November 13, 2018

Vishal J. Amin
United States Intellectual Property Enforcement Coordinator
Office of Management and Budget
Executive Office of the President
intellectualproperty@omb.eop.gov

Re: Comments of the Consumer Technology Association Regarding the Development of the Joint Strategic Plan

Thank you for the opportunity to submit comments on the ongoing IPEC effort to develop and implement an intellectual property enforcement strategy to combat infringement. Consumer Technology Association (CTA)™ is the trade association representing the $377 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.

In comments on prior Joint Strategic Plans, CTA has stressed that national borders should not be obstacles to legitimate trade, investment, and innovation. This stance is well aligned with the Coordinator's message, in the present Request for Public Comments, that we must "regard America's inventive and creative capacity as something that we must protect, promote and prioritize." In prior rounds CTA has led its Comments with strong and explicit support for national and international measures against counterfeit goods. A continuation of this progress is no less a priority today, and is addressed in detail below.

In accord with the Coordinator's request for a focus on constraints on American innovation, however, CTA leads its discussion by expressing deep concern over proposed IP-related constraints on America's Online Service Providers ("OSPs"), under consideration in the European Union and elsewhere, that would hamper the operation and innovation of American companies, as well as the right and ability of American consumers to receive information and services. Accordingly CTA recommends that the next Joint Strategic Plan should include:

- Protection from foreign impositions on or denial of U.S. users' worldwide internet access
- Recognition in IP of U.S. First Amendment and Public Domain values, including:
    - International recognition of private noncommercial use and other fair uses
    - Statutory damage reform / avoidance so that IP is not used to silence dissent
    - Opposition to government "backdoors" to private encryption
- A reliable framework for protecting the international flow of personal data, while avoiding data localization
- A direct right of action for US content providers against overseas infringers
- A continued emphasis on combating counterfeit products

Oppose Link and Tax Mandates and Constraints on U.S. Online Service Providers

The proposals pending in the European Union to punish and constrain OSPs for the conduct of their users (Article 13) and to tax news reporting (Article 11) are aimed at U.S. OSPs[1] and are directly contrary to U.S. and North American public policy as most recently iterated in the USMCA.

- Article 13 of the Digital Single Market (DSM) provision would impose mandatory content filters as the only alternative to punishing OSPs for user conduct. While useful in voluntary or safe harbor contexts, *ex ante* filtering cannot deal with speech, such as fair use, satire, and parody, that is protected by U.S. laws and values.[2] Such filters can be no more than approximate in their operation, and are widely known to flag lawful content and be subject to abusive claims.
- Article 11 imposes a "link tax" on the identification of news articles. Such provisions would stifle speech and have led to lawsuits rather than revenue for publishers.[3]

Although aimed at successful U.S. OSPs, these provisions would be even more damaging to local startups. The United States, joined by Canada and Mexico, chose to avoid this direction in

[1] "In Germany, the measure was aimed at Google News, requiring the internet giant to pay German newspapers for the snippets presented in the Google News search results. Instead, though, publishers opted-in without receiving payment as their traffic would've suffered as a result." Graeme Burton, *MEPs reject draft copyright directive that would have mandated copyright filters*, Computing, (July 5, 2018, "Burton"), https://www.computing.co.uk/ctg/news/3035418/meps-reject-draft-copyright-directive-that-would-have-mandated-copyright-filters.

[2] *See, e.g.*, Cory Doctorow, *Not In Our Name: Why European Creators Should Oppose the EU's Proposal To Limit Linking and Censor The Internet*, Electronic Frontier Foundation (Sept. 10, 2018), https://www.eff.org/deeplinks/2018/09/not-our-name-why-european-creators-should-oppose-eus-proposal-limit-linking-and.

[3] Burton, *id*.

the Intellectual Property Chapter[4] of the USMCA. Article 20.J.11 provides that each nation must include:

> (1)(b) limitations in its law that have the effect of precluding monetary relief against Internet Service Providers for copyright infringements that they do not control, initiate or direct, and that take place through systems or networks controlled or operated by them or on their behalf.

This U.S. and North American policy commitment cannot live alongside provisions requiring mandatory filters and takedowns.

The European Union is not the only arena for this contest of values and national laws. The "ASEAN+6" nations, which include China and India, are negotiating an Intellectual Property Chapter of a Regional Comprehensive Economic Partnership.[5] Whether this agreement will follow the North American or the apparent EU lead is very much in play.[6] ***It seems fundamental to IPEC's mission to argue and lobby for the American approach.***

Protect U.S. and Overseas Consumers' Access to Online Information

U.S. internet users, personal and commercial, should not be subject to foreign restrictions on public information, such as the "Right To Be Forgotten." Yet litigation pending in the EU would require U.S. OSPs to be punished for making factual information available to U.S. internet users. Such provisions threaten *both* U.S. companies and U.S. consumers, as they would limit the information available to U.S. internet users, and would punish U.S. companies for practices undertaken to serve U.S. consumers. This threat is imminent. The Court of Justice of the European Union (CJEU) is presently considering whether to penalize search engines for listing content that U.S. consumers and businesses would otherwise be entitled to see.[7]

While constraints on U.S. citizens such as the "Right To Be Forgotten" are not formally grounded in copyright, they are impositions on the Public Domain and the First Amendment, which are organic to U.S. copyright principles. Copyright exclusions, exceptions, and

---

[4] *See* https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/20%20Intellectual%20Property.pdf.

[5] *See* Peter K. Yu, *The RCEP and Intellectual Property Normsetting in the Asia-Pacific*, September 2017 89 (2017, "Yu"). Available at: https://scholarship.law.tamu.edu/facscholar/1003/.

[6] Yu at 107; Jeremy Malcolm, *RCEP: The Other Closed-Door Agreement to Compromise Users' Rights*, Electronic Frontier Foundation (April 20, 2016), https://www.eff.org/deeplinks/2016/04/rcep-other-closed-door-agreement-compromise-users-rights.

[7] *See* David Meyer, *The 'Right to Be Forgotten,' Globally? How Google Is Fighting to Limit the Scope of Europe's Privacy Law*, Fortune (Sept. 10, 2018), http://fortune.com/2018/09/10/google-eu-court-justice-right-to-be-forgotten/.

limitations, such as the exclusion of ideas and the protection of *scenes a faire*, fair use, and first sale, represent American principles protecting the freedom of information, ideas, and expression.

It should be a core IPEC obligation to insist that access to public information be respected here and abroad.

Support Free Speech By Promoting Fair Use Principles

When cultural and technological innovators seek to build creatively on elements of previously expressed ideas, they often enter what scholars have called "a culture of fear and doubt."[8] Fair use, an exception to liability for infringement,[9] is an American innovation to protect the free expression of ideas – an embodiment of First Amendment principles.[10] It has spurred creativity, innovation, and free expression. In the face of potentially chilling statutory damages, codes of consensus "best practices" based on fair use principles have provided at least some assurance to librarians, documentary film producers, and technological innovators.[11]

Because secondary liability must be based on primary user conduct,[12] the lack of a fair use doctrine can expose U.S. and other OSPs to secondary liability for user-generated conduct – outcomes contrary to our principles. As in the case of safe harbors, the global IP regime is approaching an inflection point, at which American values will be either recognized or constrained globally. ***It should be a part of IPEC's mission to argue for workable outcomes as achieved by U.S. principles such as fair use.***

Importance to democracy movements. Democracy movements in nations important to U.S. trade and security suffer if regional or local law does not recognize fair use or First Amendment principles. Professor Yu discusses an example:

> Since China's resumption of sovereignty over Hong Kong in July 1997**,** the protection of free speech, free press, and other civil liberties in Hong Kong has always been the subject of heightened scrutiny by Western media. Greater freedom in developing UGC would not only protect Hong Kong's much-needed reputation for free speech and free press, but would also enhance Hong Kong's reputation as a city that respects and protects individual freedom. The protection of such freedom is especially urgent following the shocking developments

[8] Patricia Aufderheide and Peter Jaszi, Reclaiming Fair Use, 2d ed.,University of Chicago Press (2018) at 3.

[9] While procedurally a defense, Section 107 explicitly states that a fair use is not an infringement of copyright. Hence for safe harbor purposes fair use is recognized as an exception that must be respected in the first instance. *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (9th Cir. 2015).

[10] Re the interplay between fair use and the First Amendment, *see* Joseph P. Bauer, *Copyright and the First Amendment: Comrades, Combatants, or Uneasy Allies?* 67 Washington & Lee Law Review 831-914 (2010), http://law2.wlu.edu/deptimages/Law%20Review/67-3Bauer.pdf.

[11] *See, e.g., id.* at 4 – 5.

[12] E.g., *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

surrounding the umbrella movement and the increasing discontent among local citizens.[13]

Support U.S. Statutory Damage Reform and Oppose Inordinate Impositions Abroad

Even where limitations, exceptions, and defenses should apply, the mere possibility of out-of-scale statutory damages chills innovative risk-taking to supply new goods and services. In this respect, U.S. law provides an extreme negative example that should not be copied or maintained. As CTA noted in its 2015 Comments, the potential for out-of-scale awards grows along with the scale of the internet itself. The most mundane businesses and services rely on "Big Data" analysis for efficiency, planning, and marketing. This may entail access to and temporary or transformative storage of or linking to a great many works – even for a service offered directly or indirectly by a small business.

CTA has urged statutory damage reform since the time a member manufacturer was obliged to "bet the company" on a paradigm-changing product, the consumer videocassette recorder ("VCR").[14] This product was the first to afford consumers the choice of when and with whom they would enjoy motion picture content. Ultimately the VCR created a new and substantially larger market for content providers. Yet the first company to market VCRs to consumers had to consider that the product's copyright status was a "gray area" in U.S. law, and that therefore the company faced potentially ruinous statutory damages if courts did not agree that it would be legal to distribute this product to consumers. Sony Corporation remained safe from ruin for its innovation and investment by the narrowest possible margin: a five-to-four vote, after rehearing, in the United States Supreme Court. But a smaller pioneer of a successor technology, the Digital Video Recorder ("DVR"), was essentially sued out of business.[15]

The chill of statutory damages has grown alongside courts' consideration of secondary liability, beyond the contributory infringement allegation considered in *Sony*. In *Grokster*[16] the Supreme Court, while essentially preserving Sony's contributory safe harbor for products with commercially significant non-infringing uses, opened the door to "inducement" liability for the same conduct. This doctrine continues to evolve, so remains unclear to innovators and potential plaintiffs alike. Plaintiffs and some courts[17] also continue to bypass the *Sony* safe harbor for

---

[13] Peter K. Yu, *The Quest for a User-Friendly Copyright Regime in Hong Kong*, 32 Am. U. Int'l L. Rev. 283, 305 (2016). Available at: https://scholarship.law.tamu.edu/facscholar/1005. Re the "umbrella movement" see James Griffiths, CNN, *Three years after Umbrella Movement, Hong Kongers back on the streets* (Oct. 1, 2017), https://www.cnn.com/2017/10/01/asia/hong-kong-protest-umbrella/index.html.

[14] *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

[15] *See* Katie Dean, "Bankruptcy Blues for PVR Maker," *Wired* (Mar. 24, 2003), http://archive.wired.com/entertainment/music/news/2003/03/58160.

[16] *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*., 545 U.S. 913 (2005).

[17] *See Disney Enterprises Inc. v. Hotfile Corp.* 2013 U.S. Dist. LEXIS 172339, at *124 – 135 (S.D. Fla. Sept. 20, 2013).

innovation by expanding the doctrine of vicarious liability. In such cases the trend is to seek liability against investors and officers as well as the corporation,[18] exposing them to potential damage claims that would be ruinous for most individuals and families.[19]

CTA continues to urge, as it has to the USPTO in its Green Paper development,[20] that U.S. national and international policy focus on a workable and appropriate statutory damage scale for the range of "gray area" innovation that may now be chilled:

- Widely distributed hardware and software products encounter large numbers of works so innovators are potentially subject to massive claims for statutory damages.

- Online services are threatened by claims of direct as well as secondary liability.

- The innovation threatened is that of small businesses and startups as well as of established companies, and concerns data as well as entertainment.

The potential of statutory damage claims in marginal cases to chill innovation and entry has been well documented through exhaustive study,[21] yet the benefits of giving plaintiffs the statutory damage weapon in "gray area" cases has been scarcely documented, because current law does not require any threshold determination that the remedy is appropriate to the case.[22] In particular, proponents of the *status quo* must come forward with evidence suggesting that the application of statutory damage claims to service providers, where such awards can amount to trillions of

---

[18] *Id.* at 134 – 147.

[19] *See* Michael A. Carrier, *Copyright And Innovation: The Untold Story*, 2012 Wisconsin L. Rev. 891 (2012). Carrier's research "underscores the dramatic effects of statutory damages, which can reach billions of dollars. It offers first-hand accounts of innovators who found themselves on the receiving end of personal lawsuits. It shows how the labels exploited a lack of legal clarity to promote their goals. And it highlights some of the industry's threats to innovators who sought to create legal alternatives to distribute digital music." *Id*. at 896. *See also* Pamela Samuelson, Phil Hill, &Tara Wheatland, "Statutory Damages: A Rarity in Copyright Laws Internationally, But For How Long?*" Journal of the Copyright Society of the U.S.A.*, Mar. 27, 2013, UC Berkeley Public Law Research Paper No. 2240569, "Statutory damages have often been criticized as 'arbitrary, inconsistent, unprincipled, and sometimes grossly excessive.' U.S. courts have failed to develop guidelines to ensure that these awards actually are just, and many times they are not. Virtually all of the law review literature in the United States has criticized the U.S. statutory damage regime. And yet, the United States has insisted upon exporting this 'extraordinary' remedy to other nations through bilateral and plurilateral treaties, as well as other mechanisms." Electronic copy at 1 -2, note omitted.

[20] CTA's November 13, 2013 presentation to the PTO in its Docket No. 130927852-3852-01.

[21] Carrier, *id.* at 48.

[22] Samuelson *et. al, id.*, IV.B.

dollars, actually provides meaningful marginal deterrence value.[23] Anecdotal accounts suggest that some of the most publicized judgments are far in excess of what defendants are able to pay, which again raises questions about the marginal deterrence value of these massive sanctions.[24] A focus of discussion, therefore, should also be whether and to what extent the availability of statutory damages actually does provide a deterrent against calculated infringement of copyright.

IPEC should support appropriately scaled relief here and abroad. Excessive statutory awards are a tool that can be used against U.S. policy and commercial interests around the world.

Oppose U.S. and Foreign "Backdoor" Access To Private Communications

It is ironic that just as governments consider measures such as the "Right To Be Forgotten" in the name of "privacy," they *also* consider measures such as mandated "backdoors" to encryption, which do pose a severe threat to both personal and corporate privacy and secrecy. While the U.S. has periodically backed away from looking to impose "back doors" for official inspection of encrypted transmissions,[25] it has now joined other jurisdictions in considering the idea.[26] Such "backdoors" lessen confidence in both security and government.[27] ***Official access to private communications poses risks beyond any potential benefit. The risk to U.S. interests is even greater if deployed by overseas entities and governments.***

---

[23] "[I]nevitably, if the jury gets the sense that the defendant acted wrongfully in the specific situation before them, they will be tempted to award substantial statutory damages considerably disproportionate to what might be necessary for purposes of deterrence. … The result is damages awards in copyright infringement cases that are sometimes significantly greater than any conceivable actual damages the plaintiff could have obtained if the plaintiff had elected actual damages, and that do not appear consistent with any ·principle of any kind." Hon. Jed S. Rakoff, "Copyright Damages: A View From the Bench," Forty-Fourth Annual Donald C. Brace Memorial Lecture, Nov. 3, 2014, 62 *Journal of the Copyright Society* 377, 380 (2015).

[24] *See, e.g., Columbia Pictures Indus., Inc. v. Fung*, No. 2:06-cv-05578-SVW-JC, Defendants' Supplemental Brief Regarding Jury Instructions at 14 – 15 (C.D. Cal. Oct. 10, 2013) "Plaintiffs are attempting to avoid ever having to provide discovery about the value of and damages for particular works ….".

[25] *See* Ellen Nakamura and Andrea Peterson, "Obama administration opts not to force firms to decrypt data — for now," *Washington Post* (October 8, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[26] Zack Whittaker, '*Five Eyes*' *governments call on tech giants to build encryption backdoors — or else*, TechCrunch (Sept. 3, 2018), https://techcrunch.com/2018/09/03/five-eyes-governments-call-on-tech-giants-to-build-encryption-backdoors-or-else/.

[27] *See* Phil Muncaster, *Crypto-Experts Slam FBI's Backdoor Encryption Demands*, infosecurity (Feb. 15, 2018), https://www.infosecurity-magazine.com/news/cryptoexperts-slam-fbis-backdoor/.

Oppose Data Localization

Data localization regimes are trade restraints on successful international companies. They impede operations and growth of U.S. OSPs without any public benefit, here or abroad. As a recent analysis pointed out:

> Localization barriers make it harder for domestic firms to use data from overseas operations, which prevents them from using the centralized IT and analytical platforms at the heart of data-driven innovation and trade. Localization barriers discriminate against U.S. firms that use foreign data services by forcing them to use or set up local services when they otherwise would not, creating duplicative costs for businesses.[28]

In addition to hobbling international law enforcement,[29] data localization helps governments stifle dissent. For example, Vietnam, with a long history of stifling on-line dissent, is now requiring OSPs to store data locally, where it will be accessible to authorities wishing to profile citizens and monitor their activities and expression.[30]

The United States and its North American partners banned both data and facilities localization in the USMCA.[31] ***IPEC should now defend American law enforcement and First Amendment principles by opposing data localization everywhere.***

Support A Direct Right of Action Against Overseas Infringers

Complaints directed at lawful conduct of U.S. OSPs and providers of consumer electronics products are often directed, in reality, at the conduct of offshore servers providing pirated content. U.S. law and courts have rightly rejected the option of punishing the providers of lawful goods and services, or, as discussed above, requiring them to filter goods or services against possible misuse. While in theory it is possible to pursue overseas pirates in U.S. courts,[32] it is seldom practicable in the context of overseas servers. A direct right of action for U.S. rights proprietors under foreign law could make meaningful relief possible. ***It should be an objective of IPEC to establish such rights for U.S. interests.***

---

[28] Nigel Coery and Alan McQuinn, *Will the US capitalize on its opportunity to stop data localization?* The Hill (Sept. 9, 2018), https://thehill.com/opinion/cybersecurity/405422-will-the-us-capitalize-on-its-opportunity-to-stop-data-localization.

[29] *Id.*

[30] *See* Mike Masnick, *Vietnam Expands Decades Long Effort To Crack Down On Any Dissent Online By Demanding Data Be Kept In The Country*, TechDirt (Oct. 19, 2018), https://beta.techdirt.com/articles/20181015/16230840845/vietnam-expands-decades-long-effort-to-crack-down-any-dissent-online-demanding-data-be-kept-country.shtml.

[31] Articles 19.11(1) and 19.12. *See* Jacqueline Yin, *Cross-border Data Continues to Flow under the USMCA*, DISCO (Oct. 5, 2018), http://www.project-disco.org/21st-century-trade/100518-cross-border-data-under-the-usmca/.

[32] *See, e.g., Los Angeles News Service v. Conus Communications Co. Ltd.,* 969 F. Supp. 579 (C.D. Cal 1997); *Shropshire v. Canning,* 809 F. Supp. 2d 1139 (N.D. Cal 2011).

Enhance Measures Against Counterfeit Products

As noted at the outset, CTA has long encouraged IPEC's mission of keeping counterfeit products off U.S. markets. CTA applauds IPEC's efforts and provides, below, an updated summary of its recommendations for enhancement, as shared with the Senate Judiciary Committee on June 29 of this year:

- **Access to government data on counterfeiting.** A prime CTA recommendation has been that, in order to warn consumers, businesses should have ready access to warnings compiled by Customs and other authorities. As CTA advised IPEC, "government customs and enforcement officials must share information and analysis with the makers and sellers of legitimate products that are counterfeited, and vice versa."[33]

- **Consumer, dealer, and law enforcement education.** CTA manufacturer members use a range of strategies to inform to consumers, dealers, repair professions and law enforcement about counterfeiting challenges. These include training sessions for customs and border officials, social media outreach, and the production of instructional videos.

- **Defensive product identification, authentication, and tracking.** New technologies such as blockchain create opportunities for protecting legitimate supply chains. Tools are available for tracking and identification, component analysis, and the mutual sharing of information with customs and enforcement officials, to avoid non-authentic components from infiltrating final product supply chains, and to avoid counterfeits invading retail streams of commerce.[34]

- **Worldwide enforcement as to goods in transit.** According to the French Association Against Counterfeiting, a 2009 European court decision has meant that "most customs regulations do not apply to goods, counterfeit or otherwise, in transit. … Since this case, there has been a 65 percent decrease in seizures of infringing goods as well as an increase of counterfeiting trade in and out of the European market (European Commission, 2014)."[35]

- **Consumer education and officials' training.** According to the National Intellectual Property Rights Coordination Center, consumer education and awareness on intellectual property issues should focus more on counterfeit goods, and their potential for social and economic damage. Such training should include consumer awareness, as well as appreciation of harm. Similarly officials need to be trained to identify and take action, and consumer and official awareness programs need to be coordinated.[36]

---

[33] *See, e.g.*, the compendium published by Jeremy M. Wilson, director of Michigan State University's Center for Anti-Counterfeiting and Product Protection ("Wilson"), "Brand Protection 2020 – Perspectives on the Issues Shaping the Global Risk and Response to Product Counterfeiting" (hereinafter, "A-CAPP Symposium") (September, 2015), at 3.

[34] *Id.*, e.g., at 4, 26.

[35] *Id.* at 14 – 15, submission of Christian Peugeot, President, Union des Fabricants.

[36] *Id.* at 16 – 17, 25 – 26.

- **Accurate CPSC product attribution.** Counterfeits are sometimes mistakenly attributed to the legitimate manufacturer when listed in the CPSC's public database www.saferproducts.-gov. Unfortunately, CPSC sometimes publishes consumer complaints even when product identification (i.e. counterfeit or legitimate) is highly questionable. Even when the legitimate manufacturer protests and asks that the report of counterfeit-caused harm be excluded, CPSC generally moves forward with publication if the manufacturer cannot definitively show that the counterfeit another manufacturer's product. More, the CPSC sometimes publishes a report even where the evidence (e.g., the counterfeit itself) isn't preserved for examination.

- **Litigation against counterfeit sellers.** eCommerce requires new partnership strategies among brands, marketplace providers, and authorities. In a recent example,[37] a product designer received notices from border agents, and notified the eCommerce marketplace provider, Amazon. The designer, Vera Bradley, sued the seller for infringement, whereas the marketplace provider, Amazon, sued the seller for breach of contract and impounded the goods still in warehouse. Similarly, Alibaba has instigated litigation against counterfeiters in connection with multiple brands on the grounds of breach of contract and harm to reputation. In one particularly noteworthy case in China, Alibaba successfully established that counterfeit sellers can be liable to the platform whose services they misuse in connection with the sale of counterfeit goods.[38] However, as was noted at the Committee hearing referenced in the Senate Finance Committee May 30, 2018 letter to stakeholders, there are presently restrictions on the amount of information that authorities can share with brand owners and e-commerce companies.[39] Congress and enforcement authorities should ensure that brands owners and e-commerce companies have access to information to act quickly against counterfeiters.[40]

- **Brand registry and best practices.** Establishing best practices, such as a brand registry initiative, takes testing and balancing against drawbacks, such as additional burdens for private label sellers.[41] It also requires continuous private and public sector outreach.[42] More,

---

[37] Monica Nickelsburg, *Amazon files lawsuits over counterfeit Vera Bradley purses and Otterbox phone cases*, Geekwire (March 8, 2018), https://www.geekwire.com/2018/amazon-files-lawsuits- counterfeit-vera-bradley-purses-otterbox-phone-cases/.

[38] Alexis Kramer, *Alibaba Wins Suit Over Allegedly Fake Cat Food*, Bloomberg Law **(**July 21, 2017), https://www.bna.com/alibaba-wins-suit-n73014462276/.

[39] Statement of Kimberly Gianopoulos, Director, International Affairs and Trade (March 6, 2018) at 9.

[40] Statement of Kimberly Gianopoulos, Director, International Affairs and Trade, March 6, 2018, at 9.

[41] *See, e.g.*, Kym Ellis, JungleScout, *Navigating the New Amazon Brand Registry* (July 11, 2017), https://www.junglescout.com/blog/new-amazon-brand-registry/.

[42] *See, e.g.*, Progress Report, https://brandservices.amazon.com/progressreport.

it is important that online marketplaces providing third party sellers a platform for commerce also facilitate prompt and effective removal of products that enable unsafe use or abuse. In 2017, Amazon launched a Brand Registry service that provides rights holders with text-and image-based search capabilities and automated protections that use machine learning to predict and prevent future defects. The 60,000 brands already enrolled in this service are finding and reporting 99% fewer suspected infringements than before its launch.[43] Some registries, including Amazon's Brand Registry, now include tools to proactively remove infringing listings, reducing the burden on rights holders to file reactive notices on potential counterfeits.

- **Cooperation with foreign governments.** The USTR 2017 Out-of Cycle Review of Notorious Markets[44] noted as "positive developments" since the 2016 review that several foreign governments and registrars – UK, Netherlands, Spain, the EU – had taken positive steps as to online markets, and others – Argentina, Thailand – with respect to physical markets. This opens the door for enhanced private sector partnerships. Countries such as India have also set up registries and made tools available.[45]

CTA appreciates this opportunity to provide its views.

Respectfully submitted,

Michael D. Petricone
Senior Vice President
Government Affairs

[43] Amazon Brand Registry Progress Report, https://brandservices.amazon.com/progressreport.

[44] USTR, Executive Office of the President, at 4 – 8, https://ustr.gov/sites/default/files/files/Press/Reports/2017%20Notorious%20Markets%20List%201.11.18.pdf.

[45] Anurag, *10 Myths About India on Counterfeiting*, TradeVigil (Sept. 13, 2017), https://www.-tradevigil.com/10-myths-india-counterfeiting/.