Statement of Dean S. Marks
Executive Director and Legal Counsel
Coalition for Online Accountability

Before the
**SENATE COMMITTEE ON THE JUDICIARY**
**SUBCOMMITTEE ON INTELLECTUAL PROPERTY**

Hearing: "The Role of Private Agreements and Existing Technology in Curbing Online Piracy"

December 15, 2020

Thank you, Chairman Tillis, Ranking Member Coons and members of the Subcommittee on Intellectual Property, for your inquiry into the efficacy of the Digital Millennium Copyright Act ("DMCA") and the hearings you have held on various aspects of the DMCA over the course of this year. I thank you for the honor of being invited to testify at today's hearing on "The Role of Private Agreements and Existing Technology in Curbing Online Piracy."

My name is Dean Marks and I am Executive Director of the Coalition for Online Accountability ("COA"), a group of major copyright industry companies, trade associations and performing rights organizations. COA focuses on representing copyright interests with respect to policy issues in the internet domain name space, including those developed and implemented by the Internet Corporation for Assigned Names and Numbers ("ICANN"). Prior to my work with COA, I served as Deputy General Counsel and Chief of Global Content Protection for the Motion Picture Association ("MPA")[1] and before MPA over 25 years as an intellectual property attorney for Time Warner—now WarnerMedia. While my work for these various entities has shaped my perspectives on the DMCA and the issue of voluntary measures, the views expressed in this testimony are my own and do not necessarily reflect the policy positions of COA members, MPA or WarnerMedia.

**Introduction**

As you have likely heard many times during the course of these DMCA hearings, there is no "silver bullet" to the challenge of copyright piracy, particularly in the online environment. Rather, a multi-pronged approach must be embraced. This includes effective laws that provide ready civil remedies, productive and practical tools and criminal penalties. It also requires government agencies willing to combat piracy through investigations and prosecutions. Another important prong consists of innovative and collaborative government law enforcement programs that take input from the private sector such as the IPR Center's "Operation Intangibles" and most recently the Digital Piracy MOU entered into in September 2020 designed to supplement Homeland Security Investigations ("HSI") digital piracy investigations.[2] These programs serve as shining examples of public-private partnership; they should be both commended and further encouraged.

[1] Formerly called the Motion Picture Association of America ("MPAA")
[2] See IPR Center "Motion Picture Association signs up to assist the IPR Center with anti-piracy efforts"https://www.iprcenter.gov/news/motion-picture-association-signs-up-to-assist-the-ipr-center-with-anti-piracy-efforts

I would like to share with the Subcommittee the great privilege I had during my tenure with the MPA of collaborating with extremely talented, dedicated, and effective U.S. government officials to take down one of the most prominent copyright piracy peer-to-peer torrent sites, the operators of which were based overseas. In particular, this success could not have been achieved without the brilliant work, tenacious efforts and collaborative approach of HSI special agent Jared Der-Yeghiayan, who led the investigation.[3]

While such government action is absolutely critical in the fight against copyright piracy, by itself it is not sufficient. Other paths must also be pursued including civil litigation and the topic of today's hearing: voluntary measures.

**The DMCA and Incentives for Voluntary Measures**

From the testimony of other witnesses, you have heard how the DMCA Section 512 safe-harbors and the notice and takedown regime, particularly as these provisions have been interpreted by the courts, have largely resulted in an expensive and rather ineffective "whack-a-mole" endless cycle of sending millions of takedown notices and subsequent re-postings of copyright infringing files. The Copyright Office came to the same conclusion in its May 2020 report on Section 512.[4] Furthermore, others have explained that Section 512 has not fostered the high level of cooperation and engagement that Congress expected it to achieve between copyright owners and digital service providers of all kinds to develop voluntary and pragmatic measures to fight online piracy. While I largely agree with those assessments, I submit that tangible progress has been achieved with respect to voluntary measures and great potential exists to expand such measures.

When it comes to these voluntary measures, it is clear how copyright owners benefit from them but some may ask why service providers adopt them absent either a very credible risk of direct or secondary liability or a "sword of Damocles" threat of legislation or regulation. Congress certainly intended Section 512 to create strong incentives for service providers to take proactive steps in collaboration with copyright owners to curb online piracy.[5] Unfortunately, as noted by the Copyright Office in its report on Section 512, the statute has fallen short of this goal and instead has largely created "a static system that locked in place the anti-piracy toolkit of the 1990s."[6] Nonetheless, some incentives remain for service

[3] See Will Ockenden, ABC News "Kickass Torrents: How did the US Government bring down this file-sharing site?" (July 21, 2016) "Until today, Kickass Torrents (KAT) was one of the most visited websites on the internet and brought in tens of millions of dollars a year in advertising. Now the website is no more. It has disappeared from the internet and its 30-year-old alleged founder and operator, Ukranian (sic) Artem Vaulin, has been arrested and is facing extradition to the United States. The domain names KAT used—and there are several—are in the process of being seized by the US Government. It was the result of years of investigation by Jared Der-Yeghiayan, a special agent with the US Department of Homeland Security." https://www.abc.net.au/news/2016-07-21/how-the-us-government-brought-down-kickass-torrents/7649862

[4] The Copyright Office stated "the notice-and-takedown system does not effectively remove infringing content from the internet; it is, at best, a game of whack-a-mole." See U.S. Copyright Office, "Section 512 of Title 17: A Report of the Register of Copyrights" (May 2020) at page 33 https://www.copyright.gov/policy/section512/section-512-full-report.pdf

[5] See, e.g., Conference Report, H.R. Report No. 105-796 at page 72 (1998) https://www.congress.gov/105/crpt/hrpt796/CRPT-105hrpt796.pdf

[6] U.S. Copyright Office, "Section 512 of Title 17: A Report of the Register of Copyrights" (May 2020) at page 66: https://www.copyright.gov/policy/section512/section-512-full-report.pdf

providers to engage in voluntary initiatives. For example, pirate websites and illicit apps designed to stream infringing content pose a much higher risk of malware, ransomware, identity theft and other types of cyberattacks than legitimate websites and devices. Therefore, service providers sometimes appreciate that facilitating the operations of pirate websites and apps may cause consumer backlash. A recent study indicated that consumers using pirate devices are three times more likely to encounter malware and other cyberattacks than those who do not use such devices.[7] Last year the Federal Trade Commission issued a warning to consumers that "purveyors of pirated content are now spreading apps and add-ons that work with popular streaming devices. If you download one of these illegal pirate apps or add-ons, the chances are good that you'll also download malware."[8] Similarly, a study of piracy websites by RiskIQ and the Digital Citizens Alliance found that one out of every three piracy websites contained malware and that consumers are twenty-eight times more likely to get malware from a piracy website than on similarly visited mainstream websites.[9] Clearly for end users, piracy websites, apps and services pose significant harmful risks of which they are often unaware. In its 2019 Review of Notorious Markets for Counterfeiting and Piracy, the U.S. Trade Representative devoted an entire section of its report to the close nexus between malware and online piracy.[10] Given these significant risks to end users, legitimate service providers understand that if their services can be viewed by consumers as supporting sources of direct harm to consumers, (such as malware and cyberattacks), then that may well tarnish the reputation and brand of such services.

An appreciation of these risks was a significant factor in the successful and ongoing online advertising voluntary effort known as the Brand Integrity Program Against Piracy under the direction of the Trustworthy Accountability Group ("TAG"). Major companies understood that they did not want their name and brand associated with piracy websites that were not just illegal in nature, but also risked significant harm to end users from malware. Major online advertising agencies and placement services also realized that, in response to their clients' demands, they needed to undertake effective processes and safeguards in order to ensure that their clients' ads did not appear on pirate websites. The TAG Brand Integrity Program Against Piracy was built upon active collaboration with organizations with significant knowledge of and expertise in online piracy, such as the MPA, the Recording Industry Association of America ("RIAA"), Independent Film & Television Alliance ("IFTA"), Copyright Alliance, and CreativeFuture.[11] This collaboration has continued and as a result advertising revenue to piracy sites has

[7] See Digital Citizens Alliance, "As More Americans Turned to Streaming Entertainment During Coronavirus Cyber-attacks from Use of Piracy Devices Increases, New Survey Finds" (June 22, 2020) https://www.digitalcitizensalliance.org/news/press-releases-2020/as-more-americans-turned-to-streaming-entertainment-during-coronavirus-cyber-attacks-from-use-of-piracy-devices-increases-new-survey-finds/

[8] Alvaro Puig, FTC, "Malware from illegal video streaming apps: What to know" (May 2, 2019) https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know

[9] Digital Citizens Alliance, "Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack Into Internet Users' Computers and Personal Data" (December 2015) See page 4 for summary of findings: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf

[10] See "Issue Focus: Malware and Online Piracy" at pages 8-11 of the 2019 Notorious Markets Report: https://ustr.gov/sites/default/files/2019_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy.pdf

[11] TAG, "Advertising Industry Launches Initiative to Protect Brands Against Piracy Websites" (February 10, 2015). This announcement of the launch of the program by TAG identifies the cooperating parties https://www.tagtoday.net/pressreleases/advertising-industry-launches-initiative-to-protect-brands-against-piracy-websites

been significantly reduced.[12] One of the key benefits of voluntary efforts like the TAG Brand Integrity Program Against Piracy is the flexibility to adapt as the forms of online piracy change. For example, in 2015 when the Program launched, peer-to-peer and torrent websites were the major sources of online piracy for film and television content. Now illegal streaming subscription services and pirate streaming apps are the main piracy challenges facing the film and television industry. Through the ongoing collaboration described above, the TAG Program has evolved and now covers pirate apps and streaming services to divert advertising revenues away from them.[13]

**Trusted Notifier Agreements with Domain Name Registries**

The voluntary measures about which I have the most personal knowledge are the Trusted Notifier agreements that the MPA put in place with domain name registries Donuts and Radix in 2016. Under these arrangements, the MPA sends referrals of websites with pervasive copyright infringement operating under a top-level domain administered by the registry. The registry then examines the referral and if it agrees, it will suspend or lock the domain name of the pirate website, which essentially makes the website no longer visible or readily available on the internet. Before sending a referral to the registry, the MPA must first alert and seek redress with the relevant registrar of the domain and hosting provider of the pirate website. A report issued earlier this year by the Information Technology & Innovation Foundation describes these particular Trusted Notifier agreements in greater detail.[14]

I negotiated the Trusted Notifier agreements on behalf of MPA with Donuts and Radix and would like to share some of my insights with respect to the process of creating these particular voluntary measures. First, Donuts and Radix both saw benefits to making their top-level domains as places for legitimate websites and commerce where pirate and other websites engaged in illegal activity were neither welcomed nor ignored. Thus, complimentary incentives existed motivating both the online service provider and the copyright owners. Even with these complimentary incentives forming a foundation, however, the agreements did not come together in a matter of days or weeks. Rather, they were the result of several months of ongoing conversations.

Second, each party listened to the other party's concerns and priorities with openness and patience and genuinely sought to understand each other's perspectives. Third, the ongoing conversations served to build a relationship of respect, trust and confidence. While this factor may be the least concrete, it was critical to "closing the deal" and to sustaining the ongoing arrangement. Finally, the arrangement was purely a voluntary one with no compensation express or implied.

---

[12] Indeed, an Ernst & Young analysis published in September 2017 found that just in 2016—one year from the launch of the TAG Brand Integrity Program Against Piracy—the Program resulted in an estimated $102 to $177 million reduction in advertising revenues flowing to pirate websites from the U.S. online advertising market alone. See in particular pages 3 and 4 of the Ernst & Young report "Measuring digital advertising revenue to infringing sites" (September 2017) https://www.tagtoday.net/hubfs/Measuring%20digital%20advertising%20revenue%20to%20infringing%20sites.pdf?t=1507150221706

[13] See description of TAG's Pirate Mobile App List at TAG, "Promote Brand Safety" https://www.tagtoday.net/brand-safety#pmal

[14] Nigel Cory, ITIF, "How Voluntary Agreements Among Key Stakeholders Help Combat Digital Piracy" (February 24, 2020) at pages 3-5 https://itif.org/publications/2020/02/24/how-voluntary-agreements-among-key-stakeholders-help-combat-digital-piracy

**So Called "Shadow Regulation" Objections to Voluntary Measures**

When the first Trusted Notifier agreement was finalized with Donuts in February 2016, both parties agreed to make a joint public announcement.[15] The following day the Electronic Frontier Foundation ("EFF") published an article criticizing the arrangement as "censorship" and stating "expect to see MPAA and other groups of powerful media companies touting the Donuts agreement as a new norm, and using it to push ICANN and governments towards making all domain name registries disable access to an entire website on a mere accusation of infringement."[16] Over time, EFF and others began to label these and other voluntary measures as "shadow regulation." The main objections the "shadow regulation" advocates make are: (i) voluntary measures amount to content regulation and "censorship," (ii) such measures do not involve due process or court orders, and (iii) the arrangements are not transparent, lack public accountability and do not involve the participation of civil society groups such as EFF.[17]

Clearly, free speech is a critical value and right to be safeguarded online. But I strongly disagree with the "shadow regulation" objections that have been raised about the Trusted Notifier agreements and other voluntary measures to combat online piracy for the following reasons. First, wholesale copyright infringement is not protected by the First Amendment; rather it is exploitative illegal activity. In the copyright area, there are certainly sometimes grey areas between infringement and fair use and well-versed copyright lawyers and scholars often disagree about where the proper line is to be drawn between fair use and infringement. But the websites and online activities that are subject to voluntary measures, such as the Trusted Notifier agreements, are far removed from these grey areas and instead involve pervasive and wholesale infringement of copyrighted works for illicit gain. Removing pirate websites simply does not impinge on free speech or amount to content regulation. As the co-founder and Executive Vice President of Donuts, Jon Nevett, stated when concerns were raised directly with him about potential content regulation resulting from the Trusted Notifier agreement with MPA, Donuts "is not interested in content regulation, but in regulation of crime in its domain extensions, whether that is child imagery abuse or theft [of copyrighted materials]."[18]

Second, court orders are not necessary for an online intermediary or service provider to terminate its service to a customer when that customer violates the terms of the contract with the service provider. Take the example of domain names. ICANN requires in its accreditation agreement with domain name

---

[15]Donuts, MPAA "Donuts and the MPAA Establish New Partnership to Reduce Online Piracy" (February 9, 2016) https://www.motionpictures.org/wp-content/uploads/2016/02/Donuts-and-MPAA-Establish-New-Partnership-2.9.16.pdf

[16]Mitch Stoltz, EFF, "MPAA May Like Donuts, But They Shouldn't Be the (Copyright) Police" (February 10, 2016) https://www.eff.org/id/deeplinks/2016/02/mpaa-may-donuts-they-shouldnt-be-copyright-police

[17]See, e.g., Jeremy Malcolm, Mitch Stoltz, EFF, "Shadow Regulation: the Back-Room Threat to Digital Rights" (September 29, 2016) https://www.eff.org/deeplinks/2016/09/shadow-regulation-back-room-threat-digital-rights and Dugie Standeford, Intellectual Property Watch, "ICANN Is Moving Toward Copyright Enforcement, Academic Says" (February 28, 2017) https://www.ip-watch.org/2017/02/28/icann-moving-toward-copyright-enforcement-academic-says/

[18]Dugie Standeford, Intellectual Property Watch, "ICANN Is Moving Toward Copyright Enforcement, Academic Says" (February 28, 2017) "The registry's partnership with the MPAA 'has been helpful in combating online crime in the form of pervasive theft of copyrighted materials,' Nevett told *Intellectual Property Watch*. 'It is not interested in content regulation, but in regulation of crime in its domain extensions, whether that is child imagery abuse or theft,' he said." https://www.ip-watch.org/2017/02/28/icann-moving-toward-copyright-enforcement-academic-says/

registries that downstream contracts with domain name registrants prohibit them "from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."[19] Therefore, when a company or individual acquires a domain name—and becomes a domain name registrant—they sign a contract and agree not to use the domain name to engage in prohibited activity, including copyright infringement. When a customer breaches a contract, a court proceeding or order is not required to terminate the contract. As an obvious example, if a cable television subscriber stops paying his or her bill, the cable company will cut off service; the company doesn't need to wait until a court determines that the contract has been breached and termination is warranted. Typically, terms of use in contracts with online service providers of all kinds prohibit customers from engaging in illegal activity via their services and reserve the right of the service provider to terminate service if the customer does so. Thus, voluntary measures entered into by copyright owners with such service providers (such as the Trusted Notifier arrangements with Donuts and Radix) do not change the terms, expectations or reliance of customers with respect to their contracts with such service providers. Rather, these voluntary measures function to provide the online service provider with information and insight about activity of which they are likely unaware so they can better enforce their own contracts and terms of use.

Notwithstanding the foregoing, the "shadow regulation" advocates argue that neither a copyright owner nor a service provider should be permitted to determine what constitutes copyright infringement and that such a determination may only be made by a federal court. But federal case law with respect to Section 512 of the DMCA firmly rejects this assertion. Under Section 512(i)(1)(A), the safe harbor limitations on liability are conditioned on the service provider's adoption and reasonable implementation of a policy that "provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers[.]" In the case BMG Rights Management v. Cox Communications, 881 F.3d 293 (4th Cir. 2018), Cox Communications argued that only customers who had been adjudicated by a court for multiple instances of copyright infringement could be considered "repeat infringers" for purposes of Section 512. Both the District Court and Fourth Circuit Court of Appeals soundly rejected that argument. In its opinion, the Fourth Circuit held that "the term 'infringer' in Section 512 is not limited to adjudicated infringers" and explained that "the risk of losing one's Internet access would hardly constitute a 'realistic threat' capable of deterring infringement if that punishment applied only to those *already* subject to civil penalties and legal fees as adjudicated infringers." (emphasis in original)[20] In its May 2020 Report on Section 512, the U.S. Copyright Office came to the same conclusion. The Copyright Office stated that requiring a subscriber to be held by a court to have infringed copyright in order to qualify as an infringer "seems wholly out of step with a system explicitly premised on a non-judicial resolution of infringement

[19] See pages 97-98 of ICANN Registry Agreement at:
https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf
[20] BMG Rights Management v.Cox Communications, 881 F.3d 293 at 302 (4th Cir. 2018)
https://law.justia.com/cases/federal/appellate-courts/ca4/16-1972/16-1972-2018-02-01.html

claims. And, as the Fourth Circuit noted in *Cox*, nowhere else in the Copyright Act is "infringer" used to refer only to adjudicated infringers. *Cox*, 881 F.3d at 301"[21]

Clearly Congress intended that court adjudicated infringement is not a prerequisite for an online service provider to terminate service to a customer. Indeed, requiring service providers to terminate customers engaged repeatedly in copyright infringement without the need for any court ruling of infringement was established by Congress as a key condition for qualifying for the Section 512 liability safe harbors. Therefore, it defies logic, Congressional intent and the law to contend that voluntary measures that bring evidence and information about copyright infringement to service providers' attention so that such service providers may act to suspend or terminate services somehow violate due process because such voluntary measures are not restricted to court adjudicated infringers.

Finally, in terms of transparency and accountability, voluntary measures such as the Trusted Notifier agreements MPA entered into with Donuts and Radix are often made public.[22] Not only did MPA and the relevant registries make public announcements, but shortly thereafter MPA and Donuts jointly released a document entitled "Characteristics of a Trusted Notifier Program," a copy of which is attached as Annex A to this Statement. The TAG initiatives described earlier are also transparent. Although the EFF and others dub TAG as "shadow regulation," TAG operates a publicly accessible website that is entirely devoted to explaining its various programs, guidelines and certifications.[23]

Those seeking to combat online copyright piracy are not alone in disputing the "shadow regulation" narrative. Earlier this year, the Information Technology & Innovation Foundation ("ITIF") published a report entitled "How Voluntary Agreements Among Key Stakeholders Help Combat Digital Piracy." In addressing the "shadow regulation" arguments, the ITIF stated "EFF and likeminded academics seem only interested in inaction, as they see efforts to limit piracy as an attack on their view of Internet freedom, and digital rights as license, not responsibility."[24] Paul Vixie, computer scientist and Internet Hall of Fame Innovator who designed software protocols and applications related to the domain name system,[25] wrote an article in 2017 praising the Donuts – MPA Trusted Notifier arrangement and rebutting point-by-point the "shadow regulation" arguments from both a technical and internet governance perspective. He stated "every representative of every economy and every industry has clamoured—and reasonably so!—for better accountability and recourse among Internet participants."[26]

**Potential for Further Expanding Trusted Notifier Agreements**

While the Trusted Notifier agreements put into place with Donuts and Radix have been successful, I was disappointed that MPA and other organizations with copyright and anti-piracy expertise met resistance

[21] Footnote 523 of page 99 of Copyright Office Section 512 Report https://www.copyright.gov/policy/section512/section-512-full-report.pdf

[22] Not all voluntary measures are made public for various reasons, including avoiding giving pirates a roadmap for evading such measures.

[23] See: https://www.tagtoday.net/

[24] Nigel Cory, ITIF, "How Voluntary Agreements Among Key Stakeholders Help Combat Digital Piracy" (February 24, 2020) at page 12: https://itif.org/publications/2020/02/24/how-voluntary-agreements-among-key-stakeholders-help-combat-digital-piracy

[25] See "Internet Hall of Fame: Inductees" https://www.internethalloffame.org//inductees/paul-vixie

[26] Paul Vixie, CircleID, "Notice, Takedown, Boarders, and Scale" (March 1, 2017) http://www.circleid.com/posts/20170301_notice_takedown_borders_and_scale/

to such voluntary measures from other major domain name registries, particularly Verisign—a U.S. publicly traded company—and the registry for the majority market share top level domains of .com and .net, among others.

In November 2018, the National Telecommunications and Information Administration ("NTIA") announced, in connection with its extension of its cooperative agreement with Verisign, that "NTIA looks forward to working with Verisign and other ICANN stakeholders in the coming year on trusted notifier programs to provide transparency and accountability in the .com top level domain."[27] Unfortunately, to my knowledge, Verisign did not adopt any trusted notifier programs in 2019—certainly none related to copyright piracy. In its 2019 Review of Notorious Markets for Counterfeiting and Piracy, the U.S. Trade Representative identified twenty-three piracy websites, including cyberlockers, torrent sites, and stream ripping sites.[28] Of these twenty-three piracy websites identified, thirteen were located on .com or .net domain names, all administered by Verisign. But even on the basis of a U.S. government report, Verisign will not suspend the domain names of websites devoted to copyright piracy or counterfeiting absent an explicit court order to do so. This flies in the face of the collaboration that the DMCA was supposed to encourage and the observation of the U.S. Trade Representative in the 2019 Notorious Markets Report that "platforms need to take additional actions to combat trafficking in counterfeit and pirated goods[.]"[29] Indeed, the situation with respect to copyright piracy, counterfeiting and illegal activity of all kinds online has become more difficult since May 2018 when the WHOIS directory of domain name registrant contact information essentially went dark.[30] This was a result of ICANN's misapplication of the European Union's General Data Protection Regulation and has created obstacles to investigations of online illegal activity by both private parties, such as copyright owners, and government agencies such as law enforcement and even European Data Protection authorities.

Earlier this year, the Department of Commerce and the Department of Health and Human Services announced a Trusted Notifier program with Verisign, Neustar and Public Interest Registry involving websites illegally selling opioids.[31] Under this voluntary program, the Food and Drug Administration serves as a trusted notifier and sends referrals of such websites to the relevant registry that administers the domain name under which the website operates. The registry will then review the referral and suspend, lock or place the domain on hold. This evolution of the Trusted Notifier program is a positive step forward in terms of curbing the online sale of illegal opioids. Perhaps if the Department of

---

[27] NTIA Statement on Amendment 35 to the Cooperative Agreement with Verisign (November 1, 2018) https://www.ntia.doc.gov/press-release/2018/ntia-statement-amendment-35-cooperative-agreement-verisign

[28] This number does not include the e-commerce platform sites and hosting services that the Report identified. See pages 13-32 of 2019 Notorious Markets Report at: https://ustr.gov/sites/default/files/2019_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy.pdf

[29] Ibid. at page 14

[30] From the earliest days of the internet until May 2018, WHOIS data was publicly accessible. Congress has recognized the challenges and dangers that the current lack of access to WHOIS poses. As stated in H. Res.875—116th Congress (2019-2020) (introduced 02/27/2020) "domain name registration information, referred to as 'WHOIS' information, is critical to the protection of the United States national and economic security, intellectual property rights enforcement, cybersecurity, as well as the health, safety, and privacy of its citizens, and should remain readily accessible." https://www.congress.gov/bill/116th-congress/house-resolution/875

[31] Wilbur Ross, Department of Commerce, "Commerce Department Announces NTIA Pilot Program with HHS, FDA to Fight Illegal Online Opioid Sales" (June 8, 2020) https://www.commerce.gov/news/press-releases/2020/06/commerce-department-announces-ntia-pilot-program-hhs-fda-fight-illegal

Commerce and/or other U.S. government departments and agencies actively engage with these same registries, then they will expand their Trusted Notifier arrangements to websites engaged in pervasive copyright piracy as well.

**The Role of Government in Facilitating Voluntary Measures**

The illegal opioid Trusted Notifier program sets an example of the role that the government can and should take in encouraging internet service providers to adopt voluntary measures to curb illegal activities of all kinds that rely on their platforms or services. The ways the government can help in this regard are wide ranging. In the area of copyright piracy, this has been demonstrated by numerous successful instances.

For example, the January 2012 criminal indictment of the notorious cyberlocker Megaupload specifically identified PayPal as the means through which financial transactions were made with respect to criminal copyright infringement, conspiracy to commit copyright infringement, conspiracy to commit money laundering and other alleged crimes. [32] Although PayPal was not indicted as part of the conspiracy, being named repeatedly (thirty-five times to be precise) in this major criminal indictment was hardly a positive development for PayPal and served as a wake-up call. Following the Megaupload indictment, PayPal began cooperating with organizations such as the MPA to develop criteria to identify cyberlockers involved in rampant copyright infringement that should not be allowed to use PayPal's services.[33] This was followed up two years later by Senator Patrick Leahy, who, as Chairman of the Senate Judiciary Committee, wrote to the CEOs of MasterCard and Visa urging them to stop supplying payment services to cyberlockers involved in massive copyright infringement.[34] In his letters Senator Leahy urged MasterCard and Visa "to swiftly review the complaints against those cyberlockers and to ensure that payment processing services offered by [MasterCard/Visa] to those sites, or any others dedicated to infringing activity, cease. I also urge you to continue working with copyright owners and their representatives to develop methods and practices for the efficient investigation of sites alleged to engage in infringement. Voluntary agreements, developed and refined over time between the relevant stakeholders, hold great promise for addressing the problem of infringement online."[35]

As a result of Senator Leahy's letters and follow-up by the Intellectual Property Enforcement Coordinator ("IPEC"), MasterCard, Visa and other payment processors cooperated with copyright owners and their representatives to develop processes for identifying websites devoted to piracy and to terminate, or refuse to provide in the first place, payment services to such websites. The productive relationships established as a result of these efforts permitted the flexibility to adapt the voluntary measures to the ever-changing online piracy landscape. For example, as online piracy of film and television content has evolved and streaming of pirate content has replaced peer-to-peer and torrent

[32] See in particular paragraphs 41,69,79,80 and 84 of Indictment at: https://www.dmlp.org/sites/citmedialaw.org/files/2012-01-05-Indictment.pdf

[33] PayPal's collaboration with copyright owners to avoid providing payment services to entities engaged in piracy has continued to this day and is much appreciated.

[34] Washington Legal Foundation, "Update: Senate Judiciary Committee Chairman Urges Payment Processors To Deter Online Copyright Piracy" (November 25, 2014) https://www.wlf.org/2014/11/25/wlf-legal-pulse/update-senate-judiciary-committee-chairman-urges-payment-processors-to-deter-online-copyright-piracy/

[35] https://www.leahy.senate.gov/imo/media/doc/Binder1.pdf

downloads as the dominant threat, copyright owners and payment processors have worked together to put in place voluntary measures to terminate payment services to pirate streaming services and apps.

Another path for the government to pursue to achieve the development and adoption of voluntary measures is to exercise its convening influence to bring copyright owners and service providers to the table and actively encourage them to work out solutions to online piracy. But convening meetings and generating reports isn't sufficient. Rather, the government needs to demonstrate a commitment to overseeing the process and spurring the creation of pragmatic and effective solutions. Perhaps one of the most successful recent examples of this "convening and encouraging" government approach is the United Kingdom's work in bringing to fruition the Voluntary Code of Practice on Search and Copyright ("Voluntary Code") related to search engines and websites devoted to copyright infringement.[36]

The Voluntary Code was announced in February 2017 after nearly three years of roundtable discussions that were initiated by the UK Intellectual Property Office. The participants in the discussions were the leading search engines Google, Yahoo and Bing and the British Phonographic Industry ("BPI"), the trade association for the British recorded music industry, the MPA and the Alliance for Intellectual Property, a UK based coalition of organizations representing intellectual property. The relatively limited number of participants made the discussions manageable. But more importantly, the oversight and active involvement of the UK government was crucial to pushing the parties towards consensus on the Voluntary Code. Indeed, the UK Minister for Intellectual Property at the time, Baroness Neville-Rolfe, personally participated in many of the meetings and pressed the participants in late 2016 to conclude negotiations and produce a substantive result.

The Voluntary Code[37] sets forth concrete procedures and commitments to demote infringing websites from appearing in search results from neutral queries. It also provides for the removal of advertisements and sponsored sites that link to infringing content. Further, it sets forth a commitment to prevent the generation of search query autocomplete suggestions that would lead consumers to infringing websites. The Voluntary Code commits the parties to collaborating on techniques and exchanging information on a confidential basis in order to fulfill the goals set forth in the Voluntary Code. It also provides for periodic monitoring and assessment by the UK Intellectual Property Office to evaluate progress towards meeting the goals. Finally, the Voluntary Code commits to ensuring that "progress or best practice in this area (to the extent that such information is non-confidential) is shared widely with smaller search engines and independent rights holders."[38]

Although the Voluntary Code was negotiated in the UK, the search engines have applied it on a global basis. Moreover, the Voluntary Code established a foundation for ongoing constructive cooperation between the copyright owner representatives and the search engines. As a result, even though the language of the Voluntary Code itself has not been modified, the parties have cooperated to improve demotion algorithms and have achieved substantial mitigation of the problem of copyright infringing

[36] UK Government, Intellectual Property Office, "Search engines and creative industries sign anti-piracy agreement" (February 20, 2017) https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement

[37] The text of the Voluntary Code is available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609478/code-of-practice-on-search-and-copyright.pdf

[38] Ibid. at paragraph 20

websites and services appearing prominently in search results. Furthermore, the collaboration initiated by the Voluntary Code has led to a higher level of trust and confidence among the parties that has built on its own momentum to enable them to address the changing landscape of online piracy.

Yet another tool the government can employ to foster voluntary measures to combat online piracy is the right kind of legislation. In my view the "right kind of legislation" consists of statutory provisions that are technologically neutral, high-level in nature, and take a long-term approach towards the problem of rampant copyright infringement. One way of explaining this is by a counter-example. Section 1201 of the DMCA concerning circumvention of copyright protection systems has a provision at Section 1201(k) that sets forth detailed requirements for analog video cassette recorders (spelling out separate requirements for VHS, Beta and 8mm format recorders) to conform to a particular copy control technology called automatic gain control that prevented the copying of pre-recorded video cassettes. Section 1201(k) has almost no relevance today, but frankly it was already obsolete less than ten years after the passage of the DMCA.[39] By that time the digital DVD format was by far the dominant market share of the home video market in the U.S. and digital piracy, including via direct downloads and peer-to-peer file sharing, was the most pressing challenge with respect to copyright infringement of film and television content. Please understand, however, that I am not pointing a finger at Congress about Section 1201(k). It was the film industry itself that pressed for inclusion of this particular provision and I participated in the negotiations with counterparts in the consumer electronics industry over some of the terms of Section 1201(k).

An example of what I consider the "right kind of legislation" to address copyright piracy and encourage the adoption of voluntary measures is Article 8(3) of the EU Directive on the harmonization of certain aspects of copyright and related rights in the information society ("Information Society Directive") of 2001.[40] Article 8(3) is a single sentence provision that "ensure[s] that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe copyright or related right." This provision—often referred to as "no fault injunctive relief"—was explained in some detail in the written testimony to the Subcommittee by Stanford McCoy at the hearing entitled "Approaches of Foreign Jurisdictions to Copyright Law and Internet Piracy."[41] Recital 59 of the Information Society Directive explains that: "In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary[.]"

Article 8(3) is perhaps best known for providing the ability of copyright owners to obtain site blocking injunctions to require internet access providers to disable access to a particular pirate website. However, Article 8(3) has been used with respect to a wide range of service provider/intermediary

[39] For the avoidance of doubt, the fundamental anti-circumvention provisions of Section 1201 are both functional and essential and they remain very relevant. They have served as and continue to provide the foundation for robust and evolving digital distribution of copyrighted works from physical optical discs, such as DVDs and Blu-rays, to online subscription streaming services.

[40] For the full text of the Information Society Directive see: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001L0029&from=EN

[41] Testimony of Stanford K. McCoy (March 10, 2020) https://www.judiciary.senate.gov/imo/media/doc/McCoy%20Testimony.pdf

activities. Injunctions have been issued under Article 8(3) to stop hosting providers from hosting pirate websites, to require the complete removal or delisting of pirate websites from search engine results and to order domain name registries and registrars to suspend the domain names of pirate websites. The key to the success and utility of Article 8(3) in effectively combatting online copyright infringement is two-fold.

First, Article 8(3) is very high-level in nature. It does not enumerate the particular service providers or intermediaries to which it may be applied. Furthermore, it does not specify the types of injunctive relief that copyright owners may seek and obtain. Therefore, the relief it provides can readily adapt to the fast-changing nature of the digital and online environment.

Second, Article 8(3) does not involve any pre-requisite finding of liability of any kind (e.g., direct or secondary liability) on the part of the service provider. This "no-fault" approach has been critical to its success. Compare, for example, Section 512(j) of the DMCA that details a number of forms of injunctive relief that may be granted with respect to service providers that qualify for the safe harbor limitations on liability. Section 512(j) by its terms is tied to Section 502 of Title 17; and therefore, ambiguity exists as to whether or not Section 512(j) injunctive relief necessitates a finding of liability on the part of the service provider for infringement—even when the service provider qualifies for the safe harbor limitations. This ambiguity, unfortunately, has served to hinder rather than foster collaboration among copyright owners and service providers.

Article 8(3) has served to provide effective court ordered injunctive relief to copyright owners throughout the European Union—without "breaking the internet." But equally important, its "no fault" approach has engendered significant voluntary cooperation between copyright owners and service providers in Europe. For example, a number of internet access providers that have been subject to site blocking orders have set up informal voluntary processes with copyright owners to identify "mirror sites" and new domain names to which a pirate website that was the subject of a site blocking order moves. Other voluntary processes have been formalized into codes of conduct or memoranda of understanding. Under the Danish voluntary Code of Conduct, for example, if a site blocking order is obtained with respect to one Danish internet access provider, other access providers operating in Denmark will disable access to the same pirate website without the need for a court order.[42] The potency and success of these measures has been well documented.[43] Similar productive voluntary measures and processes have been put in place with respect to other service providers in Europe, such

[42] See this article for a description of the initial voluntary Code of Conduct established in 2014: Maria Fredenslund, Kluwer Copyright Blog, "Denmark: Code of Conduct on website blocking" (October 24, 2014) http://copyrightblog.kluweriplaw.com/2014/10/24/denmark-code-of-conduct-on-website-blocking/ The Code was recently updated in May 2020 and reflects the ability of voluntary measures to adapt and evolve. See here for a description and link to the updated Code in English: https://piracymonitor.org/rights-alliance-updates-antipiracy-guidelines/

[43] See this report from the Danish Rights Alliance that describes how site blocking orders combined with the Code of Conduct and voluntary measures to direct online users to legitimate content services have dramatically decreased the traffic/visits to pirate websites by Danish internet users and has significantly increased visits to legitimate content websites and services: Piracy Monitor, "Denmark: Rights Alliance organization updates site-blocking guidelines" (May 22, 2020) https://piracymonitor.org/rights-alliance-updates-antipiracy-guidelines/ and English translation of report "Report on Share with Care 2" https://rettighedsalliancen.dk/wp-content/uploads/2020/06/Report-On-Share-With-Care-2_Final.pdf

as hosting providers. This demonstrates how government can serve as the catalyst for the adoption of voluntary measures by enacting "the right kind of legislation."

One last point about government involvement with voluntary measures. Senator Tillis asked in his Questions for Stakeholders concerning the DMCA about possible regulatory review of voluntary measures to ensure that: (i) they do not prohibit legal activity, and (ii) independent creators and copyright owners are not shut out from their benefits. I do not believe such specialized regulatory review or oversight is either necessary or advisable. First, there has been no evidence that existing voluntary measures have interfered with non-infringing activity, such as fair uses. Service providers are generally market incentivized to permit utilization of their services for legitimate activities and not to obstruct or terminate legal uses. Nor are copyright owners seeking, through voluntary measures aimed at piracy, to restrict legal activity; rather their focus is commercial scale infringement. Finally, these voluntary arrangements represent agreements between private parties, and therefore existing oversight and/or enforcement mechanisms such as by the Federal Trade Commission or antitrust via the Department of Justice or state equivalents and private parties already apply and suffice. No need exists for special oversight or regulation to ensure voluntary measures do not impinge on legal activity; the free market itself already ensures this outcome.

From my personal experience of negotiating voluntary measures, achieving trust and the confidence among private parties to develop and implement effective anti-piracy measures was challenging. The prospect of specialized regulatory review would add further challenges, increase hesitation and, I believe, serve as a disincentive for service providers to come to the table. Under such circumstances, the only group that would benefit from the regulatory review would be the pirates who would be less constrained from continuing their infringing activities with impunity.

When pirate websites and services are disabled, benefits accrue to content creators large and small. With respect to the concern about independent and smaller creators being denied the benefits of voluntary measures, this appears more relevant to technical measures that some service providers have implemented to fingerprint or identify content. That concern may be better suited to an inquiry as to the possibility of such technical measures being classified as "standard technical measures" under Section 512(i)(2) so that they would be made "available to any person on reasonable and nondiscriminatory terms."

**Conclusion**

While no simple and overall solution exists to the ongoing challenge of online piracy, voluntary measures can fulfill a significant role when coupled with continued law enforcement investigations and criminal enforcement, civil lawsuits, and legislation that provides for readily achievable effective remedies. Particular benefits of voluntary measures include: (i) the ability to adapt them to evolving technology and changing forms of online piracy, (ii) the flexibility to modify and improve them in light of experience and evidence, and (iii) perhaps most importantly the building of trust and genuine collaboration between copyright owners and service providers to combat online piracy with a mutual understanding of service providers' and copyright owners' challenges and constraints.

The U.S. government already has and can continue to serve an important role in encouraging voluntary measures and more widespread adoption of them. This can be achieved by holding hearings such as this one and sending inquiries and requests to service providers. Exercising the convening power the

government holds to bring parties to the table and actively facilitate the negotiation and adoption of voluntary measures is another valuable tool. Finally, in enacting or amending legislation, the government can adopt approaches such as the general no-fault injunctive relief set forth in Article 8(3) of the Information Society Directive that not only provide readily obtainable, wide-ranging and future-proof remedies to curb online piracy, but also encourage voluntary measures and collaboration between copyright owners and services providers.

Thank you again for the opportunity to participate in this Hearing and I am happy to answer any questions.

Annex A

**CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM**

Trusted Notifier Status

- The Registry must be willing to accept and act on referrals received from the Trusted Notifier. As such, it is important for the Trusted Notifier to be a recognized authority within the field in which it operates.
- Characteristics of a Trusted Notifier include an industry representative trade association that represents no single company, a recognized not-for-profit public interest group dedicated to eliminating illegal behavior, or a similarly situated entity with demonstrated extensive expertise in the area in which it operates and ability to identify and determine the relevant category of illegal activity.
- The Trusted Notifier must be willing to stand behind its referrals.
- The relationship is voluntary in nature – either party may withdraw from the program at any time.

Operations

- Both the Registry and Trusted Notifier provide designated points of contact for the sending and receiving of referrals regarding abuse in a TLD.
- The Trusted Notifier's referrals will be treated expeditiously and with a presumption of credibility, though the Registry may conduct its own investigation.

Standards for Referrals

Referrals from the Trusted Notifier must include, at a minimum:

- A statement that the Trusted Notifier is authorized to submit the referral (e.g. for copyrights, the Trusted Notifier has authority to assert a claim on behalf of the rights holder);
- Detailed description of the abusive activity (i.e., sample URLs, screen shots);
- Non-exhaustive Identification of the law(s) being violated by the activity;
- Clear and brief description of why the site's activity violated the specified law(s);
- Statement that, prior to sending the referral, the Trusted Notifier alerted or attempted to alert the registrar of record and hosting provider, including a description of the response received, if any, from registrar and hosting provider and an explanation of why such responses failed to mitigate the abuse;
- Statement that the referral is submitted with a good faith belief that the information contained therein is true and accurate; and
- Confirmation that the referral was subject to careful human review by the Trusted Notifier—not submitted solely based on automated Internet scanning or scraping services.

In addition to satisfying all of the elements above, before submitting a referral, the Trusted Notifier will make a good faith effort to determine whether the domain is operating with false Whois

information. Where applicable, the referral will also include the following to the best of Trusted Notifier's knowledge:

- Statement that Whois information provided by the registrant contains false or misleading information; and
- Identification of which Whois field may be false or misleading.

Actions by the Registry

- Registry will review the referral on an expedited basis;
- Registry will coordinate with the applicable registrar;
- As appropriate, registrar (or Registry if registrar declines) may provide the referral to the registrant, and will set a reasonable deadline in which to receive a response;
- If Registry agrees that the domain clearly is devoted to abusive behavior as reported in the referral, the Registry, in its discretion, may suspend, terminate, or place the domain on registry lock, hold, or similar status as it determines necessary to mitigate the harm and that such action may constitute an appropriate response to a domain engaged in clear and pervasive abusive behavior;
- If the Registry has concerns, questions the scope or nature of the reported abuse, or has received alternative instruction from law enforcement or similar authority, the Registry should provide a written explanation promptly to the Trusted Notifier and give the Trusted Notifier opportunity to supplement or amend its referral;
- Absent exceptional circumstances, the Registry will endeavor to determine a course of action and inform the Trusted Notifier of its decision within 10 business days of receipt of the referral.