeits.”

For example, Amazon has partnered with the International Trademark Association and not-for-profit career student organization DECA to launch the Unreal Campaign Challenge, a campaign to make consumers better aware of the risks that counterfeit goods pose.

The counterfeit goods trade often supports organized crime, including gangs, drug cartels and terrorist organizations. Profits from counterfeit sales can fund other illegal activities, contributing to societal harm. Another byproduct is environmental: Counterfeit goods often bypass environmental regulations, leading to harmful production practices and waste disposal methods.

Worldwide trade in counterfeit products adds up to more than $500 billion each year. But retailers and online marketplaces are working hard and taking proactive steps to protect consumers and legitimate business services.

### Extend: “Cyber Attacks Won’t Escalate”

#### History disproves escalation

Erica Lonergan and Shawn Lonergan, 2023 - Erica D. Lonergan is an assistant professor at the Army Cyber Institute at the US Military Academy at West Point and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Shawn W. Lonergan is a US Army Reserve officer assigned to 75th Innovation Command and a senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers. Escalation Dynamics in Cyberspace, google books, p. 6-7 //DH

The NotPetya case is just one example. Nevertheless, the overall absence of any meaningful instances of cyber escalation raises questions about the extent to which the cyber domain is truly escalatory, let alone more dangerous than other domains of warfare or strategic competition. In other words, there is a significant mismatch between the cyber escalation views held by many prominent experts and the available evidence. Three factors could account for this gap.

First, differences between theoretical expectations and empirical reality may stem from definitional issues—specifically, how those who assert that the cyber domain is inherently escalatory define what "escalation" means. As we discuss in detail later in this chapter, we conceptualize escalation as something that changes the nature of a strategic interaction between parties in a way that makes war more likely or, if conflict is already taking place, more severe. According to this definition, neither the sheer volume of cyber incidents in the international system nor evidence of any type of response to a cyber incident necessarily constitutes escalation.2, In contrast, some may point to the observation of a high volume of cyber incidents or any form of tit-for-tat dynamic (irrespective of the relative level of cost and risk they may generate) as forms of escalation. However, the mere presence of behavior or activity per se is not sufficient evidence of escalation.

Alternatively, some may acknowledge that cyber escalation has not yet occurred, but it could be lurking around the next corner. This reasoning has some parallels to academic debates about the success of nuclear deterrence during the Cold War. Deterrence optimists opined that the absence of nuclear war between the United States and Soviet Union was due to the success of the strategy, while others have argued that the world simply got lucky.28 However, unlike the Cold War, where neither superpower ultimately chose to unleash its nuclear arsenal on the other, the offensive employment of cyber capabilities is hardly unthinkable. States have developed and employed offensive cyber capabilities since the 1980s and their use is only becoming more prevalent.29 The sheer number of cyber incidents that has occurred over the course of multiple decades raises questions about how likely it is that cyber escalation would take place in the future, given the multi-decade track record of cyber incidents not causing that outcome. That said, as part of our analysis in this book we explore plausible hypothetical escalation scenarios, with a focus on cyber operations that take place during conflict. Finally, there may simply be a mismatch between the conventional wisdom about cyber escalation and the empirical reality because the conventional wisdom is wrong. This is the core contention of our book.

#### Crisis diplomacy and restraint disproves the impact

James Lewis, 2021 – Senior Vice President and Director, Strategic Technologies Program at the Center for Strategic and International Studies, “Toward a More Coercive Cyber Strategy” 3/10, <https://www.csis.org/analysis/toward-more-coercive-cyber-strategy> //DH

The risk of escalation is grossly exaggerated. Countless Track II dialogues are undertaken to reduce the risk of miscalculations that could lead a cyber incident to escalate into kinetic violence. Yet, in two decades of malicious cyber action, there has never been an incident that has led to escalation. While there have been a few instances of unintended consequences and collateral damage, these did not lead to an escalation of conflict. We can now reject the initial hypothesis of miscalculation and escalation as inaccurate. The likely reasons there have been no cyber incidents that resulted in escalation is that states maintain careful control of their most dangerous cyber capabilities and have devoted their own strategies to reduce risk. We should learn from their experience of tight leadership and control as we design our own active policies.

A new strategy must use communications, messaging, and signals with opponents, allies, and publics. This does not mean that every action should be accompanied by a press release, but a new cyber strategy will need to use public and private communications to shape opinion in ways favorable to the United States and make it clear that our actions are guided by international law and agreement. Adopting a more assertive posture in cyberspace is in itself a message that will improve our position with opponents. Diplomatic and public messaging can help manage escalation risk and strengthen collective responses with allies while shaping opponents’ planning. Decisions on timing and audience will be determined by the specifics of each action, but our overall goal should be to end Strangelovian opacity.

#### No one’s ever died from cyber, and even the hypothetical catastrophes are not as bad as a war

Erica D. Lonergan & Shawn W. Lonergan, 2022 - Erica D. Lonergan is an assistant professor at the Army Cyber Institute at the US Military Academy at West Point and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Shawn W. Lonergan is a US Army Reserve officer assigned to 75th Innovation Command and a senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers. “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises,” Security Studies, 31:1, 32-64, DOI: 10.1080/09636412.2022.2040584 //DH

Finally, an essential aspect of cyber operations’ strategic effects is the level of harm to the target. Most malicious cyber activity to date has not risen to a threshold of significant harm, violent effects, or loss of life.44 This is especially the case when compared to other military capabilities.45 That said, there are different ways to operationalize level of harm. One potential metric is loss of life. To date, no one has reportedly died as a direct result of a cyberattack, despite over thirty years of recorded cyber operations. 46 Even in hypothetical catastrophic scenarios, the cost in terms of human casualties is relatively low compared to other military capabilities. For instance, a common worst-case scenario is a cyberattack on a power grid.47 However, the 2015 Russian cyberattack against Ukraine’s power grid, the first known example of an offensive cyber operation targeting a state’s power grid, did not lead to any reported casualties.48

It is also possible to measure the harm cyber operations inflict in treasure rather than blood. According to this metric, the financial or economic costs of cyberattacks are significant. For example, the total cost of the most expensive cyberattack in history, the 2017 NotPetya attack, is estimated at $10 billion.49 However, governments have largely avoided characterizing these operations as crossing an “act of war” or “use of force” threshold.50 While still of strategic consequence, cyber operations (especially absent physical violence) appear to be perceived differently than other military operations.51

Given different approaches, we chose to measure level of harm in terms of the target state’s perception of a cyber operation’s national security consequences. Perception may not perfectly align with the objective human or economic costs. For instance, the SolarWinds supply chain breach, revealed in December 2020, compromised many US federal government and private sector networks but did not cause loss of life.52 Nevertheless, the US government chose to activate the response process outlined in Presidential Policy Directive 41, which applies to cyber incidents that rise to a certain level of significance.53 This example illustrates how the perceived level of harm ultimately is a political or strategic assessment, rather than an objective measure of calculatable damage.

Taken together, the strategic effects of most cyber operations are relatively limited when compared to other types of military operations. That said, different types of cyber operations vary in their level of effects. These two points have implications for accommodative signaling. Specifically, in the context of an international crisis, the relative effects of a cyber operation inform how the adversary perceives the intent behind the signal.54 In this sense, the key audience for a cyber operation’s effects is the adversary government. Because cyber operations lack the physical violence and permanent destruction associated with other military capabilities—and may even be less painful than some economic instruments, such as sanctions— they could signal restraint relative to other options. Moreover, the choice of a disruptive cyber operation that has temporary effects, in comparison to a destructive cyber operation with longer-term effects, could also send an accommodative signal. The sequencing of the cyber operation could also inform its interpretation. For instance, if a cyberattack follows a kinetic one, it could be perceived as a de-escalatory choice.

#### Cyberattacks are minor and manageable

John Mueller, 2022 - Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute “The Cyber-Delusion: Digital Threats Are Manageable, Not Existential” Foreign Affairs, 3/22, <https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion> //DH

This contemporary approach to cyberthreats resembles the aftermath of 9/11, when almost all experts believed an even larger terrorist attack would soon take place. Then, as now, the threat is overblown. Although occasionally dramatic, cyberattacks have turned out to be a comparatively minor and manageable threat. Far too much discussion around the issue focuses on worst-case scenarios, fails to contextualize the problem, and neglects to weigh the costs of cyberattacks against the enormous value of the Internet and artificial intelligence. Most commentary, moreover, does not fully appreciate the ability of the business sector—by far the most tempting of targets for malevolent hackers—to develop effective countermeasures.

CYBERWAR

Over the past decade, the global obsession with digital threats has taken various forms, with a particular focus on the potential military implications of emerging cyber-capabilities. To be sure, the military needs to worry about keeping its communications and command and control operations secure from hostile attackers. Any disruptions, however, are more likely to be instrumental or tactical than strategic.

Despite statements to the contrary, the U.S. military itself seems to have recognized this reality. When Panetta proclaimed in 2013 that cyber was “without question, the battlefield for the future,” political scientist Micah Zenko observed at the time that the Pentagon was spending less than one percent of its budget on cybersecurity, and an assessment from 2019 suggests it may be more like one-tenth of one percent. If those funds prove adequate for the challenge, it would be something of a bargain.

### Extend: “Power Grids Are Resilient”

#### Grids are resilient and disruption is temporary

John Mueller, 2022 - Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute “The Cyber-Delusion: Digital Threats Are Manageable, Not Existential” Foreign Affairs, 3/22, <https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion> //DH

Cyber-alarmists have also warned about hackers disabling major infrastructure such as power grids—potentially crippling entire countries. Grids do go down occasionally, but the culprits are typically squirrels and lightning. Regardless of the source, such disruptions are usually brief and bearable, and engineers are increasingly designing systems that are resilient to such threats. Estonia, for instance, the victim of a major and oft-discussed cyberattack in 2007, is now the home of NATO’s Cooperative Cyber Defence Centre of Excellence.

#### Grid cybersecurity is increasing

Sonal Patel, 2024 – staff writer “The Power Sector’s High-Stakes Battle for Cyber-Resiliency” Power: News & Technology for the Global Energy Industry, <https://www.powermag.com/the-power-sectors-high-stakes-battle-for-cyber-resiliency/> //DH

A Collective Push Toward Resilience

For the power sector, cyber threats remain top-of-mind, but its quest for good cybersecurity posture has evolved into a crucial risk management strategy with several new drivers. For one, significant security risks are associated with the changing resource mix. The grid transformation “is expanding the existing attack surface due to the use of emerging technologies, additional communications, and industrial controls as well as remote control capabilities,” explains the North American Electric Reliability Corp. (NERC), a quasi-governmental compliance enforcement authority.

Modern cybersecurity, which includes several security principles and concepts, typically comprises a defense-in-depth philosophy, but these were not historically integrated into the planning, design, and operation of the grid’s OT systems, NERC notes. As part of their embrace of digitalization, power companies are increasingly connecting the OT environment to outside networks through the incorporation of intelligent devices capable of internet protocol (IP) communications. “These channels provide opportunities for adversaries to exploit latent vulnerabilities within the existing system, as cybersecurity was not part of the design equation for legacy equipment, software, and networks. The introduction of new technologies and new types of entities entering electricity markets also present new cyber-attack vectors,” it added.

In North America, power entities abide by NERC Critical Infrastructure Protection (NERC CIP) standards, which have set requirements for cybersecurity management and control, personnel training, incident reporting, response planning, recovery plans for critical cyber assets, and security controls for grid technology and product suppliers. The European Union, meanwhile, in October 2023, modernized its 2016 Network and Information Directive (NIS). The update broadens the scope of critical entities to recharging point operators and various electricity market participants, and it reinforces cybersecurity requirements along their supply chain.

Power sector cybersecurity posture has also been guided by voluntary cybersecurity frameworks, including from the DOE and the National Institute of Standards and Technology (NIST), and public-private collaborations, such as an effort led by the Electricity Information Sharing and Analysis Center (E-ISAC). One example is the Cybersecurity Risk Information Sharing Program (CRISP), which facilitates the timely bi-directional sharing of unclassified and classified threat information, and development of situational awareness tools. CRISP participants currently provide power to more than 75% of U.S. customers, the DOE said.

However, the power sector’s cybersecurity imperative also largely responds to shareholder concerns about corporate risks posed by cybersecurity. In March 2022, the U.S. enacted the Cyber Incident Reporting for Critical Infrastructure Act, placing a reporting obligation on companies in some critical infrastructure sectors, including energy and nuclear reactors. And in July 2023, the U.S. Securities and Exchange Commission (SEC) finalized a rule that mandates disclosure regarding cybersecurity risk management, strategy, governance, and incident reporting for publicly traded companies. Future rules may hinge on the White House’s March 2023 rollout of a National Cybersecurity Strategy, which envisions “fundamental shifts” in how the U.S. allocates roles, responsibilities, and resources in the cyberspace.

Industry-Led Innovation

“Regulations, if done correctly, are good and required to set a baseline,” noted Patrik Boo, portfolio manager of Cyber Security Services at ABB. “The risk, when regulations are not done well, is that they set a minimum level,” he noted. Industry appears to understand this. Despite pressures, it is today leveraging a legacy in innovation and has embarked on exploring new tools to enhance cybersecurity along with efficiency.

Some companies are looking into integrating artificial intelligence (AI) to enhance and streamline cybersecurity. AI for cybersecurity offerings also appears to be ramping up. Technology firm NVIDIA recently rolled out Morpheus, an open application framework that “enables cybersecurity developers to create optimized AI pipelines for filtering, processing, and classifying large volumes of real-time data,” It essentially brings a “new level of security to the data center, cloud, and edge,” by using AI to “identify, capture, and act on threats and anomalies that were previously impossible to identify.” One attribute, for example, uses digital fingerprinting of the AI workflow to “uniquely fingerprint every user, service, account, and machine across the network—employing unsupervised learning to flag when activity patterns shift.”

Efforts are also progressing to integrate blockchain—best known for securing digital currency payments—with cybersecurity. A project under Oak Ridge National Laboratory’s Darknet initiative had developed a framework to detect unusual activity, including data manipulation, spoofing, and illicit changes to device settings. “Cyber risks have increased with two-way communication between grid power electronics equipment and new edge devices ranging from solar panels to electric car chargers and intelligent home electronics. These activities could trigger cascading power outages as breakers are tripped by protection devices,” ORNL noted. The framework proposes a “totally new capability” to respond to anomalies rapidly,” it said. “In the long run, we could more quickly identify an unauthorized system change, find its source, and provide more trustworthy failure analysis. The goal is to limit the damage caused by a cyberattack or equipment failure.”

The DOE’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is spearheading several notable partnerships with industry, including funding initiatives, aimed at enhancing power sector cybersecurity. A notable program is the Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program at Idaho National Laboratory, which tests critical system components to identify cyber vulnerabilities before they are exploited. The effort is geared to improve the security of ICS and software supply chains.

### Extend: “Cooperation Turn”

#### Cooperation is a prerequisite to solvency. Platforms don’t have access to brand data so they can’t determine whether a mark is counterfeit

Matt Schruers, 2023 - President Computer & Communications Industry Association. Written Statement submitted to the Senate Judiciary Committee, “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” Senate Hearing, 10/3, <https://www.judiciary.senate.gov/imo/media/doc/2023-10-03_-_testimony_-_schruers.pdf> //DH

III. Concerns with SHOP SAFE

CCIA has significant concerns with SHOP SAFE including broad, ambiguous definitions, prescriptive and inflexible requirements to escape automatic liability, and lack of meaningful responsibilities on the brand side, which mean the bill will not successfully accomplish what it seeks to address.

a. Lack of Rightsholder Participation

SHOP SAFE's new regulatory responsibilities place enormous burdens on small businesses, of which the vast majority are operating legitimately. We should not impose an unreasonable compliance burden on small U.S. sellers, particularly if the principal beneficiaries are to be overseas luxury brands that don't care for pro-consumer retail practices in the first place. In order for digital services to effectively protect consumers from unsafe counterfeit goods, brand owners must be required to provide detailed information to digital services about the scope of their trademark rights and licensing. "Counterfeit mark," as defined by statute,8 turns on non-public information about when manufacture occurred and whether it was licensed at the time. With no way of proactively determining whether a seller was licensed to manufacture a particular product at a point in the past, digital services cannot plausibly administer this definition without possessing up-to-date and comprehensive information controlled by brand owners.

Everyone in the retail ecosystem has an important role to play. If there are data gaps that can only be populated with non-public information then this legislation should ensure that brand-owners share this data. Unfortunately SHOP SAFE does not balance burdens between digital commerce sites and brands.

Notably, the revised version also removed the cause of action for "material misrepresentations," aimed at abusive takedown notices provided by brands.9 Unfortunately, this continues to demonstrate the unbalanced nature of SHOP SAFE that places all significant burdens on sellers and not brands who are best positioned to accurately identify and report counterfeit items. The new version appears to attempt to add one new minimal obligation on brands to provide a notice of their mark and point of contact in advance of electronic commerce platforms adopting proactive measures. However, Paragraph 4(B)(iv)(III) removes any obligation of the registrant to participate. Under this language, if information about their marks is publicly available, they don't have to participate, and information about all registered marks is publicly available through the USPTO. In addition, the legislation prevents registrants from being required to participate in any program designed by the electronic commerce platform to crack down on counterfeiting. To truly combat trademark infringement we need significantly more cooperation on the brand side. Small and medium-sized businesses simply do not have the bandwidth and resources to spend multiple days investigating such claims and could be forced out of business for an incorrect challenge from a brand. Unfortunately SHOP SAFE does not contain any small seller exception ensuring that all sellers, no matter how small, will be bound by the terms of the law.

#### Requiring proactive screening creates enormous compliance costs and means platforms will reduce infringement enforcement to solely what the law requires

Matt Schruers, 2023 - President Computer & Communications Industry Association. Written Statement submitted to the Senate Judiciary Committee, “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” Senate Hearing, 10/3, <https://www.judiciary.senate.gov/imo/media/doc/2023-10-03_-_testimony_-_schruers.pdf> //DH

b. Compliance Burdens

SHOP SAFE is very prescriptive and inflexible, with numerous mandates to escape automatic liability ("shall be contributorily liable") — a drastic change to existing U.S. trademark law. These requirements include "proactive measures for screening listings", a three-strikes repeat infringer policy, and to "expeditiously disable or remove from the platform any listing for which the platform has actual or constructive knowledge of the use of a counterfeit mark."

1. Requiring proactive screening measures before listings go live would take an untold amount of technological and human resources, both for smaller firms and larger services operating at scale. Under existing intellectual property law, there is no obligation on the part of online service providers to proactively monitor users for potential infringements. Rather, this is a matter of discretion and policy for each service, and should remain that way because, as discussed above, sellers are not in a good position to identify potentially infringing activity. Specifically, Paragraph 4(B)(iv)(I) should be clarified to better understand the burdens on registrants and online service providers. For example, the legislation is ambiguous as to whether online services are expected to provide screening capabilities to the registrants, and whether these provisions apply to the seller's own goods, or goods being transacted under the first-sale doctrine. Under this regime, existing digital services would likely be disincentivized from developing new and innovative brand protection strategies, instead conforming solely to what the law required. This would benefit neither consumers nor brands. In addition, the monitoring contemplated under these provisions unnecessarily undermines user privacy.

#### The status quo is the best option – platforms work cooperatively with brands now to proactively enforce

Jonathan Berroya, 2021 - Senior Vice President and General Counsel, Internet Association. Testimony before the Subcommittee On Courts, Intellectual Property, and The Internet Judiciary Committee U.S. House of Representatives. The SHOP SAFE Act: Stemming the Rising Tide of Unsafe Counterfeit Products Online. 5/27, <https://docs.house.gov/meetings/JU/JU03/20210527/112713/HHRG-117-JU03-Wstate-BerroyaJ-20210527.pdf> //DH

Anyone who has enforced IP rights can tell you that identifying counterfeit goods can be difficult - if not impossible unless you have a high level of expertise and familiarity with the brand and products that are being counterfeited. Trademark owners often hire employees and consultants who are solely focused on expertly identifying the subtle differences between genuine products and counterfeits in support of their enforcement efforts. These individuals work with a host of federal, state, and local agencies, including the U.S. Department of Justice (“DOJ”), U.S. Customs and Border Protection (“CBP”), and state and local police departments, as well as district attorneys’ offices that have staff dedicated to enforcing criminal anti-counterfeiting laws.21

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

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

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

## Money Laundering Advantage Answers

### 1NC – Money Laundering Advantage Answers

#### 1. Anti-money laundering fails – terrorists and kleptocrats circumvent restrictions

Elisabeth Krecké, 2024 – independent, Luxembourg-based economist, as well as a former policy advisor and university professor “Why anti-money laundering policies are failing” GIS Reports, 2/15, <https://www.gisreportsonline.com/r/why-anti-money-laundering-policies-are-failing/> //DH

**KYC = Know Your Customer regulations, AML = Anti-money laundering**

When it comes to the benefits, it is worth asking tough questions. For instance, do KYC and anti-money laundering regulations adequately protect consumers, investors and the overall financial system from financial crime? How much do they deter would-be criminals? How much of the illicit flows are recovered thanks to such checks?

A 2018 study by American political scientist Ronald Pol suggested that the overall impact of AML policy intervention on criminal finances is less than 0.1 percent – that is, absolutely negligible.

Mr. Pol’s findings are in line with those of a 2011 research report by the UNODC, according to which “much less than one percent (probably around 0.2 percent)” of the proceeds of crime laundered via the global financial system are seized and frozen.

A 2023 Europol report confirmed what one could have suspected: terrorists, criminals and fraudsters always find ways to circumvent even the most complicated regulatory processes. Among others, they exploit cutting-edge technologies much faster than authorities can keep up.

If criminal enterprises are keeping 99.8 percent or more of their dirty money, it is hard to call the current regulatory systems efficient. Mr. Pol acknowledged that his data and methodology could be subject to criticism. Money laundering is a secretive activity, so accurate information on illicit flows is difficult to obtain and estimations cannot be definitive.

Nevertheless, the gap between policy intent and results is huge. A similar critique also came from Christopher Giancarlo, former chairman of the United States Commodity Futures Trading Commission (CFTC).

#### 2. Alternate causality – shell companies in the US make circumvention inevitable

Casey Michel, 2024 – journalist. “How the US Became the World’s Refuge for Dirty Money” Mother Jones, Jan-Feb, <https://www.motherjones.com/politics/2024/01/dirty-money-united-states-bahamas-sioux-falls-financial-crimes/> //DH

It was the first time that FinCEN—ever, in its 30-year history—had busted a trust company for violating money-­laundering­ prevention laws. And its investigation spotlighted not just the lapses of Kingdom Trust but an entire system that helps kleptocrats (who have looted their countries for private gain) and wealthy Westerners alike anonymously route their money through the US economy. It’s a system that’s evolved over decades—a race to the bottom led by states desperate to ensure a steady flow of revenue. It involves a sprawling network of trust companies, law firms, and real estate agencies that facilitate the transfer of suspect money. And it’s made the United States one of the world capitals of kleptocratic cash.

Today, there’s no need to stash your money in the Bahamas, Malta, or the Caymans when you can keep it in places like Sioux Falls, South Dakota. Thanks to favorable laws that make it an ideal refuge for the world’s wealth, America now sits at the center of the global offshore economy—an international pot of riches even larger than the GDP of China, by some estimates.

Journalistic investigations like the Panama Papers and Pandora Papers have helped expose the scourge of shell companies that are the linchpins of these offshore networks. Such corporate formations—which provide anonymity to the people behind them and are largely impenetrable to authorities trying to track the money—are not unique to the United States. Other Western democracies, including the United Kingdom, have also allowed them to flourish. But the US has gone far beyond most other countries in the level of secrecy that it provides, and it has done so at a far greater clip than any of its peers.

#### 3. No nuclear terrorism – too many barriers

John Mueller & Mark G. Stewart, 2021 - \*Mershon Center for International Security Studies, Department of Political Science, Ohio State University and \*\*Centre for Infrastructure Performance and Reliability, The University of Newcastle “Terrorism and Bathtubs: Comparing and Assessing the Risks,” Terrorism and Political Violence, 33:1, 138-163, DOI: 10.1080/09546553.2018.1530662, online at Taylor & Francis, Accessed via University of Michigan //DH

Thus far, 9/11 stands out as an extreme outlier: scarcely any terrorist act, before or after, in war zones or outside them, has inflicted even one-tenth as much total destruction. That is, contrary to common expectations, the attack has thus far been an aberration, not a harbinger.8 And al-Qaeda central, the group responsible for the attack, has, in some respects at least, proved to resemble President John Kennedy's assassin, Lee Harvey Oswald—an entity of almost trivial proportions that got horribly lucky once. The tiny group of perhaps 100 or so does appear to have served as something of an inspiration to some Muslim extremists. They may have done some training, may have contributed a bit to the Taliban's far larger insurgency in Afghanistan, and may have participated in a few terrorist acts in Pakistan. In his examination of the major terrorist plots against the West since 9/11, Mitchell Silber finds only two—the shoe bomber attempt of 2001 and the effort to blow up transat- lantic airliners with liquid bombs in 2006—that could be said to be under the "command and control" of al-Qaeda central (as opposed to ones suggested, endorsed, or inspired by the organization), and there are questions about how full its control was even in these two instances, both of which, as it happens, failed miserably.9 And, although some al-Qaeda affiliates have committed substantial damage in the Middle East, usually in the context of civil wars, their efforts to carry out terrorism in the West have been rare and completely ineffective.10 Even under siege, it is difficult to see why al-Qaeda could not have carried out attacks at least as costly and shocking as the shooting rampages (organized by other groups) that took place in Mumbai in 2008 or at a shopping center in Kenya in 2013. Neither took huge resources, presented major logistical challenges, required the organization of a large number of perpetrators, or needed extensive planning.

However, there is of course no guarantee that things will remain that way, and the 9/11 attacks inspired the remarkable extrapolation that, because the terrorists were successful with box cutters, they might soon be able to turn out weapons of mass destruction— particularly nuclear ones—and then detonate them in an American city. For example, in his influential 2004 book, Nuclear Terrorism, Harvard's Graham Allison relayed his "considered judgment" that "on the current path, a nuclear terrorist attack on America in the decade ahead is more likely than not."11 Allison has had a great deal of company in his alarming pronouncements. In 2007, the distinguished physicist Richard Garwin put the likelihood of a nuclear explosion on an American or European city by terrorist or other means at 20 percent per year, which would work out to 91 percent over the eleven- year period to 2018.12

Allison's time is up, and so is Garwin's. These oft-repeated warnings have proven to be empty. And it is important to point out that not only have terrorists failed to go nuclear, but as William Langewiesche, who has assessed the process in detail, put it in 2007, "The best information is that no one has gotten anywhere near this. I mean, if you look carefully and practically at this process, you see that it is an enormous undertaking full of risks for the would-be terrorists."13 That process requires trusting corrupted foreign collaborators and other criminals, obtaining and transporting highly guarded material, setting up a machine shop staffed with top scientists and technicians, and rolling the heavy, cumbersome, and untested finished product into position to be detonated by a skilled crew, all the while attracting no attention from outsiders.

Nor have terrorist groups been able to steal existing nuclear weapons—characteristically burdened with multiple safety devices and often stored in pieces at separate secure locales—from existing arsenals as was once much feared. And they certainly have not been able to cajole leaders in nuclear states to palm one off to them—though a war inflicting more death than Hiroshima and Nagasaki combined was launched against Iraq in 2003 in major part under the spell of fantasies about such a handover.1'1

More generally, the actual terrorist "adversaries" in the West scarcely deserve accolades for either dedication or prowess. It is true, of course, that sometimes even incompetents can get lucky, but such instances, however tragic, are rare. For the most part, terrorists in the United States are a confused, inadequate, incompetent, blundering, and gullible bunch, only occasionally able to get their act together. Most seem to be far better at frenetic and often self-deluded scheming than at actual execution. A summary assessment by RAND's Brian Jenkins is apt: "their numbers remain small, their determination limp, and their competence poor."13 And much the same holds for Europe and the rest of the developed world.16 Also working against terrorist success in the West is the fact that almost all are amateurs: they have never before tried to do something like this. Unlike criminals they have not been able to develop street smarts.

#### 4. Safe harbors fail – costs and litigation are onerous, blocking harmonization

Eric Goldman, 2021 – professor of law at Santa Clara Law. “The SHOP SAFE Act Is a Terrible Bill That Will Eliminate Online Marketplaces” Technology and Marketing Law Blog, 9/28, https://blog.ericgoldman.org/archives/2021/09/the-shop-safe-act-is-a-terrible-bill-that-will-eliminate-online-marketplaces.htm //DH

Overturning Tiffany v. eBay

In 2010, the Second Circuit issued a watershed decision about secondary trademark infringement. Essentially, the court held that eBay wasn’t liable for counterfeit sales of Tiffany items because eBay honored takedown notices and Tiffany’s claims sought to hold eBay accountable for generalized knowledge. That ruling has produced a kind of détente in the online secondary trademark infringement field, where we just don’t see broad counterfeiting lawsuits against online marketplaces any more.

The SHOP SAFE Act ends that détente. First, it creates a new statutory contributory trademark infringement claim for selling the regulated items. Second, the bill says that the new contributory claim doesn’t preempt other plaintiff claims, so trademark owners will still bring the standard statutory direct trademark infringement claim and common law contributory trademark claims (and dilution, false designation of origin, etc.). Third, online marketplaces nominally can try to “earn” a safe harbor from the new statutory contributory liability claim (but not from the other legal claims) by jumping through an onerous gauntlet of responsibilities. Those requirements will impose huge compliance costs, but those investments won’t prevent online marketplaces from being dragged into extraordinarily expensive and high-stakes litigation over eligibility for this defense. Fourth, the law imposes a proactive screening obligation, something that Tiffany v. eBay rejected. Fifth, unlike Tiffany v. eBay, generalized knowledge can create liability; and takedown notices aren’t required as a prerequisite to liability. Sixth, in litigation over direct trademark infringement and common law contributory trademark infringement claims, trademark owners can cite compliance/non-compliance with the defense factors against the online marketplace, putting the online marketplace in a worse legal position than they currently are in.

All told, the SHOP SAFE Act will functionally repeal the Tiffany v. eBay standard that has fostered the growth of online marketplaces for the last decade-plus, and usher in a new era of online shopping that will likely exclude online marketplaces entirely.

### Extend: “Anti-Money Laundering Fails”

#### Even the former head of the Financial Action Task Force admits AML efforts fail

Elisabeth Krecké, 2024 – independent, Luxembourg-based economist, as well as a former policy advisor and university professor “Why anti-money laundering policies are failing” GIS Reports, 2/15, <https://www.gisreportsonline.com/r/why-anti-money-laundering-policies-are-failing/> //DH

**AML = Anti Money Laundering**

Unexpectedly, another top financial regulator recently came to share Mr. Pol’s opinion that AML, in its present form, is “the world’s least effective policy experiment.” During a 2020 interview, David Lewis – the former executive secretary of the Financial Action Task Force (FATF), the most powerful global AML watchdog – said that despite efforts made by countries under FATF surveillance, “everyone is doing badly.” Seemingly, AML/CFT measures are often poorly implemented on a national level. Mr. Lewis lamented that some nations only want to avoid bad reports that put them on FATF’s list of low-scoring countries.

#### Organized crime adapts to AML changes faster than enforcement can keep up

Eve Sampson, 2023 – ICIJ's 2023 editorial fellow as part of the Scripps Howard Foundation’s Roy W. Howard Fellowship program. “Money-laundering criminals are adapting to new technology faster than authorities can keep up, EU report says” International Consortium of Investigative Journalists, 9/26, <https://www.icij.org/investigations/fincen-files/money-laundering-criminals-are-adapting-to-new-technology-faster-than-authorities-can-keep-up-eu-report-says/> //DH

Criminal networks in Europe are increasingly mixing illicit finances with seemingly legal businesses, and exploiting new technology to grow their operations and launder money faster than authorities can keep up, a new Europol report revealed.

Nearly 70% of criminal elements operating in the European Union use money-laundering techniques to garner revenue and hide assets, degrading the region’s financial stability and impeding its economic growth, according to the European Financial and Economic Crime Threat Assessment report released last week by the EU’s law enforcement arm, Europol. The increasing speed of deception is outpacing authorities which are struggling to uncover and prosecute financial crimes.

Though trade and technology have connected a globalized world, criminals are increasingly using modern advances to profit, Catherine De Bolle, the executive director of Europol, wrote in the report.

“Organised crime has built a parallel global criminal economic and financial system around money laundering, illicit financial transfers and corruption,” De Bolle said. “The ability to launder illicit proceeds on an industrial scale, to move them through a web of criminal financial brokers, and to corrupt the relevant actors, has become indispensable for modern organised crime.”

As services went virtual during the COVID-19 pandemic, digital banking has helped open new doors for criminal networks looking for a toehold in the financial system. Online banks, with no physical branches or offices, now offer nearly anonymous international deposits at lightning speed, making nefarious activity difficult to detect.

The Europol report cited ICIJ’s 2021 Pandora Papers investigation as an example of how criminal enterprises have found ways to hide beneficial ownership and evade sanctions through the use of intermediaries and offshore firms. The report also highlighted the criminal use of third countries to move money connected to Russia in defiance of Western sanctions levied against the country following the 2014 invasion of Ukraine.

### Extend: “Alternate Causality – Shell Companies”

#### US real estate is exempt from AML enforcement – which means it has become a safe haven for kleptocrats

Casey Michel, 2024 – journalist. “How the US Became the World’s Refuge for Dirty Money” Mother Jones, Jan-Feb, <https://www.motherjones.com/politics/2024/01/dirty-money-united-states-bahamas-sioux-falls-financial-crimes/> //DH

Tracing how US real estate became the asset of choice for sanctioned Russian tycoons, African autocrats, drug lords, and uberrich Americans requires going back to the darkest days of the early 21st century. The PATRIOT Act—passed in the aftermath of 9/11, when fears about money being spirited to terrorist cells were white-hot—contained a suite of policies to prevent suspect funds from entering the United States. American banks were required to scrutinize transactions and flag suspicious activity.

The law’s money-laundering provisions were intended to go much further, forcing other industries—particularly real estate—to shore up their dirty money defenses. But shortly after the law’s passage, the Treasury Department announced a temporary exemption for real estate deals. Bush administration officials declared that they wanted to further study the law to make sure it wouldn’t inadvertently hamstring the industry. Months passed, then years, then decades. Today, this exemption remains firmly in place, and American real estate agents and firms are still under no legal ­obligation to check the sources of their clients’ wealth or report even the most obvious red flags. Not surprisingly, the world’s elites have taken full advantage.

Pick a case of international kleptocracy, and you are likely to discover a link to US properties. Millions connected to ­Malaysia’s sprawling IMDB scandal, all looted from the country’s sovereign wealth fund, were plowed into hotels in New York and Beverly Hills. (Plundered funds, fittingly, were also allegedly used to finance the film The Wolf of Wall Street.) In 2014, the New York Times reported, the daughter of a former longtime ruler of the Republic of Congo bought an apartment at the Trump International Hotel and Tower in Manhattan. (There’s no indication Trump broke the law, but this was one of many intersections between kleptocratic regimes and his real estate empire.) Another example: The world’s second-longest-­standing dictator, Equatorial Guinea’s Teodoro Obiang Nguema Mbasogo, owns a massive home in Maryland, where for years he was neighbors with former Gambian despot Yahya Jammeh.

#### Financial secrecy makes the impact inevitable

Charles G. Davidson and Ben Judah, 2023 – \*publisher of The American Interest and a former Freedom House board member. From 2014 to 2018, he was executive director of the Hudson Institute’s Kleptocracy Initiative, and \*\*senior fellow at the Atlantic Council “How Financial Secrecy Undermines Democracy” Journal of Democracy, October, <https://www.journalofdemocracy.org/articles/how-financial-secrecy-undermines-democracy/> //DH

Beneath the surface of our financial system lies an unseen world worth trillions of dollars. This vast and expansive realm, both offshore and onshore, is undermining capitalism and democracy from the inside. Raymond Baker calls it the financial-secrecy system, and among today’s grave threats to democracy it is one of the least acknowledged.1 Made up of millions of hidden accounts, secret trusts, disguised entities, artificial trades, opaque ownerships, and more, this parallel world could not differ more starkly from what the average citizen of a Western democracy experiences as the financial system. Rather than being a space under intense scrutiny and observation, monitored by everything from the latest banking algorithms to the beady eyes of tax officials, this hidden dimension is where those wealthy enough to gain access to it go to hide their wealth and avoid taxes. Rather than serving as an asset to Western capitalism and democracy, this secret world and its covert dealings are acting on both as a quiet poison.

Or perhaps the poison is no longer so quiet: This parallel world has now grown so large that it is visibly cracking the political order from which it sprang. Financial secrecy has swollen in recent years as elites have abandoned their duty to pay their fair share. A metastasizing culture of tax avoidance by corporations and the wealthy has weakened national values, institutions, and goals across the West while fueling levels of inequality that wreck national cohesion, drive spiraling resentment, and stoke anger. This is empowering the enemies of democracy at home and abroad, be they domestic populists who vow to crush the abusive system, or authoritarian kleptocrats and criminals who manipulate the system to cover their own misdeeds.

#### The scale of American financial secrecy has created a money laundering golden age

Charles G. Davidson and Ben Judah, 2023 – \*publisher of The American Interest and a former Freedom House board member. From 2014 to 2018, he was executive director of the Hudson Institute’s Kleptocracy Initiative, and \*\*senior fellow at the Atlantic Council “How Financial Secrecy Undermines Democracy” Journal of Democracy, October, <https://www.journalofdemocracy.org/articles/how-financial-secrecy-undermines-democracy/> //DH

Accepting secrecy’s “enablers” and the full spate of its instruments is also undermining the West’s ability to compete with authoritarian powers and protect Western political institutions.17 Kleptocrats in Russia or China can move money anonymously into the West, buying assets and building networks that facilitate political interference and compromise Western nations’ security and democratic institutions. The sheer scale of global financial secrecy, moreover, has made possible a golden age of money laundering that aids kleptocrats in converting stolen wealth into new sources of power. These can include corrupted Western officials, private armies of mercenaries, and phalanxes of enablers recruited from Western professional ranks.18

### Extend: “No Nuclear Terrorism”

#### Terrorism risk is very low

Daniel Silverman et al, 2022 – Institute for Politics and Strategy, Carnegie Mellon University“Putting Terror in Its Place: An Experiment on Mitigating Fears of Terrorism among the American Public” Journal of Conflict Resolution 2022, Vol. 66(2) 191 –216, <https://journals.sagepub.com/doi/pdf/10.1177/00220027211036935> //DH

The American public’s fear of terrorism persists in spite of the fact that the actual risk of terrorism for those in the United States is extremely low. Over the past half-century, the chance that an American would be killed by a terror attack on U.S. soil is roughly 1 in 3.5 million, with under ninety deaths per year between 1970 and 2007. Even in 2001, a year when terrorism was uniquely dangerous in the United States, terrorism accounted for less than 0.14 percent of deaths in the country. In contrast, the risk of death from other hazards like cancer (1 in 540), car accidents (1 in 8,000), drowning in a bathtub (1 in 950,000), and flying on a plane (1 in 2.9 million) are all greater than terrorism (Mueller 2006).

#### Too many obstacles exist to getting a nuke

John Mueller, 2020 – emeritus professor of political science at Ohio State “Nuclear Alarmism: Proliferation and Terrorism” 6/24, <https://www.cato.org/publications/nuclear-alarmism-proliferation-terrorism> //DH

However, thus far, terrorist groups seem to have exhibited only limited desire and even less progress in going atomic. That lack of action may be because, after a brief exploration of the possible routes, they — unlike generations of alarmists — have discovered that the tremendous effort required is scarcely likely to be successful.34

Obtaining a Finished Bomb: Assistance by a State

One route a would‐​be atomic terrorist might take would be to receive or buy a bomb from a generous like‐​minded nuclear state for delivery abroad. That route is highly improbable, however, because there would be too much risk — even for a country led by extremists — that the ultimate source of the weapon would be discovered. As one prominent analyst, Matthew Bunn, puts it, “A dictator or oligarch bent on maintaining power is highly unlikely to take the immense risk of transferring such a devastating capability to terrorists they cannot control, given the ever‐​present possibility that the material would be traced back to its origin.” Important in this last consideration are deterrent safeguards afforded by “nuclear forensics,” which is the rapidly developing science (and art) of connecting nuclear materials to their sources even after a bomb has been exploded.35

Moreover, there is a very considerable danger to the donor that the bomb (and its source) would be discovered before delivery or that it would be exploded in a manner and on a target the donor would not approve of — including on the donor itself. Another concern would be that the terrorist group might be infiltrated by foreign intelligence.36

In addition, almost no one would trust al Qaeda. As one observer has pointed out, the terrorist group’s explicit enemies list includes not only Christians and Jews but also all Middle Eastern regimes; Muslims who don’t share its views; most Western countries; the governments of Afghanistan, India, Pakistan, and Russia; most news organizations; the United Nations; and international nongovernmental organizations.37 Most of the time, it didn’t get along all that well even with its host in Afghanistan, the Taliban government.38

Stealing or Illicitly Purchasing a Bomb: Loose Nukes

There has also been great worry about “loose nukes,” especially in postcommunist Russia — weapons, “suitcase bombs” in particular, that can be stolen or bought illicitly. A careful assessment conducted by the Center for Nonproliferation Studies has concluded that it is unlikely that any of those devices have been lost and that, regardless, their effectiveness would be very low or even nonexistent because they (like all nuclear weapons) require continual maintenance.39 Even some of those people most alarmed by the prospect of atomic terrorism have concluded, “It is probably true that there are no ‘loose nukes,’ transportable nuclear weapons missing from their proper storage locations and available for purchase in some way.“40

It might be added that Russia has an intense interest in controlling any weapons on its territory because it is likely to be a prime target of any illicit use by terrorist groups, particularly Chechen ones of course, with whom it has been waging a vicious on‐​and‐​off war for two decades. The government of Pakistan, which has been repeatedly threatened by terrorists, has a similar interest in controlling its nuclear weapons and material — and scientists. As noted by Stephen Younger, former head of nuclear weapons research and development at Los Alamos National Laboratory, “Regardless of what is reported in the news, all nuclear nations take the security of their weapons very seriously.“41 Even if a finished bomb were somehow lifted somewhere, the loss would soon be noted and a worldwide pursuit launched.

Moreover, finished bombs are outfitted with devices designed to trigger a nonnuclear explosion that would destroy the bomb if it were tampered with. And there are other security techniques: bombs can be kept disassembled with the components stored in separate high‐​security vaults, and security can be organized so that two people and multiple codes are required not only to use the bomb but also to store, maintain, and deploy it. If the terrorists seek to enlist (or force) the services of someone who already knows how to set off the bomb, they would find, as Younger stresses, that “only few people in the world have the knowledge to cause an unauthorized detonation of a nuclear weapon.” Weapons designers know how a weapon works, he explains, but not the multiple types of signals necessary to set it off, and maintenance personnel are trained in only a limited set of functions.42

There could be dangers in the chaos that would emerge if a nuclear state were to fail, collapsing in full disarray — Pakistan is frequently brought up in this context and sometimes North Korea as well. However, even under those conditions, nuclear weapons would likely remain under heavy guard by people who know that a purloined bomb would most likely end up going off in their own territory; would still have locks (and in the case of Pakistan would be disassembled); and could probably be followed, located, and hunted down by an alarmed international community. The worst‐​case scenario in that instance requires not only a failed state but also a considerable series of additional permissive conditions, including consistent (and perfect) insider complicity and a sequence of hasty, opportunistic decisions or developments that click flawlessly in a manner far more familiar to Hollywood scriptwriters than to people experienced with reality.43

Building a Bomb of One’s Own

Because they are unlikely to be able to buy or steal a usable bomb and because they are further unlikely to have one handed off to them by an established nuclear state, the most plausible route for terrorists would be to manufacture the device themselves from purloined materials. That is the course identified by a majority of leading experts as the one most likely to lead to nuclear terrorism.44

The simplest design is a “gun” type of device in which masses of highly enriched uranium are hurled at each other within a tube. Such a device would be, as Allison acknowledges, “large, cumbersome, unsafe, unreliable, unpredictable, and inefficient.“45

The process of making such a weapon is daunting even in this minimal case. In particular, the task requires that a considerable series of difficult hurdles be conquered and in sequence.

To begin with, now and likely for the foreseeable future, stateless groups are incapable of manufacturing the requisite weapons‐​grade uranium themselves because the process requires an effort on an industrial scale. Moreover, they are unlikely to be supplied with the material by a state for the same reasons a state is unlikely to give them a workable bomb.46 Thus, they would need to steal or illicitly purchase the crucial material.

A successful armed theft is exceedingly unlikely, not only because of the resistance of guards but also because chase would be immediate. A more plausible route would be to corrupt insiders to smuggle out the necessary fissile material. However, that approach requires the terrorists to pay off a host of greedy confederates, including brokers and money transmitters, any one of whom could turn on them or — either out of guile or incompetence — furnish them with stuff that is useless.47 Moreover, because of improved safeguards and accounting practices, it is decreasingly likely that the theft would remain undetected.48 That development is important because if any missing uranium is noticed, the authorities would investigate the few people who might have been able to assist the thieves, and one who seems suddenly to have become prosperous is likely to arrest their attention right from the start. Even one initially tempted by, seduced by, or sympathetic to, the blandishments of the smooth‐​talking foreign terrorists might soon develop sobering second thoughts and go to the authorities. Insiders tempted to assist terrorists might also come to ruminate over the fact that, once the heist was accomplished, the terrorists would, as analyst Brian Jenkins puts it none too delicately, “have every incentive to cover their trail, beginning with eliminating their confederates.“49

It is also relevant to note that over the years, known thefts of highly enriched uranium have totaled fewer than 16 pounds. That amount is far less than that required for an atomic explosion: for a crude bomb, more than 100 pounds are necessary to produce a likely yield of one kiloton. Moreover, none of those thieves was connected to al Qaeda, and, most arrestingly, none had buyers lined up — nearly all were caught while trying to peddle their wares. Indeed, concludes analyst Robin Frost, “There appears to be no true demand, except where the buyers were government agents running a sting.” Because there appears to be no commercial market for fissile material, each sale would be a one‐​time affair, not a continuing source of profit such as drugs, and there is no evidence of established underworld commercial trade in this illicit commodity.50

If terrorists were somehow successful in obtaining a sufficient mass of relevant material, they would then have to transport it out of the country over unfamiliar terrain, probably while being pursued by security forces. Then, they would need to set up a large and well‐​equipped machine shop to manufacture a bomb and populate it with a select team of highly skilled scientists, technicians, and machinists. The process would also require good managers and organizers. The group would have to be assembled and retained for the monumental task without generating consequential suspicions among friends, family, and police about their curious and sudden absence from normal pursuits back home. Pakistan, for example, maintains a strict watch on many of its nuclear scientists even after retirement.51

Some observers have insisted that it would be “easy” for terrorists to assemble a crude bomb if they could get enough fissile material.52 However, Christoph Wirz and Emmanuel Egger, two senior physicists in charge of nuclear issues at Switzerland’s Spiez Laboratory, conclude that the task “could hardly be accomplished by a subnational group.” They point out that precise blueprints are required, not just sketches and general ideas, and that even with a good blueprint, the terrorist group “would most certainly be forced to redesign.” They also stress that the work, far from being “easy,” is difficult, dangerous, and extremely exacting and that the technical requirements “in several fields verge on the unfeasible.“53

### Extend: “Safe Harbors Fail”

#### SHOP SAFE’s ambiguous on requirements to meet a safe harbor – that prevents it from functioning

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

The SHOP SAFE Act had a laudable goal (to reduce or eradicate the use of counterfeit marks in connection with the sale and distribution of goods that implicate health and safety on e-commerce platforms), but the Act simply went too far. Rather than addressing the real question-the level of knowledge required for any third party accused of contributory infringement-SHOP SAFE was limited to e-commerce platforms, and it attempted to impose on the platform the burden of demonstrating that it took twelve separate steps to verify the identity of the listing party and the authenticity of marks used in connection with the sale of goods, in order to avoid liability. The processes to be implemented were not gauged to any perceived risk that the items offered for sale might be counterfeit or could potentially cause a level of harm to purchasers or end users. Further, many of the terms in the act were ill-defined, and there was much ambiguity about precisely what was required from the ecommerce platforms in order for them to avoid contributory liability. For example, the proposed act required "reasonable proactive technological measures for screening goods before displaying the goods to the public" in order to prevent use of a counterfeit mark,416 but it was unclear whether this was intended to require screening of the actual goods themselves, images depicting the goods, descriptions of the goods, or something else entirely. "Reasonable technological measures for screening third-party sellers" were also required, in order to ensure that terminated sellers do not later rejoin the platform under an alias,417 but again no further details were provided.

# Circular Economy Disadvantage

### 1NC – Circular Economy DA

#### The next offcase position is the circular economy da

#### Online platform innovation is driving a transition to a circular economy through secondary markets. Circularity will double by 2030

Brian Eastwood, 2023 – freelance writer, quotes Peter Evans, PhD and chief strategy officer at McFadyen Digital. “Platforms could power the circular economy” MIT Sloan School of Management blog, 9/11, <https://mitsloan.mit.edu/ideas-made-to-matter/platforms-could-power-circular-economy> //DH

If there’s one constant in the platform economy, it’s change. Platforms started out fueling the matchmaking economy (eBay) and have evolved to further encompass the sharing economy (Airbnb) and the gig economy (Upwork).

The next phase: platforms supporting the circular economy, which reuses raw materials and products by connecting consumers to enterprises and to each other to reuse, repair, refine, or recycle goods.

“When it comes to the future of platforms, one of the big forces at work is growing concern about sustainability and climate change. The heat waves, the fires, and all sorts of other phenomena happening in the world are increasing anxiety,” said Peter Evans, PhD ’05, the chief strategy officer at McFadyen Digital. “There’s an opportunity for platforms to be incredible engines for driving a circular economy, not just the linear economy.”

Speaking at the 2023 MIT Platform Strategy Summit, Evans offered a look at why platforms are a good fit for the circular economy and the questions that remain about circular platform adoption.

A new use for goods, thanks to a wider reach

In a linear economy, goods move in one direction, from raw material to production, use, and then waste. Making new goods requires finding and using new and increasingly scarce resources. Meanwhile, products that are “used” but still have value often end up in landfills, waterways, or the atmosphere.

A circular economy, however, keeps raw materials and products “in circulation for as long as possible,” in the words of the U.S. Environmental Protection Agency. It’s a matter of reusing materials, redesigning products, and recapturing waste — scrapping a car for its parts rather than sending it to the dump, for example.

Platforms have excelled in the linear economy, Evans said. But while they’ve disrupted innumerable markets by reducing the friction of matching buyers and sellers, they haven’t disrupted underlying economic models. “It’s actually making the existing system more efficient,” he said. “It’s reinforcing the linear model and not changing it very much.”

But platforms could adapt well to the circular economy, Evans added, and provide benefits such as lower transaction costs, more buyers and sellers, and positive network effects.

One key outcome would be expanding the reach of materials beyond the industry in which they originated. Batteries in electric vehicles, for example, can have a second life in the energy sector once the car itself is out of commission.

“What do consumers of vehicles know about the power sector? Not very much. The platform could set up new matching markets,” Evans said. “If you keep in your own industry, you’re not going to take advantage of where the highest use value is.”

Current success, future uncertainty

McFadyen Digital estimates that today’s circular economy has a global value of nearly $410 billion, with platforms accounting for roughly a quarter of that. By 2030, the circular economy should be worth $1.5 trillion — and circular platforms will account for nearly 60% of that, or $863 billion.

Success stories abound. ThredUp, which connects buyers and sellers of secondhand apparel, went public in 2021 at a $1.3 billion valuation. Paris-based Back Market, an online marketplace for refurbished electronics, reached a valuation of $5.7 billion in 2022 after raising $510 million in a Series E funding round. Alibaba subsidiary Idle Fish has 500 million registered users in China and hosts transactions for secondhand goods worth $70 billion annually, Evans said.

#### Increasing contributory liability causes trademark bullying – brands will sue to shut down secondary markets and stifle platform innovation

Matt Schruers, 2023 - President Computer & Communications Industry Association. Written Statement submitted to the Senate Judiciary Committee, “Back to School with the SHOP SAFE Act: Protecting Our Families from Unsafe Online Counterfeits” Senate Hearing, 10/3, <https://www.judiciary.senate.gov/imo/media/doc/2023-10-03_-_testimony_-_schruers.pdf> //DH

Existing law correctly recognizes that trademark owners are in the best position to accurately and efficiently distinguish counterfeit products from authentic goods. Shifting legal responsibility to e-commerce sites, online marketplaces, or other third-party intermediaries through new liability rules would stifle innovation, reduce cooperation, and fail to prevent counterfeiting.

The current doctrine of secondary liability in trademark law achieves the proper balance, fostering a diverse ecosystem of online marketplaces that benefits small businesses and consumers. When intermediary services fail to act on specific knowledge of infringement (for example, when a brand owner has notified an online service of a counterfeit product), courts have generally held services liable. The existing regime has helped provide the legal framework to grow a robust secondary market for safe, genuine goods at competitive prices. Consumers derive enormous value from secondary markets, where they have the opportunity to resell products they no longer need, or purchase genuine products at a discount.

Historically, premium brands have disliked secondary markets because they do not afford brandowners total control over the pricing or images of their merchandise. Yet U.S. law has never afforded that. The U.S. approach to trademark is one that acknowledges your personal property rights in the goods you buy. Many brands would prefer consumers not resell what they lawfully own. To respect property rights means honoring the principle that if you bought it, you own it. If consumers buy a legitimate, lawfully manufactured luxury good, they have the right to do whatever they want with their property, including reselling that good online. Even if some prominent foreign brand owner would rather not compete against that resale market.

We must ensure that any new legislation does not undermine personal property rights, or harm the valuable resale market for consumers. Changing secondary liability rules could encourage trademark owners to engage in anticompetitive practices and pursue secondary market goods that may not be counterfeit but may be competing with the trademark owner's products. In fact we're already seeing evidence of this.7 Aggravating this phenomenon would result in the diminution of the secondary market, harming consumers; to avoid increased liability, e-commerce sites would allow only sellers authorized by the trademark owner.

Additionally, changes would not eliminate counterfeit goods. Infringement analysis is often too fact-specific to permit wide-scale removal by services while maintaining a fair and robust marketplace. Liability for e-commerce sites and marketplaces would instead incentivize trademark owners to go after intermediaries instead of the actual bad actors: the counterfeiters.

#### A transition to a circular economy prevents global environmental collapse – it’s try or die

Miriam Eimannsberger, 2019 - Master Thesis in the Department of Forest Economics at Swedish University of Agricultural Sciences. “Transition to a circular economy – the intersection of business and user enablement” <https://stud.epsilon.slu.se/15070/1/eimannsberger_m_190923.pdf> //DH

Since the industrial revolution the dominant economic model in high income countries has been a linear economy. In a linear economy a take-make-use-dispose mentality directs societal consumption behaviour. The almost inevitable fate of a product is its disposal at the end of its product life. According to Lieder & Rashid (2016 p. 37) this is explained by “disposable products with the explicit purpose of being discarded after use (planned obsolesce) heralded the era of fashion and style hence stimulating throwaway-mindset which is today known as linear consumption behaviour”. This system reaches the limits of its capacity. A wide range of environmental problems, water and air pollution and resource depletion call for a radical change and transition to a sustainable economic system. Scarce resources will be under even more pressure as material intensity is predicted to increase with the global middle class, i.e. the largest resource demanding consumer group, doubling in size to 5 billion by 2030 (EMF 2013b). Human survival is at stake as the stability of economies is threatened together with the “integrity of natural ecosystems” (Ghisellini et al. 2016 p. 11). To do justice to the demanding consumers, the supplying producers but also the struggling environment a solution serving all stakeholders needs to be implemented as quickly as possible. A possible and not at all new but rather rediscovered solution can be the implementation of a circular economy (CE).

In short, CE is about creating closed loop material flows keeping “products, components and materials at their highest utility and value” (EMF 2013a) and use them through multiple phases. CE is also about waste prevention, resource efficiency, leakage minimisation and dematerialisation (Geissdoerfer et al. 2017). Figure 1 depicts a principle model for a CE where raw materials are only added for manufacturing and re-manufacturing of products or components already in the system. These have been recycled or re-used by the consumer maybe several times already. Waste is almost non-existent and leaves the system as residual waste if not further used.

The shift from a predominantly linear to a circular economy needs the active involvement of many different stakeholders at several different levels. Some major enablers and also potential preventers that should be named are industries, companies or businesses, policy makers and users or consumers. Ghisellini et al. (2016 p. 11) accentuate their role in CE implementation as “cleaner production patterns at company level, an increase of producers and consumers responsibility and awareness, the use of renewable technologies and materials [and] the adoption of suitable, clear and stable policies and tools” are their main tasks. Companies and consumers can exert a major influence on an economy. Figure 2 shows the rapid historical and predicted growth of the middle-class from 1950 to 2030.

There is a rapid increase in the world middle class taking place since the early 2000’s. With this comes an increase in purchasing power and, consequently, a shift in demand from loose, unpacked products to manufactured, packaging goods leading to higher material and waste impact (EMF 2013b).

In addition, Table 1 shows the immense power companies and businesses wield in the global economy. It is shown that 50 % of the world’s 50 largest economies in revenue generation in US$ in 2016 were corporations rather than countries (countries coloured in black, corporations coloured in red). This does not only emphasize the immense influence the companies can exercise but also the responsibility, difference and guidance companies can embody in a shift towards a more environmentally friendly and sustainable economic system. Walmart Inc., for example, had a higher yearly revenue in 2016 than countries such as Spain, Sweden or Russia.

Besides consumers and businesses, policy makers can drive change towards CE. One example for a policy maker acting on the need for a systematic shift is the European Union. In 2015 the EU published their “Closing the loop – an EU action plan for the circular economy”. This states that a circular economy will “save energy and help avoid the irreversible damages caused by using up resources at a rate that exceeds the Earth's capacity to renew them” (EC, 2019, 2, p. 2). The action plan presents the regulatory framework for an EU-wide transition to circular economy including guidance for circular solutions supporting production, waste management, consumption and renewable energies.

## 2NC / 1NR - Blocks

### They Say: “Nonunique – Circular Economy Decreasing”

#### Startup platform innovation is spurring the transition to circularity

Peter Evans, 2024 – Chief Strategy Officer, McFadyen Digital and Co-Chair, MIT Platform Strategy Summit. “'Green Unicorns': Circular Marketplaces Can Lead The Way” Forbes, 3/8, <https://www.forbes.com/sites/forbesbusinesscouncil/2024/03/08/green-unicorns-circular-marketplaces-can-lead-the-way/> //DH

Individual companies, ranging from Patagonia to Caterpillar, have been embracing circularity. This is a positive step, but not enough. Meaningful circularity requires scale and therefore more than what one company can typically do on its own. This is where marketplaces come in. Circular marketplaces connect multiple buyers and sellers of used, repaired, refurbished, remanufactured or recycled goods, components or materials. Circular marketplaces have the potential to play a major role in transforming the way we approach material reuse, with a market size that has real impact.

Green Unicorns

The term "unicorn" has been used to signify the rare class of startups that reach a value of $1 billion or more. Within this group, there is a small subset of startups advancing sustainability and environmental goals. These startups, even more rare, have become known as "green unicorns." Examples include Back Market, Carousell, Vestiaire Collective, Wallapop, Letgo, StockX, Depop and Grover.

These companies facilitate circular business models by enabling peer-to-peer exchange, rentals, subscriptions or redistribution of used goods across categories like electronics, fashion, appliances and more. Their ability to achieve valuations over $1 billion demonstrates the growing potential of circular economy platforms and marketplaces.

The Circular Marketplace Advantage

Circular marketplaces offer several key advantages that position them as powerful agents of change in driving the growth of the circular economy. One major advantage is lower transaction costs. By providing a centralized platform for buying and selling pre-owned goods, circular marketplaces reduce the time, effort and expense involved in finding buyers and sellers for used products. This increased efficiency lowers the barriers to participation in the circular economy.

Additionally, circular marketplaces benefit from positive network effects. As more buyers and sellers participate, the selection of available products grows alongside the potential customer base. This creates a self-reinforcing cycle where a larger network of users makes the platform more valuable, attracting even more participants. These strong network effects can rapidly accelerate the adoption and scale of circular business models.

Moreover, circular marketplaces are well-positioned to leverage cutting-edge technologies like tracing, artificial intelligence and advanced analytics. Product tracing allows the authentication and tracking of an item's history, building trust. AI can optimize pricing, inventory management and demand forecasting. And analytics provide insights to streamline operations and create superior user experiences. By rapidly integrating these innovations, circular marketplaces can gain an edge over traditional linear businesses and drive transformative change toward a more circular economy.

Launching A Circular Marketplace

Startups aiming to establish and rapidly scale a circular marketplace and potentially become a green unicorn should consider several factors:

First, market selection is crucial. The startup should target high-volume, high-value markets like electronics. Used smartphones, laptops, tablets and EV batteries often have predictable residual value and high potential for reuse or refurbishment, but are not currently serviced by national or regional wholesale circular marketplaces.

Second, the startup should invest in a scalable, modular technology stack that can handle high traffic and adapt to changing business needs. This could involve using cloud-based solutions, microservices architecture and platforms like Encore by SAP that are designed for circular economy business models. The tech stack should support features like inventory management, pricing algorithms, logistics integration and seamless user experiences.

Third, operational excellence is paramount. The startup should build efficient processes that account for the special characteristics of circular transactions for product sourcing, inspection, grading, refurbishment, pricing and reverse logistics. Building an ecosystem of reliable suppliers, refurbishment centers and logistics providers is crucial. The startup must also develop robust quality control measures, coupled with insurance and guarantees, to ensure customer satisfaction and to maintain the platform’s reputation.

Finally, the startup should seek investment from venture capital firms or impact investors with a proven track record in marketplaces, circular economy and sustainability. This is a small but growing category and includes companies like FJ Labs, which can provide valuable guidance, industry expertise and connections.

Conclusion

The world needs more circular marketplaces, especially ones that can grow to green unicorn status. Linear marketplaces have proven their ability to efficiently scale—Amazon now seamlessly connects more than 2 million sellers with over 310 million buyers. If we are to transition to a more circular economy, we need business models, processes and transactions that can scale on that level. Circular marketplaces offer this potential.

As we grapple with how to improve global circularity, circular marketplaces have a promising role to play. Building circular ecosystems holds the key to overcoming the limitations of individual initiatives. The combination of lower transaction costs, positive network effects and the agility to adopt new technologies like tracing and AI uniquely empower circular marketplaces to catalyze the transition to a more resource-efficient and sustainable economic model.

These advantages make circular marketplaces formidable enablers of systemic change.

#### Circular economy is growing through the online secondhand market

Jonas Strandell, 2024 - Chief Marketing Officer for Besedo, an online platform ”The Second-Hand Trend: The Future of Online Marketplaces” 3/13, <https://besedo.com/blog/second-hand-online-marketplace/#:~:text=The%20resale%20of%20used%20items,a%20thredUP%20and%20GlobalData%20report>. //DH

The circular economy is in full swing, and for an excellent reason. With finite natural resources on the planet and the demand for resources exceeding what the earth can regenerate each year, we cannot continue with our current linear production path. The second-hand trend is here to stay.

The circular economy aims to transition into consuming less natural resources by reusing, upgrading, and recycling products. There are many benefits to this way of thinking, including reducing waste, extending the life of products, and saving resources. It’s also been shown to boost the economy by creating jobs in the recycling and reuse industry.

The resale of used items – an integral part of the circular economy – is booming as people grow more accustomed to buying second-hand. Resale has grown 21 times faster than the retail apparel market. It will become more significant than fast fashion by 2028, according to a thredUP and GlobalData report.

The second-hand market

Many companies are now looking to tap into the $24 billion second-hand market, and it’s easy to see why. Second-hand goods are often cheaper than their new counterparts, and there’s a growing consumer preference for sustainable and environmentally friendly products.

By bringing together buyers and sellers in one online space, online marketplaces help streamline the second-hand market. Thus making it more accessible to consumers. And with the added benefit of lower prices and greater sustainability, it’s easy to see why the second-hand trend is worth watching.

#### The circular transition is building, but online platform innovation will take the transition to scale

Peter Evans, 2023 – Chief Strategy Officer, McFadyen Digital and Co-Chair, MIT Platform Strategy Summit.”How to scale the circular economy” Circular: For Resource and Waste Professionals. 9/25, <https://www.circularonline.co.uk/features/how-to-scale-the-circular-economy/> //DH

Momentum is building to advance a more circular economy globally. Many major companies, start-ups, cities, countries, and international organisations have all embraced circular economy principles and launched supporting initiatives.

Venture capital and private equity investment into circular economy businesses has grown since 2020, indicating growing commercial interest. Multilateral organisations, such as the OECD (Organisation for Economic Co-operation and Development), World Economic Forum and United Nations (UN) all have major initiatives to accelerate the transition to a circular economy.

This momentum stems from concerns over resource scarcity and sustainability, as well as shifting consumer demand and commercial interest in circular models that emphasise reuse, repair, and recycling.

However, there is still much more that needs to be done. Measures are needed to scale circular transactions, across a wide range of sectors, including apparel, electronics, plastics, machinery, EV batteries and commercial buildings.

Circular platforms

One way to ensure circular economy initiatives scale is through circular platforms.

By connecting buyers and sellers of underutilised assets, facilitating resale marketplaces, streamlining reverse logistics, providing data insights, and building circular economy communities, platforms can create digital infrastructure to advance the circular principles of reuse, repair, refurbishment, and recycling.

The connectivity, information exchange, material tracking and quality assurance enabled by platforms allow stakeholders to participate in circular activities like resource sharing, redistribution of used goods, and closed-loop material flows.

Platform business models have demonstrated the ability to successfully scale and achieve widespread adoption in a variety of industries and use cases, enabling connection and exchange among large networked user bases. Key factors like network effects, discovery engines, and buyer and seller aggregation have facilitated growth.

#### Business and consumers are shifting to a circular economy now

Daniel R. Cahoy, 2023 – Robert G. and Caroline Schwartz Professor of Business Law, Research Director for the Center for the Business of Sustainability, Smeal College of Business, Pennsylvania State University “Trademark’s Grip Over Sustainability” Colorado Law Review, v94, n4, 6/1, <https://lawreview.colorado.edu/print/volume-94/trademarks-grip-over-sustainability/> //DH

Moreover, there are signs that product disposal trends are slowing (or at least attitudes may be shifting). In addition to the percentage of recycling efforts that work, consumers and firms are also finding it easier to preserve existing goods by repairing them[45] or remaking them into new, usable products.[46] Instead of filling landfills and junkyards, or inflicting mountains of waste on vulnerable populations, there is a growing market in product renewal. To some degree, the interest in such products reflects a sustainability mindset. But in some cases, it is nothing more than a desire for less expensive versions of new products. There are even instances in which the remade article is actually more expensive and luxurious than the original. Increasingly, there is a real business case to be made for alternatives to disposal.

B. The Novel Outlets and Supply Chains for Existing and Remade Products

An alternative to recycling is the reuse of a product or some piece of the product. In some cases, there is an easily understandable market. Consider vintage goods, which may be acquired for less money and may convey a fashion or historical/collectable cachet.[47] In this context, consumers reject the attraction of “new and improved” in favor of a connection to the past. That connection could be sentimental or ironic, and it ensures a longer life for a good that is at least temporarily saved from the refuse bin.

But of course, desiring old for the sake of old is a limited aspect of the overall marketplace. More interesting and significant is the ability to restore, refurbish, and improve goods for continued use so that no functional sacrifice is made. An increasing number of companies are seeing the value in participating in this market. Others feel the pressure to join as a matter of social responsibility. Regardless, we seem to be witnessing a revolution in the effort to keep products in circulation and avoid early obsolescence.

### They Say: “No Link: Safe Harbor”

#### SHOP SAFE’s safe harbor is untested and technological limitations make it hard for platforms to comply

Megan Bannigan et al, 2024 - Partner, Debevoise & Plimpton LLP “Does the US SHOP SAFE Act go too far in shifting liability?” World Trademark Review, 4/20, <https://www.worldtrademarkreview.com/article/does-the-us-shop-safe-act-go-too-far-in-shifting-liability> //DH

Shifting the burden of detecting counterfeits

The SHOP SAFE Act’s safe harbour provisions provide some reasonable requirements of marketplaces: for example, encouraging programmes to quickly remove suspected counterfeit listings and terminating sellers who repeatedly list counterfeit products. But the overall scheme creates a new and untested landscape by shifting the burden for policing for counterfeits from brand owners onto marketplaces. There are substantial technological limitations to screening technology, and platforms are often not well positioned to know every product a brand has made and how to identify every counterfeit that might be out there. To combat counterfeiting, platforms need to implement policies for screening and terminating listings, and sellers and brand owners need to provide platforms with the information to effectively do so.

#### Even with perfect compliance, small platforms will be subject to greater litigation – large platforms will use the threat of liability to shut them down

Nicholas Garcia, 2022 - Policy Counsel at Public Knowledge, focusing on emerging technologies, intellectual property, and closing the digital divide. JD, Georgetown “SHOP SAFE Act: The Trademark Timebomb Masquerading as Consumer Protection” 2/15, <https://publicknowledge.org/shop-safe-act-the-trademark-timebomb-masquerading-as-consumer-protection/> //DH

The host of new regulations and increased liability created by SHOP SAFE would be catastrophic for competition in e-commerce. This regime would devastate smaller online platforms like Etsy, OfferUp, and other small platforms that allow third-party sellers because it applies to any platform with just $500,000 in sales in the past year—for comparison, Amazon had $364.38 billion in sales in the U.S. last year. So, while this bill seems to target tech giants like Amazon, their ample resources for regulatory compliance and deep pockets to fight lawsuits, really makes SHOP SAFE an opportunity to eliminate many of their smaller competitors through legislative games instead of offering better products or services.

Any site with “features that allow for arranging the sale or purchase of goods” qualifies as an “electronic commerce platform” and this could include messaging apps, forums, and any small-scale online seller. Even the $500,000 threshold is entirely undermined by a provision that applies the requirements in the bill to platforms of any size if they are served with 10 notices of trademark infringement—with no time frame limitation specified. Anyone familiar with the rampant copyright takedown notice abuse enabled by the Digital Millennium Copyright Act will recognize that aggressive rightsholders will easily be able to extend SHOP SAFE to any platform under this law.

The law includes an onerous suite of regulations that sites must comply with, making its broad applicability particularly concerning. Many of the requirements will be difficult and expensive to implement for most smaller platforms, and perhaps impossible for others. For example, one requirement is that platforms implement “reasonable proactive measures for screening goods before displaying the goods to the public.” To operate at any scale, such measures would require automated content filtering systems that are both expensive and difficult to design and implement. Similarly, the bill also requires platforms to ensure that third-party sellers “use images that accurately depict the goods sold, offered for sale, distributed, or advertised on the platform.” Again, analysis and approval of images, and verification that said images are accurately linked to the third-party seller’s wares, pose significant technical and content moderation challenges for smaller platforms.

These kinds of regulations, combined with the broad definition of applicable platforms, conspire to make many online platforms—even those not specifically designed for e-commerce—responsible for undertaking costly and complex new systems to remain compliant with SHOP SAFE’s requirements. And even with total compliance, platforms still remain open to litigation—the statutory obligations, if followed, merely create an affirmative defense from the contributory liability claims. This expensive and extensive set of requirements will functionally doom smaller competitor platforms and further cement the dominance of large firms like Amazon and Facebook.

#### Even if lawsuits are meritless, the mere threat from trademark bullies will shut down secondary resale markets

Nicholas Garcia, 2022 - Policy Counsel at Public Knowledge, focusing on emerging technologies, intellectual property, and closing the digital divide. JD, Georgetown “SHOP SAFE Act: The Trademark Timebomb Masquerading as Consumer Protection” 2/15, <https://publicknowledge.org/shop-safe-act-the-trademark-timebomb-masquerading-as-consumer-protection/> //DH

The real beneficiaries of the SHOP SAFE Act are not consumers but big brands that want to aggressively pursue knockoffs, cheap competition products, and the secondary resale market. Trademarks can be extraordinarily broad, encompassing certain colors or even common words or phrases. Creating such an expansive regime of trademark liability online will inevitably lead to brands pursuing aggressive protection of anything they deem remotely infringing with little regard for SHOP SAFE’s intended purpose of protecting consumers. For example, the infamously litigious Monster Cable Products, Inc. has more than 70 trademarks on the word “monster” and has gone after auto transmissions, carpet-cleaning machines, mini-golf, people selling t-shirts, the job-hunting site monster.com, Monster energy drink, and even Disney over “Monsters Inc.” merchandise. It is easy to imagine how aggressive rightsholders will abuse SHOP SAFE by bullying platforms into settlements over meritless claims of infringement.

### They Say: “No Link: Reputational Harm and Sanctions”

#### Empirically – brands accuse legitimate resale as being counterfeit. They’ll over-enforce and shut down legitimate resale markets

Jonathan Berroya, 2021 - Senior Vice President and General Counsel, Internet Association. Testimony before the Subcommittee On Courts, Intellectual Property, and The Internet Judiciary Committee U.S. House of Representatives. The SHOP SAFE Act: Stemming the Rising Tide of Unsafe Counterfeit Products Online. 5/27, <https://docs.house.gov/meetings/JU/JU03/20210527/112713/HHRG-117-JU03-Wstate-BerroyaJ-20210527.pdf> //DH

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

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

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

#### Shaming won’t stop bullying

Leah Chan Grinvald, 2021 – \* Associate Dean for Academic Affairs and Professor of Law, Suffolk University School of Law. “Trademark Enforcement and Statutory Incentives” <https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=2390&context=facpub> //DH

One downside to over-enforcement may cause the balance of benefits to sway the other way—the potential for shaming by the trademark owner’s consumers or the broader public.121 In these days of over-sharing on social media, it is easy for recipients of abusive ceaseand-desist letters to post them or share that they have received such demands.122 Unfortunately, though, the prospect of shaming or being labeled a “#trademarkbully” does not deter all entities, and additionally, not all shaming is successful.123 Given that there are no provisions in the Lanham Act that penalize entities for over-enforcing their marks, some entities could see only benefits to enforcement. Post-Romag, these benefits have potentially increased.

#### The incentives for trademark bullying are stronger - brands perceive they have a duty to police or they’ll lose their trademark

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

**Italics in original**

Although the Lanham Act does not explicitly require trademark owners to "police" their marks, over a half-century's worth of court cases does appear to place some type of burden on an owner to ward against infringing uses of their trademark. 239 The specifics of this duty, however, remain unclear.240 What is clear, though, is the *perception* by some trademark owners that this "duty" requires them to pursue possible infringers aggressively or else "lose their mark."241 This perception is fueled by judicial statements such as this one from a 2003 Federal Circuit opinion, "Trademark law requires that the trademark owner police the quality of the goods to which the mark is applied, on pain of losing the mark entirely." 242 However, the actual loss of one's mark is extremely rare243 and is therefore not a valid reason for over-enforcement.

The real driver for aggressive enforcement is the reward, as well as a lack of consequences for over-stepping the legal boundaries. Courts have taken as probative evidence aggressive enforcement strategies as proxies for a "strong" mark.244 As one of us has argued in previous works, this aggressiveness can often cross the line into abusiveness where the parties in the dispute are imbalanced.245 It is easy for a mark owner to slide into abusiveness, as trademark law lacks any mechanisms to hold trademark bullies accountable. There are virtually no consequences for overenforcement.246 But the rewards are great, as a strong or famous trademark is granted a larger scope of protection. Trademark owners whose marks are considered strong may bring infringement actions against defendants using the same or similar marks on unrelated products. In addition, owners of famous trademarks may bring dilution actions where defendants are using marks that can be associated with the famous mark, but is not even causing a likelihood of confusion. This enlarged scope of protection can provide some trademark owners with the ability to claim almost complete exclusivity over all uses of their marks. Given this lack of understanding of the duty to police one's trademark, the potential rewards, and the lack of consequences for over-enforcement, it is easy to understand aggressive (and perhaps even abusive) enforcement in the online space where uses of trademarks are ubiquitous.247 Trademarks appear everywhere online, from blogs to reviews, to sales of used product listings.248 An industry of "brand management" has arisen to help trademark owners police their trademarks online, which gives owners the ability to note any use of their mark.249 Unfortunately, while not every use of a trademark is infringing, it may appear infringing to an over-zealous policer as long as it is unauthorized.250 What this does is place trademark owners into overdrive in sending cease-and-desist letters or including trademark claims within take-down notices to platforms. As discussed above in Parts II and III, this places not only a serious burden on the platform, but risks unbalancing the ecosystem of the macrobrands and microbrands.

#### There are no consequences to bullying, so companies will weaponize the plan to attack legitimate competition – that prevents a functional e-commerce marketplace

Anthony James Dispoto, 2015 - J.D. Candidate 2015, University of San Diego School of Law. “Protecting Small Businesses against Trademark Bullying: Creating a Federal Law to Remove the Disparity of Leverage Trademark Holders Maintain over Small Business,” 16 SAN DIEGO INT'l L.J. 457 (2015). Hein Online, accessed via University of Michigan //DH

These threatened legal actions burden the targeted company rather than the trademark holders that send out the cease-and-desist letters.7 6 The targeted company is in a precarious situation in deciding which action to take.77 They can choose to wait and see if the threatening party will take legal action against them, while continuing to potentially infringe the trademark. Otherwise, the targeted company may seek a declaratory judgment, which could state that its trademark does not infringe upon the other party's mark, thereby precluding further legal action against it.78 The threatening party suffers no consequences from sending such letters. Since they are often viewed as aggressive policing tactics, no sanctions are imposed and the threatening party can decide whether or not to pursue legal action. 79 Small businesses are particularly influenced by the potential threat of litigation, which in turn is externalized as a cost to the consumer and the economy.80

By extrapolating the theory of famous economist Adam Smith, it seems that this externalized cost in trademark bullying creates a barrier to entry, which in turn limits the choices available to consumers. ' It does so by imposing higher costs in the market place, thereby increasing the initial amount of capital investment needed for new market entrants and ultimately limiting the amount of entrants who are capable of success in the market.82 Cease-and-desist letters specifically impose high costs on businesses, not just in legal fees, but also in time diverted from the business.83 This harms the consumer, because the fewer companies that are in the market, the fewer products that are available to the public, and those available will tend to be of a lower quality. 84 Competition between companies improves the quality of products and lowers prices, because competitors produce better and cheaper goods or services in order to win consumers.85

### They Say: “No Impact: Circular Greenwashing”

#### Greenwashing causes consumers to seek out more information and adopt greater circular consumption behaviors

João M. Lopes et al, 2023 - Miguel Torga Institute of Higher Education & NECE-UBI—Research Unit in Business Sciences, University of Beira Interior, Covilhã, Portugal “The Dark Side of Green Marketing: How Greenwashing Affects Circular Consumption?” Sustainability 2023, 15, 11649. <https://doi.org/10.3390/su151511649> //DH

This study makes valuable contributions to the existing literature by establishing connections among the conceptual frameworks of greenwashing, environmental concerns, sustainable information collection, and circular consumption. The results augment our theoretical comprehension of how consumers adjust their behaviors and information-seeking habits in response to corporate actions such as greenwashing. These findings resonate with the norm activation theory, suggesting that when consumers perceive a problem, such as greenwashing, it activates personal norms (like environmental concerns), leading to a change in behaviors, such as the collection of sustainable information.

Simultaneously, the study sheds light on the role of consumers’ reactions to greenwashing and their implications for circular consumption intentions. This examination provides a richer understanding of consumer behavior in the context of a circular economy. This relationship can be interpreted through the lens of the Theory of Planned Behavior, which highlights greenwashing as a significant external influence capable of shaping attitudes—in this case, environmental concerns; molding subjective norms, exhibited as sustainable information collecting; and influencing perceived behavioral control, represented as circular consumption intentions. The study’s findings offer a deeper understanding of the paradoxical scenario where consumers confronted with deceptive environmental claims respond by adopting more sustainable behaviors. The findings illustrate that consumers’ exposure to greenwashing stimulates their awareness and concern about environmental issues and that environmental concerns mediate the effect of greenwashing on circular consumption intention.

#### Consumer demand is the vital internal link to a circular economy – negative reactions to greenwashing shift consumer behavior

João M. Lopes et al, 2023 - Miguel Torga Institute of Higher Education & NECE-UBI—Research Unit in Business Sciences, University of Beira Interior, Covilhã, Portugal “The Dark Side of Green Marketing: How Greenwashing Affects Circular Consumption?” Sustainability 2023, 15, 11649. <https://doi.org/10.3390/su151511649> //DH

Furthermore, the study introduces sustainable information collection as an intermediary between greenwashing and circular consumption intention. This presents a valuable addition to the discourse on sustainable consumption, as it highlights the importance of information accessibility in sustainable decision-making. Our results lend support to the hypothesis that consumers who are aware of greenwashing tactics are not passively influenced by them but instead respond by actively seeking more reliable information about the products or services. The more they engage in sustainable information collection, the more likely they are to intend to participate in circular consumption behaviors. This reinforces the idea that information seeking is a powerful tool consumers can utilize to make more sustainable decisions [54,55]. Therefore, understanding the mediating role of sustainable information collection provides valuable insights into how consumers process and respond to greenwashing. It indicates that consumer empowerment, through the provision and active seeking of reliable sustainability information, could be a potent mechanism to mitigate the negative effects of greenwashing and promote circular consumption.

#### The circular transition is more than just recycling – production and consumption will shift downward

Paula Tejón Carbajal, 2020 – Global Campaign Strategist for Greenpeace International. “Slowing the circular economy” 7/17, <https://www.greenpeace.org/international/story/44079/slowing-the-circular-economy/> //DH

Let’s start by adding “slow” to the term “circular economy”, because language matters.

For our economy to be restorative and generative, not just cycling more and more resources around faster and faster, we need to both: slow the flow and close the loop by reducing production and consumption. This means reversing the waste hierarchy and putting “refuse” (as in, “don’t want it”) and “reduce” at the top of the list. This allows us to tackle consumerism, overconsumption and overproduction head-on while questioning the notion of growth altogether.

Yes.. this means consuming less and…

… rolling-out mindful and ecological designs that enable sustainable ecosystems for all of us.

It should look like this:

SIMPLE – It should be created with tools that are easy to understand and repair

INPUT-ORIENTED – Production must understand the value of all resources and how to conserve and use resources effectively, with a minimum of waste.

WITH PURPOSE – Products must be designed for longevity, promoting extended use to reduce buying more of the same stuff. They must be durable as well as repairable, reusable, refurbishable, recyclable. The end of life of the product and its disposal must be factored into this design phase as well as the material mix.

FOR MULTI USE- Reverse-engineering and modularity are key to enable repair and different uses of the product.

DESIGN GLOBAL, MANUFACTURE LOCAL — Combining globally shared productive knowledge, with distributed manufacturing closer to the place of use and demand.

… emphasize genuine sustainability to prevent and reduce environmental impact across the entire life-cycle of products to protect our planet, and:

PREVENT and minimise the impact of parts and materials.

Source your parts and materials LOCALLY.

Use efficient and RENEWABLE ENERGY.

Eliminate all TOXIC chemicals and pollution.

Avoid WASTE and make the by-products of today’s resources for tomorrow.

… open source information and standards to enable to repair and foster innovation, which is:

FREE – Information freely available for anyone to access.

EDITABLE – in formats that allow people to remix, add, build upon, learn and improve.

OPEN – share under open licenses to enable legal decentralised collaboration and enable the right to fix and the access to repair tutorials or spare parts.

So, Is this slow circular economy already happening??

Yes! Some concrete steps that are already changing the landscape of the economy and our cultural attitudes are tax incentives for repair, setting limits on advertising, mandatory take-back schemes or Extended Producer Responsibility regulations. Eliminating the use of hazardous chemicals, reducing resource use, such as energy, water and raw materials, as well as carrying out better working practices (wages, standards, health, working hours etc.) for manufacturers and in farming and mining. To improve production, people are slowing it down and making it more resilient. New, alternative business models (eg. sharing, renting, cooperative, non-hierarchical, slower fashion cycles) are also a common feature of businesses and organisations and facilitate a slow circular economy

A truly slow circular economy will require all the above as well as strong transparency, accountability, collaboration and localisation across value chains, industries and movements. Eventually, all the above will lead to an economy that is built on a foundation of shared ownership designed to generate value for those that create it while delivering fair and just outcomes which preserves resources and ecosystems while benefiting the many rather than the few.

### They Say: “No Impact: Environment Resilient”

#### There are limits to resilience – surpassing too many thresholds means complete collapse

KATHERINE RICHARDSON et al, 2023 - Globe Institute, Faculty of Health, University of Copenhagen, Copenhagen, Denmark. “Earth beyond six of nine planetary boundaries” Science, 9/13, <https://www.science.org/doi/10.1126/sciadv.adh2458> //DH

The planetary boundaries framework (1, 2) draws upon Earth system science (3). It identifies nine processes that are critical for maintaining the stability and resilience of Earth system as a whole. All are presently heavily perturbed by human activities. The framework aims to delineate and quantify levels of anthropogenic perturbation that, if respected, would allow Earth to remain in a “Holocene-like” interglacial state. In such a state, global environmental functions and life-support systems remain similar to those experienced over the past ~10,000 years rather than changing into a state without analog in human history. This Holocene period, which began with the end of the last ice age and during which agriculture and modern civilizations evolved, was characterized by relatively stable and warm planetary conditions. Human activities have now brought Earth outside of the Holocene’s window of environmental variability, giving rise to the proposed Anthropocene epoch (4, 5).

Planetary-scale environmental forcing by humans continues and individual Earth system components are, to an increasing extent, in disequilibrium in relation to the changing conditions. As a consequence, the post-Holocene Earth is still evolving, and ultimate global environmental conditions remain uncertain. Paleoclimate research, however, documents that Earth has previously experienced largely ice-free conditions during warm periods (6, 7) with correspondingly different states of the biosphere. It is clearly in humanity’s interest to avoid perturbing Earth system to a degree that risks changing global environmental conditions so markedly. Ice cover is only one indicator of substantial system-wide change in numerous other Earth system dimensions. The planetary boundaries framework delineates the biophysical and biochemical systems and processes known to regulate the state of the planet within ranges that are historically known and scientifically likely to maintain Earth system stability and life-support systems conducive to the human welfare and societal development experienced during the Holocene.

Currently, anthropogenic perturbations of the global environment are primarily addressed as if they were separate issues, e.g., climate change, biodiversity loss, or pollution. This approach, however, ignores these perturbations’ nonlinear interactions and resulting aggregate effects on the overall state of Earth system. Planetary boundaries bring a scientific understanding of anthropogenic global environmental impacts into a framework that calls for considering the state of Earth system as a whole.

#### The world’s sitting on a consumption time bomb and the Earth is on the brink – without a shift to sustainable consumption, the Earth will collapse

Miriam Eimannsberger, 2019 - Master Thesis in the Department of Forest Economics at Swedish University of Agricultural Sciences. “Transition to a circular economy – the intersection of business and user enablement” <https://stud.epsilon.slu.se/15070/1/eimannsberger_m_190923.pdf> //DH

**CE = Circular Economy**

In order to supply a growing world population production keeps increasing simultaneously. With the resources being limited the demand of exponential economic and population growth becomes ever more difficult to be met (Lieder & Rashid 2016). In addition to the increasing pressure on the last limited resources for production, the Ellen MacArthur Foundation (2013b p. 15) states that “we are sitting on a consumption time bomb”. Within the next 20 years it is expected that three billion additional consumers will enter the market. One main reason is the growing middle classes in emerging markets especially in the Asia-Pacific region (EMF 2013b). With this increase comes an increase in waste generation. One explanation is the increased material intensity as the new group of consumers entering the markets chose manufactured and packaged goods instead of unbranded products. The impact of packaged goods is much higher “both because of processing losses and packaging” (EMF 2013b p. 15). Another exemplary reason for an increase in waste is the production for the mass market resulting in quantity over quality for the product and its sourcing and consequently a relatively short product lifespan (Cooper 2013). The throwaway mentality is closely linked to the linear

economic model (Gullstrand Edbring et al. 2016). Therefore, while pressure increases on resource extraction, the amount of waste keeps increasing. The amount of waste already produced is often left unused at landfill sites while it keeps growing (Lieder & Rashid 2016).

The linear model is responsible for the current wealth in many of the high income countries as relatively low resource prices in relation to the labour costs “have been the engine of economic growth” (EMF 2013b p. 17). However, this wealth has also created a “wasteful system of resource use” (EMF 2013b p. 17) and brings with it several threats. The growth in production, consumption and waste generation stresses the global environment. Providing resources, act as a life support system and being a sink for waste and emissions are economic functions the environment serves. Nonetheless, there is usually no price on the stress caused for the environment by linear produced or consumed products. Prices do not reflect the negative impact caused (Ghisellini et al. 2016).

According to Cooper (2013 p. 137) “the global predicament that this [economic growth] poses is that people in affluent countries are unwilling to give up, while in newly industrialized and other poorer countries people are unwilling to do without”. In other words, while several countries want to increase their consumption to follow the goal of economic growth, the high-income countries would need, but are unwilling, to reduce their consumption. Global resource scarcity does not allow the current levels of consumption for everyone around the globe. Gullstrand Edbring et al. (2016 p. 1) bring it to the point: “Western consumption patterns are unsustainable: if the world's 7 billion inhabitants had consumed in the same way as the Swedish population does today, we would need 3.25 Earths to support this lifestyle”. The negative impacts caused by the make-use-dispose linear economic model, therefore, threaten “the stability of the economies and the integrity of natural ecosystems that are essential for humanity's survival” (Ghisellini et al. 2016 p. 11). Humanity’s survival is on threat as “measured by the land area that can support human habitation, the earth is shrinking” (Korhonen et al. 2018 p. 38). Korhonen et al. (2018 p. 38) summarize the negative impacts by stating that “deserts are expanding, the sea level is rising, the population is growing, per capita consumption is increasing, the volume of livestock and cattle is growing and biodiversity is depleting at ever faster rates”. The rapid environmental degradation caused by the wasteful make-use-dispose system has led to a change in thinking among practitioners and academics, politicians, businesses and civilians to implement a system of sustainable development, production, consumption and policies (Heshmati 2017).

One logical way to change the linear system is its reverse: closing the waste loop to form a cyclical flow of materials and energy rather than the linear chain (Korhonen et al. 2018). A circular economy considers the value of a product to stay within the economic system even after it presumably has become a waste product. Waste emissions and generation is minimised along with an efficient energy, material and water consumption (Geng et al. 2013). By closing the loop and including the concept of CE in an economic system resource use can become more efficient, especially regarding urban and industrial waste, aiming at a better balance between the economic system, the environment and the society (Ghisellini et al. 2016).

# Information Sharing Counterplan

### 1NC– Data-Sharing CP

#### The next offcase position is the data-sharing counterplan

#### Text: The United States federal government should establish a public-private partnership between brand sellers, online marketplaces, and U.S. law enforcement agencies to share data and coordinate anti-counterfeiting enforcement, and increase resources for criminal enforcement of counterfeiting.

#### The counterplan solves the case without increasing trademark protection

Sujai Shivakumar, 2021 – former associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. “How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces” 3/3,

<https://itif.org/publications/2021/03/03/how-data-sharing-partnerships-can-thwart-counterfeits-online-marketplaces/> //DH

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

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

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

## 2NC / 1NR – Blocks

### They Say: “Platforms Won’t Cooperate”

#### The CP changes incentives – with Customs and Border Patrol taking the lead, they’ll coordinate to make sure there’s no free riding and they’ll develop stronger detection technology

Sujai Shivakumar, 2021 – former associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. “How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces” 3/3,

<https://itif.org/publications/2021/03/03/how-data-sharing-partnerships-can-thwart-counterfeits-online-marketplaces/> //DH

**CBP = Customs and Border Patrol**

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

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

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

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

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

#### Even if not every platform participates, it’s still comparatively better than the plan. Liability reduces platform cooperation more

Sujai Shivakumar, 2021 – former associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. “How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces” 3/3,

<https://itif.org/publications/2021/03/03/how-data-sharing-partnerships-can-thwart-counterfeits-online-marketplaces/> //DH

**CBP = Customs and Border Patrol**

CONCLUSION

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

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

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

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

#### The infrastructure already exists for cooperative enforcement and brands participate in Customs and Border Patrol’s IPR Center now. The CP just strengthens existing channels for enforcement

Sujai Shivakumar, 2021 – former associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. “How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces” 3/3,

<https://itif.org/publications/2021/03/03/how-data-sharing-partnerships-can-thwart-counterfeits-online-marketplaces/> //DH

CBP is also home to the IPR Center, whose role is to coordinate diverse federal efforts related to interdiction, investigation, and outreach to the public and law enforcement.41 As a part of this effort, rights holders, online marketplaces, payment processers, and companies involved in all points across the supply chain regularly meet with members of the IPR Center to share their best practices, concerns, and suggestions. This information could enable further collaboration on complex cross-cutting challenges, including enhanced information sharing, joint enforcement actions, and specialized, targeted training and outreach. For example, Amazon’s new Counterfeit Crimes Unit is already sharing and analyzing data to assist targeted inspections by CBP aimed at preventing counterfeit products from entering the U.S. markets. Amazon is also working with the IPR Center to develop an “information exchange that will enable industry participants—stores, payment service providers, banks, and shipping companies—to better identify and stop counterfeiters before they can reach consumers.”42

### They Say: “Bad Information Turn”

#### Their argument assumes status quo information-sharing which is constrained by legal barriers that only allow incomplete sharing. The CP removes those barriers and incentivizes better information

Sujai Shivakumar, 2021 – former associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. “How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces” 3/3,

<https://itif.org/publications/2021/03/03/how-data-sharing-partnerships-can-thwart-counterfeits-online-marketplaces/> //DH

**CBP = Customs and Border Patrol, TFTEA = Trade Facilitation and Trade Enforcement Act**

Despite dedicated efforts by brand sellers, online marketplaces, and law enforcement agencies, counterfeiters continue to evade detection. As noted, counterfeiters use multiple merchant accounts, withhold their business information, and provide false information to CBP (this includes covering or obscuring infringing trademarks until the counterfeit goods clear with CBP). Counterfeiters also avoid detection by shipping infringing marks separately from the goods, relying on in-country assembly and distribution after the separate components have crossed the U.S. border.44 Counterfeiters also minimize detection by CBP by intentionally mislabeling shipping containers.

For example, CBP recently seized fake Nike shoes that were incorrectly labeled as napkins on the shipping containers in an attempt to hide the counterfeit goods.45 And data for shipping manifests of small packages is often incomplete or of poor quality, which makes it difficult for CBP to use it for identifying packages at high risk of containing counterfeits.46

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

First, antitrust concerns regarding the sharing of corporate information have forestalled cooperation among various brand sellers and online marketplaces.47 Antitrust law focuses on improving consumer welfare by preventing collusion among market participants. However, active cooperation—targeted to share and analyze data concerning suppliers and map logistics networks to detect flows of counterfeit products—is needed among these participants in order to improve consumer welfare. To the extent legal and academic conceptions of antitrust lag behind advances in data innovation, the resulting ambiguity could restrain advances in anticounterfeiting policy.48

Second, U.S. laws prohibit CBP from sharing any more information about counterfeits with e-commerce platforms and common carriers (such as FedEx, UPS, and DHL). A 2019 report by the Senate Finance Committee notes that TFTEA allows CBP to share information that “appears on the merchandise and its packaging and labels” with rights holders if it believes that the good in question may infringe upon a registered copyright or trademark, but that TFTEA does not authorize CBP to share information with e-commerce platforms or common carriers.49 Sharing this information more broadly would allow these actors to work together to stop the distribution of counterfeit products. Further, TFTEA does not provide CBP sufficient authority to disclose information to rights holders regarding the containers used to ship the goods to the United Sates (exclusive of retail packaging).50 Sharing this information would improve tracking of counterfeit shipments.

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

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

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

#### Removing legal barriers to collaboration incentivizes better information sharing and new detection technology

Sujai Shivakumar, 2021 – former associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. “How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces” 3/3,

<https://itif.org/publications/2021/03/03/how-data-sharing-partnerships-can-thwart-counterfeits-online-marketplaces/> //DH

**CBP = Customs and Border Patrol**

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

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

There are statutory and regulatory barriers arising from TSTEA and TSA that inhibit some types of information sharing on counterfeit goods and distribution networks between law enforcement agencies and retailers as well as among retailers.57 Congress should remove these barriers. In addition, CBP should update its rules to permit disclosing to rights holders details about abandoned infringing goods.58

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

### They Say: “Permutation Do Both”

#### The perm fails and links to the circular economy DA – adding liability to information sharing causes risk avoidance that reduces cooperation and innovation

Sujai Shivakumar, 2021 – former associate director of the Center for Data Innovation, focusing on the impact of data innovation in the retail sector. “How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces” 3/3,

<https://itif.org/publications/2021/03/03/how-data-sharing-partnerships-can-thwart-counterfeits-online-marketplaces/> //DH

**CBP = Customs and Border Patrol, TFTEA = Trade Facilitation and Trade Enforcement Act**

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

### They Say: “Criminal Prosecution Fails”

#### Increasing criminal enforcement is comparatively better than changing liability, and provides more resources to law enforcement

Jonathan Berroya, 2021 - Senior Vice President and General Counsel, Internet Association. Testimony before the Subcommittee On Courts, Intellectual Property, and The Internet Judiciary Committee U.S. House of Representatives. The SHOP SAFE Act: Stemming the Rising Tide of Unsafe Counterfeit Products Online. 5/27, <https://docs.house.gov/meetings/JU/JU03/20210527/112713/HHRG-117-JU03-Wstate-BerroyaJ-20210527.pdf> //DH

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