June 23, 2021

Re: SHOP SAFE Roundtable Questions

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Engine works with government and a community of thousands of high-technology, growth-oriented startups across the nation to support the development of technology entrepreneurship through economic research, policy analysis, and advocacy on local and national issues. We appreciate the opportunity to submit these written responses and participate in roundtable conversations regarding the Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce (SHOP SAFE) Act of 2021.

Overall, we are concerned that the changes proposed in the SHOP SAFE Act would have an outsized, negative impact on e-commerce startups and interactive websites—and would also not have any demonstrable impact on resolving the problems of unsafe counterfeit goods.[1] Of note, for example, increasing the amount of litigation and requiring companies to use upload filters to monitor for potential infringement would create substantial costs and risks. This would raise new barriers to entry and restrict competition, and at the same time reduce the options for small businesses and digital entrepreneurs that rely on diverse e-commerce offerings.

The doctrine of contributory liability currently applied by U.S. courts is balanced and largely working well, and such areas of the law—which address the legal exposure companies can face over their user's actions—are especially important to Internet startups and smaller online platforms. Most platforms experience little, if any, alleged trademark infringement.[2] Changing the law to increase the

[1] Engine has articulated similar positions in the past. These comments draw from previous submissions, including, e.g., Comments of Engine Advocacy in Response to Secondary Trademark Infringement Liability in the E-Commerce Setting, Docket No. PTO-T-2020-0035 (Dec. 28, 2020), *available at* https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5ff37a915abd827cadbf968f/1609792145348/2020.12.28_Comments+to+Docket+PTO+T+2020+0035.pdf; Letter to Members of the Subcommittee on Courts, Intellectual Property, and the Internet from Engine (May 28, 2021), *available at* https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60b0d9a9c74bdb53c673bba0/1622202794314/2021.05.28_Engine+Letter+re+SHOP+SAFE.pdf.

[2] *E.g.*, *2019 Transparency Report*, Etsy (2020), https://extfiles.etsy.com/advocacy/Etsy_2019_Transparency_Report.pdf (of 65 million items for sale, fewer than 34,000 takedown requests, of which fewer than half pertained to trademark); *compare Shapeways Fact Sheet*, Shapeways (2018), https://static1.sw-cdn.net/files/cms/press/Shapeways-Fact-Sheet-2018-Q3.pdf *with 2018 Transparency Report*, Shapeways, https://www.shapeways.com/legal/transparency/2018 (last visited Dec. 23, 2020) (of over 45,000 postings, platform only received 331 takedown notices that involved trademark); Michal Rosenn, *Kickstarter Transparency Report 2015*, Kickstarter (Apr. 25, 2016), https://www.kickstarter.com/blog/kickstarter-transparency-report-2015 (out of over 75,000 projects, Kickstarter processed 67 total trademark claims); *compare Intellectual Property*, WordPress https://transparency.automattic.com/intellectual-property/ (last visited June 23, 2021) (reporting 3,769 trademark notices received from 2014-2020) *with* Comments of Automattic Inc., *In re* Section 512 Study, Docket No. 2015-7, at 2 (Mar. 22, 2017) (reporting tens of millions of posts and media files uploaded each month).

costs and risks those platforms face would therefore catch little, if any, additional sale of unsafe counterfeit goods.[3] But the downside of such a shift in liability would be substantial, making it harder for startups and emerging e-commerce platforms to launch and compete, and restrict economic growth in multiple sectors.[4]

Indeed, even under the current, relatively balanced approach to contributory liability, the high costs of monitoring and covering legal risk for potentially infringing user-generated posts are already seen to confer a competitive advantage.[5] Most platforms routinely implement systems for removing alleged trademark infringement they know of—e.g., upon receipt of a notice—just as they do for claims of copyright infringement.[6] But as e-commerce platforms scale, depending on a series of factors, once they can afford it many will develop technology and/or hire teams of content moderators to help flag potential counterfeits (among other things). eBay invests as much as $20 million per year in trust and safety efforts,[7] and Alibaba has made a significant investment in technology to try and identify potential infringement.[8] These and numerous other e-commerce platforms already do more than notice-and-takedown for trademark claims, but the costs of doing that are far more than what a startup could afford.[9] As scholars have noted:

> [W]hile the eBays of the world can afford to spend millions of dollars combating counterfeiting, this may not be the case for smaller-scale market participants. Requiring "mom and pop" online brokers to wage a million-dollar war against counterfeiting would likely drive these retailers out of business, undesirably narrowing consumer choice.[10]

The changes proposed in SHOP SAFE would further tilt the scales in favor of well-resourced, established companies and against smaller or nascent e-commerce platforms. For example, these smaller companies would suddenly be expected to develop inherently imperfect technology to filter all user posts—something larger incumbents already do (again, at substantial cost). Likewise, smaller

---

[3] *See, e.g.*, Katja Weckström, *Liability for Trademark Infringement for Internet Service Providers*, 16 Marquette Intel. Prop. L. Rev. 1, 45 (2012) ("[e]xposing [platforms] to a multitude of claims that demand high transaction costs to settle seems inefficient and disproportionate . . ." and "counterfeiting will likely persist, regardless of efforts or liability").
[4] *See, e.g.*, Daphne Keller, *Toward a Clearer Conversation About Platform Liability*, Knight First Amendment Institute (Apr. 6, 2018), https://knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability ("When platform liability risks expand, wealthy incumbents can hire lawyers and armies of moderators to adapt to new standards. Startups and smaller companies can't.").
[5] *See, e.g.*, Weckström, *supra* note 3, at 48 (noting "many smaller actors that cannot afford efforts like those of eBay"); *cf.* Jennifer M. Urban et al., *Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice*, 64 J. Copyright Soc'y U.S.A. 371, 397-402 (2017) (noting that shifts toward DMCA-plus are already viewed as a competitive advantage for established platforms, and can affect market entry and startup success).
[6] Thomas C. Rubin, *Leveraging Notice and Takedown to Address Trademark Infringement Online*, 37 Colum. J.L. & Arts 585, 587 (2014) (representative of trademark owner and online service provider noting that most "reputable online service platforms . . . have implemented similar notice-and-takedown systems that have proven effective").
[7] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 98-99 (2d Cir. 2010).
[8] *See, e.g.*, B. Bruce Rich & David Ho, *Sound Policy and Practice in Applying Doctrines of Secondary Liability Under U.S. Copyright and Trademark Law to Online Trading Platforms: A Case Study*, 32 Intel. Prop. & Tech. L.J. 1, 9 (2020).
[9] *Supra* note 5.
[10] Sonia K. Katyal & Leah Chan Grinvald, *Platform Law and the Brand Enterprise*, 32 Berkeley Tech. L.J. 1135, 1149-50 (2017) (quoting Jordan Teague, *Promoting Trademark's Ends and Means through Online Contributory Liability*, 14 Vand. J. Ent. & Tech. L. 461, 491 (2012)).

companies would also need the financial resources to withstand (potentially multiple rounds) of costly litigation—where damages can be automatically set at $200,000,[11] and it can easily cost $500,000 just to reach summary judgment.[12] By contrast, the average seed-stage startup raises $1.2 million, a sum that is expected to cover its costs for nearly two years.[13] And most startups do not have even close to that much money.

Instead of continuing to pursue the SHOP SAFE, we encourage Congress to consider solutions tailored to the problem of unsafe counterfeits. For example, Congress could consider disrupting the ability of bad actors to monetize the selling of unsafe counterfeits, and it could explore better coordination among public and private entities to identify bad actors.

1. **Should verification under (4)(A)(ii) require government identification? If not, what "other reliable documentation" would there be?**

At this time, we have no comments in response to this question.

2. **Should the definition of "electronic commerce platform" be revised, such as to remove the "payment, or shipping of goods" language? Why or why not?**

The definition of "electronic commerce platform" in the current bill is so broad, it would seem to capture basically any interactive website with even a tangential connection to online sales or the exchange of physical goods. Such a broad definition, coupled with the other provisions of SHOP SAFE (e.g., filtering mandates), would be highly problematic. The definition would include, for example, traditional e-commerce platforms, websites where creators and innovators raise money or monetize projects, websites that offer payment and shipping services, food delivery services, and social media sites where small businesses link to other platforms for online sales. While we might support a narrower definition, it would be important to couple that narrower definition with a legal regime better tailored to combat unsafe counterfeits, and it would be critical that any definitions be clear and predictable.

3. **Should any revisions be made to the definition of "goods that implicate health and safety"?**

Similarly, the definition of "goods that implicate health and safety" in the current bill is so broad it would seem to capture basically any physical good. Here again, though, while we might support a narrower definition, it would be important to couple that narrower definition with a legal regime better tailored to combat unsafe counterfeits—and one without so many unrelated consequences for innovation and economic growth online.

---

[11] 15 U.S.C. § 1117(c).
[12] Evan Engstrom, *Primer: Value of Section 230*, Engine (Jan. 31, 2019), https://www.engine.is/news/primer/section230costs.
[13] *The State of the Startup Ecosystem*, Engine 17 (2021), https://engineis.squarespace.com/s/The-State-of-the-Startup-Ecosystem.pdf.

4. **Should the Act require platforms to have a mechanism for consumers to contact them if they suspect they have received a counterfeit product?**

At this time, we have no comments in response to this question.

5. **Generally, should we be concerned about bad-faith use of the notice-and-take- down process? Does the SHOP SAFE Act incentivize bad-faith use of the take-down process more than the current legal structure? Why or why not? If there is a concern, how would you propose addressing it?**

Yes. Indeed, while the current doctrine of contributory liability is largely working well, there is still abuse of the system, and few opportunities for startup e-commerce platforms and users wrongfully accused of infringement to fight back. Abusive trademark assertion or enforcement has an especially "deleterious effect on startups and smaller platforms that may lack the resources to respond properly to a dispute" between a purported brand owner and the user accused of infringement.[14] This puts a fine point on the value of balanced frameworks and strongly cautions against adopting new legal doctrines which would make these forms of abuse easier or more profitable. And shifting more liability onto e-commerce platforms would end up escalating the removal of more legitimate posts and goods, which would hurt small businesses and creators who have posts improperly removed.

It is unfortunately common for purported trademark owners to overreach or send bad faith notices, for example, seeking to have non-infringing posts removed. As a number of smaller platforms have reported, spurious takedown notices can "be sent with the deliberate intent to exert unwarranted control over the free flow of information online. The rightsholder may intend to undermine a competitor or to censor critical speech, for example."[15] Examples of such improper or abusive takedown requests include:

- A small business owner that repurposes items—for example, making purses from food packaging or jewelry from building blocks—was subject to trademark infringement allegations for trying to sell those repurposed products on an e-commerce platform for homemade goods.[16]
- Volkswagen filed multiple takedown requests to remove beetle art from a digital art platform. In an apparent sweep to remove all images that were tagged with the word "beetle," Volkswagen effectively asserted ownership over bug species and asked the platform to remove images a scientist had drawn of different species of beetles. The artist had to retain a lawyer to have her art restored and lost revenue in the time her work was removed from the platform.[17]

---

[14] Katyal, *supra* note 10, at 1165.
[15] Comments of Etsy, Foursquare, Kickstarter, Meetup, and Shapeways, *In re Development of the Joint Strategic Plan for Intellectual Property Enforcement* 2 (Oct. 16, 2015), *available at* http://extfiles.etsy.com/advocacy/Etsy_IPEC_Comment.pdf.
[16] *Id.* at 3.
[17] *Volkswagen Claims Ownership of an Entire Group of Insects*, Elec. Frontier Found., https://www.eff.org/takedowns/volkswagen-claims-ownership-entire-group-insects (last visited Dec. 23, 2020).

Moreover, in the trademark context there is no formal mechanism for e-commerce platforms to restore content,[18] like the Digital Millennium Copyright Act's (DMCA) counter-notice procedure for restoring wrongfully removed content.[19] A number of e-commerce platforms have reported seeing a conflation of copyright- and trademark-related takedown requests, as the notice-sender knows "the use of [trademark-related] requests significantly reduces the ability of users targeted by an accusation of infringement to challenge that accusation."[20]

If platforms faced heightened liability for contributory trademark infringement, it would also create an incentive for them to remove more legitimate, non-infringing content. Indeed, because platforms know even less about other entities' trademarks, those platforms would have even less information than the brand owners to decide what to take down. The risk of liability when getting those questions wrong, though, would pressure platforms to increase takedowns of non-infringing posts.

Not only must policymakers proceed with caution when considering changes to the law—because it would hurt startups and hinder competition and innovation—but there are other interests at stake. Shifting liability to platforms for alleged infringement they have no knowledge of or involvement in would: give rise to "concerns about freedom of expression" and "free access to information," implicate legitimate uses of someone else's trademarks online, and restrict the "development of new technologies, including those capable of both infringing and non-infringing uses."[21] It would require platforms to "radically contract" their legitimate offerings, which would hurt small businesses, Internet users, Internet-enabled creators, and consumers that do (or could) rely on such marketplaces.[22] And that "overreactive impulse [to over-takedown] carries a disparate impact on small businesses and smaller platforms, who are often ill equipped to defend themselves against potentially false claims of contributory infringement."[23]

Finally, mandating further automation of efforts to detect trademark infringement would exacerbate the chilling effects of existing notice-and-takedown systems. We already live in a time of algorithmic trademark enforcement. Many e-commerce platforms, interactive websites, and brand owners deploy technology to automate detecting potential trademark infringement. And the negative effects of those experiences (as well as experiences in the copyright context) should caution against mandating companies take automation even further. As we have previously noted:[24]

---

[18] *E.g.*, Katyal, *supra* note 10, at 1163.

[19] This counter-notice procedure to restore wrongly removed, non-infringing content, is underutilized and largely ineffective, but it does exist. *See, e.g.*, 17 U.S.C. § 512(g) (counter notification process); *Is the DMCA's Notice-and-Takedown System Working in the 21st Century?: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116th Congress 15-17 (2020) (testimony of Abigail A. Rives), *available at* https://www.judiciary.senate.gov/imo/media/doc/Rives%20Testimony.pdf (explaining how DMCA fails to combat abuse, and describing under-utilization of counter notice procedures); *Engine Responses to DMCA Reform Bill Questions from Senator Tillis*, Engine 14-18 (Dec. 1, 2020), *available at* https://www.recreatecoalition.org/wp-content/uploads/2020/12/2020.12.01_Engine-Responses-to-DMCA-Questions-for-Stakeholders.pdf (similar).

[20] *2018 Transparency Report*, Shapeways, https://www.shapeways.com/legal/transparency/2018 (last visited Dec. 23, 2020); *see also, e.g.*, Katyal, *supra* note 10, at 1164 (noting similar reports from other platforms).

[21] *E.g.*, Miquel Peguera, *Converging Standards of Protection from Secondary Liability for Trademark and Copyright Infringement Online*, 37 Colum. J.L. & Arts 609, 611 (2014).

[22] *E.g.*, Rich, *supra* note 8, at 8; Rubin, *supra* note 6, at 590-91.

[23] Katyal, *supra* note 10, at 1148.

[24] Rives, *supra* note 19, at 23.

> Automating decisions about potential copyright infringement has far reaching consequences. Much has been said about the First Amendment problems of removing content without a full assessment of whether it is, in fact, infringing.[25] But the chilling consequences of takedown go further, as recipients of takedown notices are deterred from other forms of online communication and engagement generally. In one study, the majority of people who received a takedown notice were unlikely to repost or re-share the removed content. But 72 percent of respondents indicated they would also be less willing to share content they created personally in the future.[26] 81 percent reported concerns about their privacy after receiving such notice, and 75 percent said they would be less likely to contribute to online communities in the future.[27] Those chilling effects are even more pronounced in women than in men.[28] Before imposing more automation and rigidity on [platforms], Congress should account for the fact that individual users and creators (and even more so, women) who have a post taken offline will be less likely to share creations or participate online going forward.

Changes proposed by SHOP SAFE and proposals that could mitigate abuse or improper removal of non-infringing content: The bill proposes changes that could exacerbate the problems of abuse, such as automating decisions about potential counterfeits and imposing new rigidity around the consequences of even improper takedown requests. Introducing more flexibility into decisions about repeat infringers and the consequences of a platform receiving ten notices could mitigate some of these problems.[29]

In addition, Congress could also consider implementing something more similar to the DMCA's counter-notice procedure. However, while importing the DMCA's counter-notice structure to the trademark space would be an improvement over the status quo,[30] that is an underutilized mechanism. In the copyright space, Engine has proposed a number of changes that could further reduce the burden of improper notices.[31] Merely by way of example:

- Ensure that the standard for measuring bad faith notices or improper notices considers whether the notice was objectively improper.
- Adjust damages (including the availability of statutory damages) to be tailored to increase balance around claims of alleged infringement online.[32]
- Likewise, craft proportionate remedies for victims of improper notices.

---

[25] *E.g.*, Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 Harv. J.L. & Tech. 171 (2010).
[26] Jonathon W. Penney, *Privacy and Legal Automation: The DMCA as a Case Study*, 22 Stan. Tech. L. Rev. 412, 447 (2019).
[27] *Id.*
[28] *Id.* at 450, 470-71.
[29] *See infra* response to questions 8, 10.
[30] Comments of Etsy, *supra* note 15.
[31] *Responses to DMCA Reform Bill Questions*, *supra* note 19, at 14.
[32] The availability of statutory damages in the copyright context presumably serves a different purpose than statutory damages in the counterfeit context, so consideration of modifications to statutory damages for (unsafe) counterfeits would likely not be directly analogous to previous recommendations Engine has made in the copyright context.

- Consider a repeat false notice sender provision to allow platforms to ignore notices from repeat false senders.
- Ensure that the sending of counter-notices does not create intimidating structures that make individuals feel like they have to expose themselves to undue financial, security, or privacy risks when opposing problematic notices.

6. Should platforms be required to notify consumers when they remove a listing because it appeared to be selling counterfeit products?

If by "consumer," the question is asking whether platforms should be required to notify third-party sellers that they have been accused of selling a counterfeit product, we would support a requirement that the platform provide that notice to the third-party seller. At least in order to allow third-party sellers to challenge improper allegations of counterfeiting, those sellers would likely benefit from knowing a posting was removed.

If by "consumer," the question is asking whether platforms should be required to notify all (potential) purchasers that a given third-party seller was accused of selling a counterfeit, there are reasons to question whether that is the right response and/or when that information confers (enough) additional value. For example, if a third-party seller has been accused of infringement, but not confirmed to be selling unsafe counterfeit goods, then marking their postings as potentially-counterfeit could lead to lost sales and lost economic opportunity without justification. On the other hand, if the third-party seller is known to be selling (or having sold) unsafe counterfeit products, mere notification to (potential) purchasers alone may not be the best course. It would likely be better for the government to penalize the counterfeiter and/or for the brand owner to pursue civil remedies. This would seem to be a better focus for combatting unsafe counterfeits and comport with notions of due process.

7. Are there any points you would like us to consider with respect to the country of origin identification requirement in paragraph (vi)?

For people who are knowingly or intentionally selling unsafe counterfeits, it would be simple to also lie about the product's country of origin. As such, this requirement bears little (if any) connection to the purported goal of combatting unsafe counterfeit goods.

Yet country of origin identification requirements create substantial challenges for small businesses and third-party sellers as well as compliance hurdles for platforms. First, for many individuals or small sellers (that are not selling counterfeits) it will be difficult to verify the country of origin, or even understand what that concept means for, e.g., handmade products sewn in the U.S. (with fabric and material that may have been purchased in a store), collectibles, and/or 3D printed items.

Second, SHOP SAFE is currently structured to require platforms to display, on each listing, the country of origin and manufacture.[33] Aside from asking third-party sellers to designate the country

[33] § 1114(4)(A)(vi).

of origin, most platforms (as currently defined) would have no way of assessing country of origin for third-party posts—further complicating the issue.

8. **Is the three strikes presumption in (4)(A)(x) helpful for ease of compliance with the repeat infringer policy requirement? Considering both the three-infringing-listing threshold and "reasonable mitigating circumstances" language, is the presumption overly strict, overly permissive, or neither?**

Similar to what we have previously noted in a related copyright context,[34] e-commerce platforms and interactive websites should retain flexibility in defining and implementing repeat infringer policies. Judicial conceptions of a repeat copyright infringer are problematic, as some courts have started to treat repeat *accused* infringers as repeat *actual* infringers.[35] And the SHOP SAFE Act proposes setting up an analogous problem—because it targets someone that "uses" a counterfeit mark (without any limitations connected to health or safety), and does not define what use is. This could easily default companies and courts into assuming use of a counterfeit upon receipt of a notice alleging counterfeit. And in numerous instances an e-commerce platform will be fundamentally incapable of determining whether an accused counterfeiter is actually selling counterfeit goods, at least because the company will never interact with the product itself, further emphasizing reliance on third party notices.[36] Yet mere (and even improper) allegations of infringement should not be enough to remove someone from a platform. And platforms should not be forced to expel their customers, users, and creators based on mere allegations. Instead, they need flexibility to develop and apply repeat infringer policies, to collect and review facts of individual cases and remove those users deemed to be actual repeat infringers. Binding platforms to rigid frameworks will just make it easier for abusers to know what accusations to make to stifle competitors, other creators, or Internet users.

Finally, here again, it is worth considering if a platform's repeat infringer policy is the best policy lever to use in the face of repeated sales of unsafe counterfeits. If there is good reason to believe that a single seller has engaged in repeated instances of selling an unsafe counterfeit, it may be better for the government to penalize the counterfeiter and/or for the brand owner to pursue civil remedies.

9. **Should brand owners be affirmatively required to provide information to platforms in order to avail themselves of the provisions of the SHOP SAFE Act?**

Yes. Trademarks are pervasive across the globe. There are over 2.6 million active trademarks in the U.S. alone.[37] It would be impossible for a new e-commerce platform to learn, monitor, and identify

---

[34] Letter to Members of the House Committee on the Judiciary from Engine (Sept. 28, 2020), *available at* https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5f7257a95df2280137f185da/1601329067695/2020.09.28_Engine+Comments+re+Copyright+and+the+Internet+in+2020.pdf.

[35] *E.g.*, *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns Inc.*, 881 F.3d 293 (4th Cir. 2018).

[36] This inquiry is also complicated in the copyright context. But counterfeit is even more complicated, because knowing whether a product is, e.g., a legitimate piece of merchandise or a knock-off could be imperceptible looking only at a photograph and an online posting.

[37] *4th Quarter FY 2019, At a Glance*, United States Patent and Trademark Office, https://www.uspto.gov/dashboards/trademarks/main.dashxml (last visited Dec. 23, 2020).

alleged infringement of that many marks in the millions of products that are (or could be) posted on these sites. Volume is not the only problem—it is complex to identify specific instances of trademark infringement. Brand owners are much better suited to know what might confuse their consumers and know what products they have authorized.[38] Without brand owners identifying infringement in the first instance, platforms will both over- and under-police, unintentionally blocking legitimate content and letting some infringement slip through the cracks.[39]

10. Is there any other feedback that you would like to provide on the bill?

Mandatory filtering. As drafted, the SHOP SAFE Act requires e-commerce platforms use technology to screen goods before they can be displayed.[40] Adopting such a filtering mandate would create an impossible and unaffordable task for all but the largest, established e-commerce platforms—many of which already have systems in place—and put early-stage companies at a distinct disadvantage.[41] For one, startups would be forced to try and constantly monitor user posts to detect potentially infringing ones. This would include expenses startups, operating on thin margins, could not cover, such as hiring teams of content moderators, developing or purchasing imperfect yet costly filtering technology,[42] and setting aside litigation reserves to cover future legal exposure when that technology fails.[43]

As we have previously explained in the copyright context:

> Technology and filters have many inherent limitations which make them incapable of fully addressing online infringement. Filtering technology is imperfect, with often high false positive rates. It is categorically incapable of answering fact-specific questions of infringement, like fair use [and] licensing . . . . But these filters are also out of reach for most startups. The most sophisticated tools are so expensive that the development costs are orders of magnitude above what a startup could afford. Off-the-shelf tools, which cannot screen much content on a multimedia platform, are also too expensive

---

[38] Restatement (Third) of Unfair Competition § 20 (1995) ("One is subject to liability for infringement of another's trademark . . if . . . in marketing the actor's goods or services the actor uses a designation that causes a likelihood of confusion"); see also, e.g., id. at § 29 (addressing consent to use of a mark); id. at § 24 (addressing use of a mark on genuine goods); id. at § 28 (addressing descriptive fair use); id. at § 33 (addressing licensing of trademarks).
[39] *See, e.g.*, *supra* response to question 5 (discussion of the problem over over-removal).
[40] § 1114(4)(A)(viii).
[41] While beyond the scope of these comments, counterfeiters already find ways around the measures e-commerce platforms deploy to try and prevent trademark infringement. *See, e.g.*, Rich, *supra* note 8, at 9 (noting that even on platforms spending the most, and deploying the most sophisticated technology, it is impossible to keep trademark infringers off; for example, counterfeiters can just change their name or repost infringing items under a new name or different account).
[42] *See, generally* Evan Engstrom & Nick Feamster, *The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools* (Mar. 2017), https://www.engine.is/the-limits-of-filtering (discussing limitations of filtering technology).
[43] *See, e.g.*, Jennifer M. Urban et al., *Notice and Takedown in Everyday Practice* 64 (UC Berkeley Public Law Research Paper No. 2755628, Mar. 30, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628 (noting that some small platforms already struggle to comply with the DMCA's notice and takedown procedure for copyright, and that "[t]he struggle increased further if pressure to implement [proactive] measures arose.").

> for early-stage companies to license and maintain. All filters are limited in the type of content they screen. And for many types of content, there are no filters.[44]

Indeed, as Engine and other smaller companies have noted, there are no existing filters to accurately identify infringement on "sites that allow users to sell physical goods."[45]

The limits of filters—which will fail sometimes (likely often)—and the fact that startups would be incapable of identifying and removing all infringement on their own, also brings substantial litigation cost and risk. Expanding platform liability over users' alleged IP infringement could put early-stage companies at risk of being sued out of existence. It could also discourage entrepreneurs and investors from developing new technology or pursuing new e-commerce business models. Internet platforms, in particular, have been able to innovate and launch because they do not have to hire teams of lawyers to brace for litigation when users are accused of infringement. And investors would be reluctant to fund emerging e-commerce platforms if they knew the money would go to cover liability for user infringement.[46]

"Reasonable awareness of use of a counterfeit mark." In addition to imposing a filtering mandate, the SHOP SAFE Act also includes a requirement to remove listings when a platform has "reasonable awareness of use of a counterfeit mark."[47] This requirement is also fraught from a startup perspective. As we have previously noted in the copyright context,[48] replacing the current "red flag" knowledge standard of the DMCA with a reasonableness standard (similar to that proposed in SHOP SAFE) would be unworkable for small businesses.[49]

As it pertains to the SHOP SAFE Act, this "reasonable awareness" standard would require startups to affirmatively monitor all user posts to try and determine if any involve counterfeiting (or else face the cost and risk of contributory liability litigation). But assessing "reasonable awareness" would also have to be defined in each instance by courts, further increasing the cost and duration of litigation against intermediaries—including startup platforms.

Determining what a platform has "reasonable awareness" of would be a fact-specific inquiry. Those are the types of questions that have to go to a jury.[50] Therefore, for a startup e-commerce platform to definitively know if it had complied with SHOP SAFE and removed content for which it had the requisite reasonable awareness (or not), the company would have to defend itself in a full jury trial.

---

[44] Rives, *supra* note 19, at 2.
[45] Letter to John Kerry, United States Secretary of State, Penny Pritzker, United States Secretary of Commerce, and Michael Froman, United States Trade Representative (Dec. 16, 2016) (on file).
[46] *See, e.g.*, Matthew C. LeMerle et al., *The Impact of Internet Regulation on Early Stage Investment* (Nov. 2014), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/572a35e0b6aa60fe011dec28/1462384101881/%20EngineFifthEraCopyrightReport.pdf.
[47] § 1114(4)(A)(ix).
[48] Rives, *supra* note 19, at 20. Engine has made similar arguments as those articulated in this section in the copyright context, e.g., *Responses to DMCA Reform Bill Questions*, *supra* note 19, at 6-7.
[49] 17 U.S.C. § 512(c)(1)(ii).
[50] *Cf. Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir. 2007) (reasonableness of repeat infringer policy a question of fact); *see also Tran v. State Farm Mut. Auto. Ins. Co.*, 999 F. Supp. 1369, 1372 (D. Haw. 1998) ("An analysis of what is reasonable is almost always de facto a question for the jury.").

As noted, the cost of proceeding just through discovery in related intermediary liability contexts can exceed $500,000,[51] and taking IP cases to trial is easily in the seven-figure range.[52] If it costs more than a startup has to prove it was in compliance with SHOP SAFE, then the proposed structure for avoiding contributory liability would have little (if any) practical value.[53]

In addition, reasonableness is intentionally flexible, meaning that what is reasonable one month might not be reasonable the next, especially as technology changes, as a company grows, or as the type of infringement it encounters shifts. All of those are unpredictable occurrences, but considering the fast pace at which new technology emerges, how counterfeiters find ways around existing protective measures, and how quickly startups can (and do) grow, the problem of a shifting reasonableness standard makes it a very poor fit to this context, since a startup could never know in advance whether or not a court would find its practices to be reasonable.[54] The baseline of what is "enough" will constantly be changing, and static content moderation practices will quickly become outdated and likely be deemed "unreasonable" for purposes of SHOP SAFE.

Applicability to platforms based on annual sales or receipt of notices. The SHOP SAFE Act is written to apply to e-commerce platforms that experience annual sales of $500,000 and those that have received ten notices alleging the use of counterfeit marks by third-party sellers.[55] By contrast, many other areas of the law (including the DMCA) currently treat Internet platforms the same, regardless of size, which contributes to the certainty and clarity of those statutory frameworks—in turn, supporting innovative companies and the economic growth they enable. We are concerned that SHOP SAFE has created a structure that applies to virtually any company (regardless of size) by excluding only the very smallest of websites and creating an easy way for outside third-parties to subject a company to the law. But beyond setting the bar very low in this circumstance, we have some general concerns about proposals to treat different sized companies differently in the intermediary liability context and encourage Congress to proceed with careful thought on that front.

First, platforms excluded from SHOP SAFE would have to be very small. The bill's broad definition of e-commerce platforms implicates a range of different types of companies and websites—and as such, different financial and business models. But assuming a platform charges third-party sellers a 10 percent fee, a company could see only $50,000 in annual revenue and still be expected to have financial resources and staff to, e.g., screen all posts and cover the costs of a counterfeit lawsuit.[56] Those costs are orders of magnitude more than what the company would collect in the year.[57]

---

[51] Engstrom, *Primer*, *supra* note 12.
[52] Malathi Nayak, *Costs Soar for Trade Secrets, Pharma Patent Suits, Survey Finds*, Bloomberg Law (Sept. 10, 2019), https://news.bloomberglaw.com/ip-law/costs-soar-for-trade-secrets-pharma-patent-suits-survey-finds (median cost of patent suit with $1-10M at stake is $1.5M, and cost of patent case with over $15M at risk is $4M).
[53] *Cf.* Engstrom & Feamster, *supra* note 42, at 25.
[54] *See* Engstrom & Feamster, *supra* note 42, at 24.
[55] § 1114(4)(C).
[56] This assumption of a 10 percent fee is merely an estimate based on the fee structure of a variety of sites that would presumably meet the definition of an e-commerce platform, although those numbers vary widely depending on the company, the business model, the product sold, and the service provided. This 10 percent, overall, is on the high end based on our unscientific survey of websites such as Etsy, Amazon, eBay, PayPal, Stripe, Kickstarter, and Patreon.
[57] For example, compare the annual revenue of $50,000 to the cost of defending a lawsuit to summary judgment—$500,000—or the amount that eBay spent in 2010 to combat trademark infringement—$20,000,000.

Relatedly, SHOP SAFE proposes that even smaller platforms and websites be subject to the law's requirements if they receive ten notices of alleged counterfeiting. As currently written, this provision is also vague, putting companies in a difficult position of determining whether they have received ten notices which cover posts "that reasonably could be determined to have used a counterfeit mark in connection with . . . goods that implicate health or safety." If a platform receives ten spurious notices, it would either need to go ahead and implement upload filtering, affirmative monitoring, etc. or be ready to (pay to) defend its decision otherwise in court. This provision also means anyone could send ten notices to a platform and impose substantial costs and risks—a provision that could be easily subject to abuse. (Especially because there are no consequences in the bill for sending improper notices.)

Second, more generally, it appears that the exceptions in SHOP SAFE are geared to support smaller companies, and in our view, it is critical that Congress recognize startup needs and attend to the unique circumstances of nascent e-commerce platforms. But especially in areas like this, of intermediary liability, we have concerns about treating different sized companies differently and hope these considerations can be useful as Congress thinks about this bill.[58] As we have previously noted:[59]

> Certainty in the law is important to all businesses, especially high-tech, high-growth startups. . . . And there are problems using size as a proxy for ease of compliance with the law. There are also problems using small/large thresholds to regulate startups—because emerging technology companies are designed to scale, ideally rapidly, and often defy simple definitions.

Briefly, establishing thresholds for e-commerce platforms of different sizes risks merely delaying, rather than resolving, the consequences of imposing liability on platforms for the actions of their users. Decreasing certainty, imposing new costs, or creating new risks would have an outsized negative impact on startups and smaller tech companies, making it harder for them to succeed, attract investment, and compete. But tying those changes in the law to company size would still have a negative impact. Some of the problems may just kick-in as companies approach those thresholds. Moreover, the incorporation of thresholds could generate new uncertainties (or create traps for the unwary), incentivize unproductive behavior, and be difficult to implement in the context of high-growth startups.

Merely by way of example:

- Even with thresholds, many concerns that motivate treating smaller platforms differently would immediately re-emerge when those smaller platforms near the threshold. For example, under SHOP SAFE, when a company experiences annual sales of $500,001 it would be

[58] This response merely summarizes a few concerns that can emerge in setting thresholds around company size or age. Engine remains willing to discuss and explore these notions, and has explored some of them in a bit more detail in the copyright context. *Responses to DMCA Reform Bill Questions*, *supra* note 19, at 1-6.
[59] *Id.* at 1-2.

expected to use technology and affirmative content moderation comparable to much larger platforms. And as such, a still-very-small platform would have a harder time competing (or would have an increased incentive to be acquired by a more-established competitor that already has technological and financial wherewithal to comply with SHOP SAFE).[60]

- It can be difficult (if not impossible) for a startup e-commerce platform to predict its growth, which would in turn make it difficult (or impossible) to know when the new liabilities and monitoring costs of SHOP SAFE would kick in.
- In other areas of the law with size-based thresholds, complex legal tests have developed to determine where a given company falls relative to the threshold. The affiliation rule and "integrated employer" tests, for example, complicate the inquiry of a company's headcount for employment law and loan eligibility purposes.[61] It becomes hard for companies to know their "size," and these become fact-intensive inquiries—meaning companies have to go to court and incur legal fees to prove their size. Considering $500,000 in annual sales, for example, there are a number of variables that could create uncertainty around firm size—when is the start and end of the year, how often is a platform expected to calculate its sales, are shipping fees included or not, etc.

* * *

Thank you for your consideration and for the opportunity to submit these comments and participate in the roundtable process. Startups are an essential component of our innovation economy, and it is vital to factor their interests in policy decisions. Engine remains committed to engaging with the Subcommittee on these and other important issues.

---

[60] *Cf.* Thomas Spoerri, *On Upload-Filters and Other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market*, 10 J. Intel. Prop. Info. Tech. E-Commerce L. 173, 179 (2019), *available at* https://www.jipitec.eu/issues/jipitec-10-2-2019/4914 (referring to Europe's Article 17, explaining how "[a] small or young company offering services related to content uploaded by users and thereby trying to compete with established [OSPs] . . . will - at the latest after three years of its existence . . . - fall under the direct liability regime of article 17 DSM and have to apply filtering technologies"); Lenard Koschwitz, *Startups Told to Pack Their Bags After Three Years*, EU Observer (Feb. 8, 2019), https://euobserver.com/stakeholders/144126 (discussing Europe's carve-out from Article 17, noting that "European startups will become more likely to be acquired at an early stage instead of scaling-up"); *see also, e.g.*, Michael Mandel & Melissa Blaustein, Opinion, *Entrepreneurs Need Policy to Escape the 'Startup Trap,'* Gainesville Sun (Feb. 26, 2019), https://www.gainesville.com/opinion/20190226/point-of-view-entrepreneurs-need-policy-to-escape-startup-trap (explaining while "'carve-outs' are beneficial for companies who stay below the relevant thresholds, the threat of losing these exemptions can make entrepreneurs think twice before expanding").

[61] *E.g.*, 13 CFR 121.301(f) (affiliation rule); Kathryn L. Hickey & Erin M. Estevez, *Affiliation in the Context of SBA Loans – Guidance for Venture Capital Investor*s, NVCA (Mar. 27, 2020), *available at* https://nvca.org/wp-content/uploads/2020/03/VC-SBA-Lending-and-Affiliation-Guidance-for-SBA-Loan-Programs.pdf (four page document explaining affiliation rule for startups, specifically as it pertains to investors and access to COVID relief programs); *Grace v. USCAR*, 521 F.3d 655, 662-3 (6th Cir. 2008) (explaining Department of Labor regulations for evaluating employment relationships to assess whether an employer has to provide FMLA leave).