Questions for Dean Marks from Senator Tillis

1. I've heard that the current notice-and-takedown system in section 512 casts a shadow over most interactions between copyright owners and online service providers – including any negotiations. If section 512 is re-written, how do you think that would change the pervasiveness of voluntary agreements and the types of voluntary agreements that copyright owners and service providers are willing to enter into?

I think the section 512 safe harbor provisions, particularly as interpreted by the federal courts in the Second Circuit case Viacom v. YouTube (2012) and the Ninth Circuit cases Perfect10 v. CCBill (2007) and UMG v. Shelter Capital (2013), have not served to promote the high degree of voluntary collaboration and cooperation between online intermediaries and copyright owners that Congress anticipated. Instead, section 512 has permitted service providers simply to respond to takedown notices, not worry about the same infringing content re-appearing on their platforms, and rest assured that they will not be subject to damages or any injunctive relief.

In my view, the most effective way section 512 could be re-written both to provide meaningful relief for copyright owners and to encourage voluntary cooperation is if it explicitly permitted copyright owners to seek injunctive relief to require a broad array of service providers and intermediaries to take commercially reasonable actions to help combat online infringement without any prerequisite finding of any liability whatsoever on the part of the service provider/intermediary. I explained this in some detail in my written testimony at pages 11-13. Instead of the "one and only shot" remedy of notice-and-takedown as currently provided under Section 512, this "no fault injunctive relief" approach—which has been successfully adopted in Europe, Australia and elsewhere—would permit a wide range of remedies. These remedies include terminating hosting and other services to pirate websites, suspending domain names of pirate websites, removing pirate websites from search engine results, and blocking access to pirate websites (and the foregoing is by no means an exclusive list of remedies).

As set forth in greater detail in my written testimony, this "no fault injunctive relief" approach has, in Europe, served as a foundation upon which voluntary agreements and collaboration among copyright owners and service providers have been built. Lengthy, contentious and expensive litigation about whether or not a service provider is within or outside of the safe harbors and/or whether or not a service provider is liable for copyright infringement fails, in my view, to provide positive incentives to collaborate or to build the trust necessary for successful voluntary efforts. Indeed, to my mind this constitutes "the shadow cast" as set forth in Senator Tillis' question.

A number of the successful voluntary agreements to combat online piracy that have emerged in the United States, including the TAG program with respect to online advertising, the payment processor arrangements, and the domain name registry trusted notifier agreements, all involve intermediaries that are not covered by the safe harbor provisions of Section 512. I don't think this is a mere coincidence. Instead, I believe that Section 512 has unfortunately ended up

hindering the voluntary collaboration that it was intended to foster. Thus, I suggest that modifying Section 512 to provide for high-level, non-specific, no fault injunctive relief would be one of the best paths towards fostering wide adoption of voluntary measures across a broad range of service providers and intermediaries.

2. What is the future role of voluntary measures in combating online piracy?

I think voluntary measures will continue to play an important role in combating online piracy for three key reasons. First, no single "silver bullet" solution exists to stop online piracy. While law enforcement efforts, implementation of technical protection measures, civil litigation and "follow the money" approaches are all critically important, none of them alone—or even together—will defeat online piracy. And that holds equally true for voluntary measures. A robust multi-pronged approach is required to combat online piracy and voluntary measures are and will remain an important prong.

Second, voluntary measures—unlike statutory provisions—can be readily adapted and modified to changing circumstances and evolving technologies. For example, in just the last three or four years, the most damaging form of online piracy to the film and television industry has changed from peer-to-peer downloads to streaming. Because they can be quickly adapted to changes in technology and new forms of online piracy, voluntary measures are likely to continue to play a key role in the future.

Finally, as more service providers venture into content production and distribution (e.g., Amazon Prime, Google TV) the incentives shift to provide a better basis for collaboration to fight online piracy. Hopefully, this will lead to a stronger and more effective role in the future for voluntary measures.

3. You negotiated the trusted notifier program between the Motion Picture Association and the Donuts domain registry. Can you tell me more about how this works, whether it has been successful, and why both parties would want to enter into such an agreement?

The description of how the trusted notifier program between the MPA and Donuts works is set forth in some detail in the Annex to my written testimony entitled "Characteristics of a Trusted Notifier Program." The steps that the MPA takes in making a trusted notifier referral to Donuts are as follows:

- First alert or attempt to alert the registrar of record and the hosting provider of the pirate website to seek suspension of the domain name and/or termination of hosting services for the pirate website. If these attempts fail, then in the written referral made to Donuts describe these outreach attempts, including a description of the responses received, if any, from the registrar and the hosting provider and how the responses failed to stop the operation of the pirate website.

- Include in the referral to Donuts a detailed description of the infringing activity (i.e., sample URLs, screen shots) of the pirate website;
- Provide in the referral a non-exhaustive identification of the law(s) being violated by the activity of the website;
- Provide a clear and brief description of why/how the website's activity violates the identified law(s);
- Confirm in the referral that the investigation of the website was subject to careful human review and not submitted solely based on automated internet scanning or scraping services; and
- Include a statement that the referral is submitted with a good faith belief that the information contained therein is true and accurate.

Once the referral meeting the above requirements is submitted to Donuts, then Donuts conducts its own investigation and may consult with the relevant registrar as well as the registrant of the domain name. If Donuts agrees that the website is engaged in pervasive copyright infringement, then it will suspend or lock the domain name.

Although suspension of the domain name of a piracy website is not a "silver bullet" that ends online piracy, it is an effective tool for the following reasons. First, when a pirate website's domain name is suspended, the website essentially disappears from the internet. While a pirate website can register a new domain name under a different generic top level domain ("gTLD") or a country code top level domain ("ccTLD") and re-emerge online, there is still disruption and traffic diminishes to the pirate website.

Second, if a pirate website is subject to sequential suspension of its domain name by cooperative registries or registrars, then as it "jumps" from one gTLD or ccTLD to another, further disruption occurs and users of the pirate website become confused as to where to find it. Finally, if a very popular pirate website has its domain name suspended and needs to move to a new gTLD or ccTLD, then often a multitude of websites seeking to pose as the pirate website emerge online under a variety of gTLDs and/or ccTLDs to defraud unaware users with identify theft, credit card scams, and similar fraudulent activity.[1]

Given the above consequences, domain name suspensions via voluntary trusted notifier agreements create significant friction in the online piracy marketplace. Thus, they have proven to be an effective tool for combatting online piracy and represent a successful voluntary initiative.

In my view a good deal of the success of the trusted notifier program between the MPA and Donuts was built upon active collaboration, trust and sharing of burdens between the two

[1] For example, see James Geddes, Tech Times "Torrentz Returns As Kickass Torrents Scams And Clones Appear" (11 August 2016) https://www.techtimes.com/articles/173286/20160811/torrentz-returns-as-kickass-torrents-scams-and-clones-appear-one-alternative-mirror-site-is-really-pirate-bay.htm

organizations. The MPA focuses its referrals on the "worst of the worst" piracy websites and coordinates with Donuts so as not to overload Donuts with too many referrals at any one time. Further, if Donuts has questions about how the piracy websites operate and how direct the nexus is to the infringing content, the MPA answers those questions. These factors have sustained a mutually respectful and effective voluntary collaboration.

I believe the trusted notifier arrangement between the MPA and Donuts should serve as a model for not only other domain name registries and registrars, but also other online intermediaries, including hosting providers, content delivery networks (such as Cloudflare), cloud and other infrastructure service providers, payment providers and even search engines.

With respect to the question as to why parties would want to enter into trusted notifier arrangements, the answer varies with the particular party. Some service providers, including some domain name registries, think it is part of their civic duty to take reasonable steps to combat online copyright piracy. Others want their services to gain a reputation as being a "safe space" for legal commerce and other legitimate activity that is free from blatant illegal activity such as copyright piracy. For others, it is the fact that copyright piracy websites pose high risks of malware, phishing attacks and other cybersecurity threats and the service providers seek to protect their customers from these risks. Finally, sometimes pressure from government leads service providers to undertake voluntary measures to avoid the introduction and implementation of government regulation. Clearly the above-described motivations aren't necessarily exclusive. Furthermore, they can operate in combination to bring service providers "to the table." Irrespective of the particular motivation(s) or combination thereof, service providers often regard trusted notifier arrangements as an efficient way to gather reliable and expert information about online piracy from organizations with decades of experience, such as the MPA.

For copyright owners, trusted notifier arrangements represent a much more efficient and less costly way to fight online piracy than bringing federal court actions against the actual operators of the piracy websites, who are often located outside of the United States. If service providers cooperate with and voluntarily act upon the detailed and substantiated referrals made by copyright owners, then this represents real disruption of the online piracy marketplace. This is because the pirate website disappears (at least temporarily) from the internet if its domain name is suspended or its hosting services are terminated. If other service providers kick pirate websites off their platforms (e.g., social media, search results from search engines) in response to trusted notifier referrals, then this also serves to disrupt entire websites devoted to piracy. It is important to note that a single pirate website may be the source of hundreds or even thousands of infringing works. Hence, the remedies resulting from trusted notifier agreements are far more effective and efficient than the notice-and-takedown system embodied in Section 512, which requires copyright owners to send notices on each individual piece of infringing content to a service provider, only more often than not to see that same piece of infringing content reappear quickly on the same platform to which the copyright owner sent the notice.

Dean S. Marks –
The Role of Private Agreements and Existing Technology in Curbing Online Piracy
Questions for the Record
Submitted December 22, 2020

QUESTIONS FROM SENATOR COONS

1. Testimony at last week's hearing suggests that voluntary measures have not sufficed to combat widespread digital piracy. Some have suggested that the federal government should play a role in establishing, regulating, mediating, or otherwise overseeing standard technical measures, best practices, or other currently voluntary arrangements designed to prevent the unauthorized distribution of copyrighted works.
    a. Should the federal government serve a role in connection with such standard technical measures, best practices, or other currently voluntary arrangements?

In terms of best practices and voluntary arrangements, I believe the federal government has an important role to play in several respects. First, the federal government can enact legislation that will encourage voluntary measures and best practices. In my view, the most helpful would be for Congress to add a provision to the Copyright Act (whether as part of a revision of Section 512 or otherwise) that would permit copyright owners to seek injunctive relief to require a broad array of service providers and intermediaries to take commercially reasonable actions to help combat online infringement without any prerequisite finding of any liability whatsoever on the part of the service provider/intermediary. This approach has been adopted in the European Union and provides a wide range remedies, including terminating hosting and other services to pirate websites, suspending domain names of pirate websites, removing pirate websites from search engine results, and blocking access by ISPs to pirate websites (and the foregoing is by no means an exclusive list of remedies).

But in addition to effective remedies, this legislative "no fault injunctive relief" approach has served as a foundation upon which voluntary agreements and collaboration among copyright owners and service providers have been built in Europe. Contrast this with our more than two decades of experience under Section 512. Lengthy, contentious and expensive litigation about whether or not a service provider is within or outside of the safe harbors and/or whether or not a service provider is liable for copyright infringement fails, in my view, to provide positive incentives to collaborate or to build the trust necessary for successful voluntary efforts.

Indeed, a number of the successful voluntary agreements to combat online piracy that have emerged in the United States, including the TAG program with respect to online advertising, the payment processor arrangements, and the domain name registry trusted notifier agreements, all involve intermediaries that are not covered

by the safe harbor provisions of Section 512. I don't think this is a mere coincidence. Instead, I believe that Section 512 has unfortunately ended up hindering the voluntary collaboration that it was intended to foster. Thus, I suggest that enacting legislation to provide for high-level, non-specific, no fault injunctive relief would be one of the best paths towards fostering wide adoption of voluntary measures across a broad range of service providers and intermediaries.

Quite apart from legislation, the federal government can take other actions to encourage the adoption of voluntary measures to combat online piracy. This includes holding hearings with various classes of service providers and inquiring about the voluntary measures they are taking and asking why they are not adopting other voluntary measures, such as trusted notifier agreements and voluntary codes of conduct. Writing to service providers to urge them to undertake specific voluntary measures to address online piracy is another action that federal government can undertake. One suggested specific example would be writing to major domain name registries such as Verisign, GoDaddy Registry and Public Interest Registry to urge them to follow the example set by Donuts and to enter into trusted notifier agreements with organizations such as the Motion Picture Association and the Recording Industry Association of America to address websites operating their domains that are engaged in pervasive copyright infringement.

On pages 9 – 13 of my written testimony submitted for the December 15, 2020 hearing, I set forth more detailed explanations and examples of both the legislative and non-legislative actions the federal government can embrace to encourage the adoption of effective best practices and voluntary arrangements to combat online piracy.

b. If Congress were to conclude that the federal government should play a role, what role should that be, and what entity is best-positioned to serve in that capacity?

Clearly Congress itself could enact legislation as described in the response above and hold hearings, write letters to various service providers and convene meetings of service providers and copyright owners to work out best practices and effective voluntary arrangements to diminish online piracy. In addition, if the U.S. Copyright Office were given authority to require a wide range of service providers to adopt best practices and embrace voluntary arrangements to combat online piracy, then this could prove effective given the Copyright Office's substantive expertise.

One note of caution, however. A significant advantage of voluntary measures is that they can be readily adapted to evolving technology and changing forms of online piracy. Copyright owners (and the associations that represent them) and service providers are best situated to understand the piracy challenges and devise effective means for addressing them, provided appropriate incentives and willingness to

collaborate are present. Therefore, it would be misguided in my view if these efforts somehow became subject to the exclusive jurisdiction of government rulemaking.

c. Are there non-governmental entities that would be equally or better situated to serve in this role? If so, how would you suggest that we incentivize them to do so?

My only substantive experience with non-governmental entities in the area of policy and governance with respect to online service providers is with respect to the Internet Corporation for Assigned Names and Numbers ("ICANN") and the Domain Name System, including registries, registrars and proxy services. From my active involvement with ICANN over the past three years, I believe ICANN would be ill-suited to serve in the role of encouraging or overseeing voluntary measures, best efforts or standard technical measures with respect to combating online piracy.

2. Much of last week's testimony focused on the role of social media platforms and content owners in policing digital piracy. Some voluntary agreements designed to thwart online copyright infringement have also involved domain name registries, payment processors, and advertising networks.
   a. Among these industries, who do you believe has been most effective in voluntarily combating digital piracy, and who should do more?

My sense is that the online advertising industry as a whole has been one of the more effective in voluntarily combating digital piracy through the TAG brand integrity program. I think nearly every other industry could do more and embrace voluntary measures more broadly. For example, while the trusted notifier voluntary agreements with domain name registries Donuts and Radix have been effective at fighting online piracy due to the efficient suspension of domain names of pirate websites, they are the only two generic top level domain ("gTLD") registries to have embraced this voluntary collaboration with respect to online copyright piracy. Other major U.S. registries, such as Verisign (the registry for the by far market dominant gTLDs .com and .net), GoDaddyRegistry (the registry for .biz) and Public Interest Registry (the registry for .org), have declined to enter is such arrangements despite repeated outreach attempts.

   b. Are there additional entities that are playing or should be playing a role in voluntarily combating digital piracy?

A broad range of entities should be playing a role in voluntarily combating digital piracy. Some of the individual companies in these groups already take on some voluntary collaboration, others do not (such as in the specific example of domain name registries described above). A very wide range of intermediaries and service providers support the existence and viability of online copyright piracy websites and service providers. They include hosting providers, cloud services, content delivery network services (such as Cloudflare), domain name registrars and registries, user generated content platforms (such as YouTube), payment processors, advertising

networks and providers, search engines and social media companies. All of these categories of service providers and intermediaries can and should embrace voluntary measures to fight digital piracy. One of the most straightforward ways of doing so is to embrace trusted notifier arrangements with organizations that have deep experience in identifying websites and online services that are engaged directly in or facilitating pervasive copyright infringement. If all of these service providers and intermediaries responded in a timely fashion to referrals by trusted notifiers by terminating their services to the pirate websites and services, then this would significantly reduce online piracy. In the case of search engines, they enable pirate websites and services to be "found" by users; thus if they responded to trusted notifier referrals by de-listing such websites and services from their search results, then this would significantly diminish traffic to such websites and services. Furthermore, if internet access providers blocked access to pirate websites and online services (as is done across the European Union), this would be a very significant and effective step towards reducing online piracy.

Please note that trusted notifier arrangements are just one example of voluntary measures. Others include the formulation and use of "red flag" factors that are checked before providing services to a website. This type of measure has been adopted by some payment processors to prevent pirate websites and services from using or signing up to their payment services. Another measure that can and should be employed by domain name registrars is to verify the full identity and contact information (name, email address, postal address and telephone number) of an individual or organization that seeks to register a domain name. Such verification should be done before issuing a domain name to any prospective registrant. This is because actors who engage or plan to engage in illegal activity, such as copyright piracy, seek to hide their identity and do not want to give their true name and contact information to acquire a domain name. Thus, this type of voluntary action would help discourage and likely diminish online piracy. Ironically, under ICANN's contracts and policies governing domain name registries and registrars, registrars are supposed to take steps to ensure the accuracy of this data. Unfortunately, ICANN has not rigorously enforced these accuracy provisions in the past and has ceased doing so since 2018.

With respect to concerns that voluntary measures may end up inadvertently impacting legitimate websites and services, this can readily be addressed by incorporating an expedited and inexpensive alternative dispute resolution process ("ADR") into these arrangements. Such an ADR would permit a party impacted by a referral to appeal the decision to suspend services, de-list it from search results, etc. and make the case that the party was not engaged in or directly facilitating pervasive copyright infringement. A party that pursued such an ADR and won should then have its services immediately restored and its costs of the ADR paid for by the entity that made the inappropriate referral.

3. We heard testimony about YouTube's Content ID, Facebook's Rights Manager, and other software tools available to match user-posted content against databases of copyrighted material. Some have expressed concerns that requiring all platforms to use such tools would be unduly burdensome and serve to entrench larger, more established platforms. How do you suggest that we make this type of anti-piracy technology available to all creators without stifling innovation?

   It seems the most straightforward way to make these software tools available to smaller platforms in order to accomplish simultaneously the three goals of combating digital piracy, fostering competition and preventing undue burdens that would serve to entrench larger and more established platforms is for Congress to figure out a method (perhaps via a Copyright Office rulemaking procedure) of designating such tools as "standard technical measures" under Section 512(i)(2). In order to do so, Congress would likely have to eliminate or relax the requirement set forth in Section 512(i)(2)(A) that mandates that such measures "have been developed pursuant to a broad consensus . . . in a . . . multi-industry standards process." This is because tools such as Content ID and Rights Manager were developed by a single company (YouTube and Facebook respectively) and not pursuant to a multi-industry standards process. If Congress were able to address this obstacle and find a path forward of designating tools such as Content ID and Rights Manager as "standard technical measures," then the key provision set forth in Section 512(i)(2)(B) that such tools be made "available to any person on reasonable and nondiscriminatory terms" would apply and hence require that these tools to be made available not only to smaller platforms, but to all copyright owners as well.

4. Some witnesses warned that voluntary agreements can exclude and disadvantage smaller entities in the creative ecosystem, including creators and content owners, internet users, and internet platforms. If voluntary anti-piracy agreements are to remain truly voluntary, how do we ensure that everyone has a seat at the table?

   While it appears that some types of voluntary measures, such as Content ID, may exclude and therefore disadvantage smaller creators and content owners, that is not the case for all voluntary measures. For example, pirate websites—whether they be pirate streaming services, peer-to-peer or torrent sites and indexes, or cyberlockers—typically infringe the copyrights of both large and small content creators. Therefore, when voluntary measures are undertaken to disable such pirate websites and services, this benefits all content creators and copyright owners. Typically trade associations, such as the MPA and RIAA, tend to be the active participants in voluntary arrangements with service providers and intermediaries due to their anti-piracy expertise and their resources in terms of personnel. Nevertheless, their work benefits all creators and copyright owners whose works are being infringed by pirate websites and services when such websites and services are either hobbled financially are taken offline altogether. Examples of such voluntary arrangements include the TAG advertising brand integrity program, which works to keep online advertising away from pirate websites and services, and the collaboration with payment processors, such as PayPal, to terminate—or not provide in the first place—payment services to online

pirate websites and services. In terms of the trusted notifier agreements that I negotiated with domain name registries Donuts and Radix during my tenure with the MPA, when the MPA made a referral to either registry that resulted in the suspension of the domain name of a pirate website, the benefits did not accrue solely to the MPA and its member studios but rather to all creators and content owners whose works were being infringed by the pirate website.

Therefore, I suggest that caution be undertaken about ensuring "that everyone has a seat at the table" as a prerequisite for voluntary measures. As explained in my written testimony submitted for the December 15, 2020 hearing, successful voluntary measures require the building of mutual understanding, trust and collaboration. The more parties that at are "at the table" the more difficult that is to accomplish. Moreover, certain civil society groups that have criticized voluntary measures as "shadow regulation" and "censorship" are highly unlikely to contribute positively to the promulgation of effective voluntary measures to combat online copyright piracy. Please consider that the cherished motto of some of these groups that "Information wants to be free" often expands into outright hostility for any effective copyright protection whatsoever to creative works online.

Questions for the Record for Dean S. Marks
From Senator Mazie K. Hirono

1. **I understand that you were part of the effort to work with the manager of the ".movie" domain to combat large-scale piracy websites.**

   Yes. ".movie" is a generic top level domain ("gTLD") that is owned and administered by Donuts, Inc. a U.S. domain name registry that is based in Bellevue, WA. (See: https://donuts.domains/) As set forth in my written testimony to the Senate Judiciary Committee, when I worked at the Motion Picture Association ("MPA") as EVP, Deputy General Counsel and Chief, Global Content Protection, I negotiated a trusted notifier agreement with Donuts that applied not only to ".movie" but to all of the gTLDs that Donuts owns and administers. At the time the trusted notifier agreement between MPA and Donuts was finalized in early 2016, Donuts owned and administered nearly 200 gTLDs. Now that number has risen to nearly 300 gTLDs. As explained in more detail in my written testimony and the Annex entitled "Characteristics of a Trusted Notifier Program," the trusted notifier arrangement between Donuts and the MPA was a purely voluntary agreement aimed at terminating domain name services (e.g., suspending or locking the relevant domain name) of websites devoted to copyright piracy. Although I left the MPA in July 2017, my understanding is that the trusted notifier arrangement between Donuts and the MPA is still in place.

   In my view a good deal of the success of the voluntary trusted notifier program between the MPA and Donuts was built upon active collaboration, trust and sharing of burdens between the two organizations. For example, as set forth in the "Characteristics of a Trusted Notifier Program" Annex to my testimony, the MPA makes referrals to Donuts only after due diligence to investigate the piracy website, document the abuse and attempts to have the pirate website first removed by contacting the hosting provider and the domain name registrar. Furthermore, the MPA focuses its referrals on the "worst of the worst" piracy websites and coordinates with Donuts so as not to overload Donuts with too many referrals at any one time. These factors have sustained a mutually respectful and effective voluntary collaboration.

   a. **What efforts to combat online piracy are being taken with respect to the ".movie" domain that aren't being taken for other domains like ".com"?**

      The key difference is voluntary cooperation in the form of the trusted notifier arrangement. Donuts has exhibited leadership and responsibility in cooperating with copyright owners to engage in a trusted notifier agreement (that involves no payment or promise to purchase domain names by the notifying party—the MPA—or its member companies). Donuts acts on referrals by the MPA of websites that are engaged in pervasive copyright infringement and operating under the gTLDs for which Donuts serves as registry. By suspending or locking the domain name of piracy website, the

registry essentially causes the website to disappear from the internet. It cannot be located by users unless and until the website re-emerges under a different domain name.

This stands in sharp contrast to the registries that operate other gTLDs like ".com", ".net" and ".biz". Verisign, which is the registry for the market dominant gTLDs ".com" and ".net", has consistently refused to engage in trusted notifier arrangements to address online piracy or other forms of illegal activity, like counterfeiting and the distribution of child sexual abuse materials. I engaged in several discussions with Verisign when I was with the MPA to seek to put in place either a trusted notifier arrangement or an expedited alternative dispute resolution process, but Verisign declined. Instead, Verisign will only act to suspend the domain name of a piracy website operating under ".com "or ".net" if it is served with a federal court order that explicitly directs it to suspend such domain name. Furthermore, Verisign will only act with respect to specifically identified domain names that are spelled out in a court order. Thus, to take a hypothetical example, if a pirate website is operating under "movieforfree.com" and has a mirror/duplicate website operating under "movies4free.com," and the court order only identifies "moviesforfree.com," then that is the only domain name that Verisign will act upon.[1]

Filing a copyright infringement lawsuit in federal court and litigating the case to obtain a federal court order is expensive and time consuming. This places unnecessary burdens and costs on copyright owners and allows piracy websites to flourish on gTLDs such as ".com" and ".net" because the registry refuses to engage in voluntary cooperation with organizations such as the MPA that have decades of experience identifying and combatting online copyright piracy. Please note that this unwarranted burden and lack of responsibility and cooperation doesn't just apply to copyright piracy. Verisign refuses to engage in voluntary cooperation on a wide range of illegal activities, even though anticounterfeiting organizations and child protection organizations (just to name two areas) with expertise in identifying websites engaged in illegal activity exist and are ready to engage in cooperative arrangements. As far as I am aware, the only trusted notifier arrangement that Verisign has entered into is the one announced in 2020 with the Food and Drug Administration and NTIA to address websites engaged in the illegal sale of opioids. This was referenced and described in my written testimony on pages 7-9.

b. How effective are these efforts in combatting online piracy?

Voluntary cooperation and collaboration, such as trusted notifier arrangements with

[1]For further information about frustrated efforts to engage Verisign in voluntary cooperation, please see the two letters attached to these responses. These letters were written to NTIA in connection with the renewal of the Cooperative Agreement between the Department of Commerce and Verisign. The first letter, dated October 11, 2018, was written by me on behalf of the Coalition for Online Accountability. The second letter, dated October 18, 2018, was written by John Carr on behalf of a group of child protection organizations.

domain name registries, are quite effective in combatting online piracy. This is because when a pirate website's domain name is suspended, the website essentially disappears from the internet. While a pirate website can register a new domain name under a different gTLD or even a country code top level domain ("ccTLD") and re-emerge online, there is still disruption and traffic diminishes to the pirate website.

Furthermore, if a pirate website is subject to sequential suspension of its domain name by cooperative registries or registrars, then as it "jumps" from one gTLD or ccTLD to another, further disruption occurs and users of the pirate website become confused as to where to find it. Finally, if a very popular pirate website has its domain name suspended and needs to move to a new gTLD or ccTLD, then often a multitude of websites seeking to pose as the pirate website emerge online under a variety of gTLDs and/or ccTLDs to defraud unaware users with identify theft, credit card scams, and similar fraudulent activity.[2]

Given the above consequences, domain name suspensions via voluntary trusted notifier agreements create significant friction in the online piracy marketplace. Thus, they have proven to be an effective tool for combatting online piracy.

Moreover, it is important to note that when registries like Donuts undertake voluntary efforts, such as trusted notifier arrangements, to eliminate copyright piracy websites from their domains, pirates soon recognize that these domains do not turn a blind eye to copyright piracy. Thus, pirates will seek out other domains that will either welcome or tolerate their illegal activity. If a significant number of major domain name registries were to engage in voluntary action (via trusted notifier or similar arrangements) to suspend the domain names of websites engaged in copyright piracy, then such websites would likely end up clustering on just a few top level domains. Those top level domains would then develop a reputation for being untrustworthy and may well become subject to blacklisting by cybersecurity companies and anti-virus/malware software programs. And that serves to aid an additional layer of friction and disruption when users seek out such piracy websites. This is not merely a hypothesis. These consequences have been demonstrated with websites engaged in cybersecurity attacks, since domain name registries and registrars tend to be much more pro-active with respect to "kicking off" those types of websites.

Hence, if major domain name registries such as Verisign, Neustar (now GoDaddyRegistry since its recent acquisition by GoDaddy) and Public Interest Registry would engage in trusted notifier arrangements with copyright owners (or trade associations representing such copyright owners) to suspend the domain names of websites engaged in pervasive copyright infringement, this would significantly help disrupt online copyright piracy.

[2] For example, see James Geddes, Tech Times "Torrentz Returns As Kickass Torrents Scams And Clones Appear" (11 August 2016) https://www.techtimes.com/articles/173286/20160811/torrentz-returns-as-kickass-torrents-scams-and-clones-appear-one-alternative-mirror-site-is-really-pirate-bay.htm

Clearly, there is no single silver bullet that will end online copyright piracy. Domain name suspension—even if undertaken voluntarily by all major U.S. domain name registries—will not by itself end online copyright piracy. But it certainly would be a significant step forward in the ongoing fight against it.

c. What, if anything, is preventing other domain name registrars from taking similar steps?

My experience with these voluntary trusted notifier arrangements is with domain name registries, such as Donuts and Radix (a United Arab Emirates company and registry for gTLDs such as ".online", ".tech" and ".website") rather than registrars. Probably the easiest way to think of the difference between the two is that the registry is the "wholesaler" of the domain and the registrars are the "retailers." Multiple registrars, for example, can and do sell ".com" domain names. But there is only a single registry for ".com" and that is Verisign. All gTLDs and ccTLDs have just one registry because a single entity must be responsible for administering and coordinating the functions of the gTLD or ccTLD. As a result, there are far fewer registries than registrars and registries are nearer the "top of the pyramid" of the domain name system. During my time with the MPA, I therefore focused my efforts at securing voluntary cooperation from registries.

In terms of what is preventing other domain name registries from entering into trusted notifier or similar voluntary cooperative arrangements to combat online piracy, I think there are several explanations. First and foremost, I believe it's a matter of willingness. If a register doesn't feel pressure or a strong incentive to enter into such arrangements, then why bother? A piracy website, like other websites, pays for its domain name. Both registries and registrars make money selling domain names to websites, irrespective of whether such websites are engaged in legal or illegal activity. So, why "kick out" a paying customer? Second, if a registry makes the decision simply to comply with court orders to suspend domain names and do nothing further, then it saves costs on compliance personnel and/or the time and work involved in engaging in voluntary collaborative efforts, such as trusted notifier arrangements. Third, as set forth in my written testimony, voluntary efforts by domain name registries such as Donuts to suspend the domain names of websites engaged in copyright piracy have been criticized by some civil society groups as censorship and "shadow regulation." While, as explained in my written testimony, such arguments lack merit, I believe they have made some domain name registries and registrars back away from voluntary measures and cooperation.

While at the MPA, I worked with the legal team at Public Interest Registry, the registry for the gTLD ".org" on an arrangement to address websites engaged in copyright piracy, such as the notorious ThePirateBay.org. While Public Interest Registry was not comfortable pursuing a trusted notifier arrangement, they were open to collaborating on an inexpensive and efficient alternative dispute resolution process to allow copyright

owners to seek an arbitration order that a website operating under the ".org" gTLD was engaged in pervasive copyright infringement. If such an order were obtained, then Public Interest Registry would suspend the domain name of the website. We worked constructively for several months to hammer out the parameters for this alternative dispute resolution process and came to agreement. Unfortunately, Public Interest Registry withdrew the proposed alternative dispute resolution process reportedly under pressure from the Internet Society, which is the sole corporate member of Public Interest Registry (a 501(c)(3) non-profit corporation), and instigated by public criticism by the Electronic Frontier Foundation and some other civil society groups.

Two further observations as part of this response. First, although my efforts at voluntary collaboration were focused on domain name registries, these same voluntary collaborations could also be embraced by domain name registrars, particularly the largest ones such as GoDaddy. My sense is that the same reasons outlined above for why more registries haven't entered into voluntary collaborative efforts to combat online copyright piracy also apply to registrars.

Second, in October 2019 a group of 11 registries and registrars announced a voluntary DNS Abuse Framework. Among the original signatories and co-creators of the Framework were Donuts and Public Interest Registry. The Framework, including the current text of the Framework document, the background concerning its creation and a recent 2020 retrospective can all be found here: http://dnsabuseframework.org/ There are currently 48 registries and registrars that have signed on to the Framework.

The Framework represents a positive step forward in two respects. First, it recognizes certain categories of illegal website content (referred to in the Framework as "Website Content Abuse") that domain name registrars and registries should act upon. The categories recognized are: (1) child sexual abuse materials ("CSAM"); (2) illegal distribution of opioids online; (3) human trafficking; and (4) specific and credible incitements to violence. Second, the Framework explicitly embraces and recommends trusted notifier arrangements and states, "Trusted Notifiers can serve as a crucial resource to enhance the abuse monitoring and disruption procedures of registries and registrars." It is noteworthy—and disappointing—that Verisign, the registry for by far the largest market share of domain names with its ".com" and ".net" gTLDs, has not signed on to the Framework.

Unfortunately, the Framework does not classify copyright piracy as a category of "Website Content Abuse" that merits voluntary action by registries and registrars. Nevertheless, I think the Framework deserves to be commended and supported. My hope is that in the future more registries and registrars will be willing to expand their voluntary efforts to combat copyright piracy as well.

d. Are there steps that ICANN should be taking to encourage domain name registrars to take these steps?

I believe it likely that ICANN will maintain that it is beyond the remit of its bylaws to encourage domain name registries and registrars to take voluntary action to combat copyright online piracy. Furthermore, from my experience both at the MPA and with the Coalition for Online Accountability, I have found ICANN's compliance and enforcement undertakings to be woefully lacking. Even though registries and registrars undertake contractual commitments in the accreditation agreements they enter into with ICANN with respect to abuse and illegal activity (including intellectual property infringement) by websites operating under their domains, ICANN does not compel the registries or registrars to undertake any action to actually address such illegal activity. This lack of enforcement persists even when parties—such as copyright owners—file well documented complaints with ICANN's compliance department. Thus, my view is that ICANN will not take any meaningful steps to encourage registries or registrars to engage in collaborative voluntary efforts to suspend the domain names of websites engaged in pervasive copyright infringement.

e. Are there steps we can take as lawmakers to encourage domain name registrars to take these steps?

Yes. Because some of the largest operators in the domain name system in terms of registries and registrars are U.S. companies, such as Verisign, Public Interest Registry and GoDaddy, U.S. lawmakers can take on a significant role in encouraging these companies to follow Donuts' lead and enter into voluntary collaborative arrangements to stop websites engaged in copyright piracy from operating under their domains.

Such steps could include:

1. Requesting that these companies participate in a hearing and asking them to explain why they are unwilling to engage in voluntary arrangements, such as trusted notifier agreements, to stop copyright piracy websites from operating under their domains.

2. Writing to such registries and registrars to ask them specifically to enter into voluntary collaborative arrangements, such as trusted notifier, to stop copyright piracy websites from operating under their domains.

3. Introducing legislation to clarify that if a domain name registry or registrar is put on written notice that an identified website is engaged in pervasive copyright infringement, and the registry/registrar fails to take timely action to suspend the domain name of such website, then the registry/registrar will be secondarily liable for the copyright infringement occurring via such website. With respect to the registrar, this would apply to the registrar that sold the domain name for the piracy website and has a contract with the registrant of the particular domain name. With respect to the registry, this would apply to the registry of the gTLD that the domain name of the pirate website is

would apply to the registry of the gTLD that the domain name of the pirate website is operating under.

I would be happy to collaborate with and assist Senator Hirono's staff or any other lawmakers' staff members interested in pursuing paths (including but certainly not limited to the suggestions above) to encourage domain name registries and registrars to undertake voluntary measures, such as trusted notifier, to combat online piracy.

Coalition for Online Accountability

www.onlineaccountability.net

October 11, 2018

Honorable David J. Redl
Assistant Secretary for Communications and Information
Administrator, National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, DC 20230

Dear Assistant Secretary Redl:

The long-standing Cooperative Agreement between the Department of Commerce and Verisign with respect to .com is set to expire November 30, 2018. We write to express our concern about the disturbingly high levels of abusive and illegal activity taking place on Top Level Domains ("TLDs") administered by Verisign, and to urge that NTIA immediately conduct a "public interest review" as specifically provided for in Amendment 34 of the Cooperative Agreement. As part of such a public interest review, we request that Verisign be required to undertake reasonable and feasible steps to better protect the public interest and to preserve and enhance the security and stability of the Internet, particularly with respect to the .com TLD.

The Coalition for Online Accountability (COA) represents the interests of leading U.S. copyright industry associations, organizations and companies in ICANN-related matters.[1] But the concerns COA raises below apply more broadly to whether Verisign is adequately stepping up to its corporate responsibility to cooperate in combatting a wide range of abusive and illegal online activities that threaten the safety, security and economic interests of all Americans.

As you are aware, abusive and illegal activity over the Internet is growing. The recently released report by the Department of Commerce and the Department of Homeland Security notes that "[distributed denial of service attacks] have grown in size to more than one terabit per second, far outstripping expected size and excess capacity."[2] Similarly, the 2017 Phishing

---

[1] The members of COA are Broadcast Music, Inc.; Entertainment Software Association; Motion Picture Association of America; Recording Industry Association of America; NBCUniversal; Twenty-First Century Fox; The Walt Disney Company; and WarnerMedia.

[2] Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, p. 5
https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

Trends & Intelligence Report states that phishing volume grew by an average of more than 33% across the five most-targeted industries and phishing sites were found on more than 170,000 unique domains, representing a 23% increase over the prior year.[3] But online abuse isn't limited to cyberattacks and phishing. Trafficking in child abuse imagery, copyright piracy, the sale of dangerous counterfeit products, including pharmaceuticals, and other illegal activity also flourish online.

Unfortunately, TLDs administered by Verisign are involved in an enormous percentage of many types of such illegal and abusive online activity. For example, according to the 2017 Annual Report of the Internet Watch Foundation, "more domains than ever before are being used to show children being sexually abused—a 57% increase on last year."[4] These domains are concentrated among a handful of TLDs, "five of which accounted for 85% of all webpages identified as containing child sexual abuse images and videos." Of this 85% identified by the Internet Watch Foundation, **an astounding 79% of such child sexual abuse webpages are found on two TLDs administered by Verisign (.com—59.5% and .net—19.4%)**.[5] This represents a much higher percentage than Verisign's overall market share of websites for these two TLDs, which is 50.5% (.com—46.7% and .net—3.8%) of all websites operated under all generic TLDs and all country code TLDs (note: the Internet Watch Foundation Report covers both generic TLDs and country code TLDs).[6]

In 2015-16, **61% of the top 500 film and television piracy websites identified by the Motion Picture Association of America were operated under TLDs for which Verisign served as the registry**. These included the .com, .net, .tv and .cc domains (.tv is the country code TLD for Tuvalu and .cc is the country code TLD for the Cocos Islands; the registries for both .tv and .cc are Verisign companies). The breakdown of these top 500 film and television piracy websites is as follows: 40%--.com; 12%--.net; 7%--.tv; and 2%--.cc.

---

[3] See: https://www.phishlabs.com/phishlabs-2017-phishing-trends-intelligence-report-hacking-the-human/

[4] See: https://annualreport.iwf.org.uk/

[5] Ibid, https://annualreport.iwf.org.uk/#statistics_and_trends_2017

[6] According to W3Techs Web Technology Surveys, the combined market share of Verisign's .com and .net domains constitutes 50.5% of all websites across all TLDs, including country code TLDs. Web3Techs reports that .com accounts for 46.7% of websites and .net accounts for 3.8% of all websites. See: https://w3techs.com/technologies/overview/top_level_domain/all. We note that Verisign's own data analyzes domain name registrations, which include domain names that have been purchased but are not yet associated with any operational website. According to Verisign, .com accounts for 40% of all domain name registrations and .net accounts for 4% of all domain name registrations. See Verisign's Domain Industry Brief for Q-2 2018 at https://www.verisign.com/en_US/domain-names/dnib/index.xhtml

The 2017 Phishing Trends & Intelligence Report notes that **53% of phishing sites are located on Verisign's .com (49%) and .net (4%) domains.**[7]

Verisign enjoys a dominant position in the TLD space and--just with respect to .com and .net--serves as the registry for more than half of the websites on the World Wide Web. Although Verisign may cite its market dominance as somehow explaining the high level of abuse on its domains, we believe Verisign's success in fact heightens its responsibility to combat abuse and illegal activity vigorously. That the majority of legitimate websites – and consumers – flock to .com is all the more reason why bad actors should be prevented from operating there. Accordingly, we do not think Verisign's dominant position in any way excuses the extremely high levels of serious online abuse and illegal activity operating under the domains that Verisign administers and controls. As a U.S. publicly traded company with 2017 reported revenues of $1.17 billion, Verisign can and should do much better.

A procedure has already been forged that Verisign could readily adopt and replicate to begin to address these unacceptable levels of illegal and abusive activity: the Trusted Notifier arrangement. Under this model, organizations that have expertise in an area—such as the Internet Watch Foundation and the National Center for Missing and Exploited Children in child sexual abuse, and the Motion Picture Association of America, Recording Industry Association of America and Entertainment Software Association in online entertainment media copyright piracy—investigate websites engaged in abusive and illegal activity; verify by human review the pervasive abusive nature of the websites; and report those websites to the applicable TLD registry operator. The registry then expeditiously reviews the reported websites and, unless it discovers some mistake or discrepancy inconsistent with the report, the registry suspends the domain names of the reported websites. Several leading registry operators already participate in Trusted Notifier arrangements (whether formal and informal), and they work. For example, both Donuts and Radix have entered into Trusted Notifier arrangements with the MPAA to address websites engaged in clear and pervasive copyright infringing activity. These Trusted Notifier arrangements allow for the rapid suspension of the domain names—and therefore interruption of the underlying website's copyright piracy activities—without the burden, expense and time delay of securing a court order.[8]

We know that Verisign has been asked to enter into Trusted Notifier arrangements with regard to sites that employ domain names for which Verisign serves as the registry (e.g., a ".com" domain or ".net" domain). To our knowledge, Verisign has consistently refused to enter into such arrangements, and has insisted that it will suspend domain names only in response to U.S.

---

[7] See chart p. 15 : https://www.phishlabs.com/phishlabs-2017-phishing-trends-intelligence-report-hacking-the-human/

[8] Existing trusted notifier arrangements are described more fully in COA's (response to NTIA's Notice of Inquiry in the matter of international internet policy priorities, See pp. 3-4: https://www.ntia.doc.gov/files/ntia/publications/coa_response_to_ntia_noi_final_july_17_2018_1.pdf

court orders or Uniform Domain-Name Dispute-Resolution Policy ("UDRP") decisions (note: the UDRP is strictly limited to cases involving trademark right disputes in the domain name itself, so does not address the bulk of abuse related to copyright infringement or any other abusive activity such as phishing, trafficking in child sex abuse imagery, and the sale of dangerous counterfeit products). Verisign thus appears to be shirking the responsibility acknowledged by other leading domain name registries that have taken up the mantle of collaboration to address clearly abusive online activity. One of the many advantages of Trusted Notifier arrangements is that they can be implemented to address a wide range of abusive and illegal activity from copyright infringement, to the trafficking in dangerous counterfeit products, cyberattacks and phishing, and trafficking in child sexual abuse imagery, to name just a subset of online abusive and illegal activity. It is not difficult to identify organizations with deep expertise in the relevant areas of abusive online activity to do the "heavy lifting" of investigating websites, gathering evidence and submitting the reports. The critical missing component is the willingness of a registry to accept such reports and act expeditiously upon them.

An argument frequently raised by domain name registries (and registrars) for declining to enter into Trusted Notifier arrangements is that the registries and registrars do not think they should take up the role of "judge and jury" to make a determination of abusive and/or illegal activity and suspend the relevant domain name. But all registries and registrars reserve for themselves in their contracts the complete discretion to suspend domain names for websites engaged in activities that violate their terms of service, including abusive and illegal activity. So the ability is absolutely present and available; this is simply a question of willingness to take on responsibility.

As the leading and dominant registry in the domain name system, Verisign should take a leadership role in collaborating to reduce the amount of abusive and illegal activity online by entering into Trusted Notifier arrangements. The shares of illegal and abusive activity—whether it be the trafficking in child abuse imagery, copyright piracy or phishing attacks—attributed to domains administered and operated by Verisign (as reported by the credible third parties described in this letter) should be unacceptable to the United States government. Furthermore, they should be unacceptable to Verisign itself.

Many entities, from Europol to the Messaging Malware Mobile Anti-Abuse Working Group, have recognized that law enforcement alone and the courts alone cannot adequately address the growing levels of illegal activity that we are collectively witnessing online. Effective online safety depends on platforms assuming greater responsibility and undertaking greater collaboration with non-governmental organizations that have expertise in various types of illegal and abusive online activity.

We note that Verisign has undertaken efforts to revise its registry-registrar agreement to include more specific provisions that impose obligations on registrars to include in their own agreements with domain name registrants provisions that prohibit registrants from engaging in abusive and illegal behavior. We applaud and support these efforts and hope you will

encourage ICANN and Verisign to enshrine them in the registry agreement for .com. We also acknowledge Verisign's work to transition to a full thick WHOIS registry, which unfortunately has been stalled due to the recalcitrance of ICANN-accredited registrars. But given the scale and breadth of abusive and illegal online activity flowing from Verisign domains, these efforts alone are not sufficient.

As noted above, the Cooperative Agreement reserves the Commerce Department's "right to conduct a public interest review" to determine whether the Department will exercise its right to extend the term of the Cooperative Agreement. We therefore strongly urge that NTIA conduct such a public interest review and, pursuant to such a review, direct Verisign to undertake Trusted Notifier arrangements to reduce the levels of illegal and abusive activity occurring on the .com TLD. We also urge that the Cooperative Agreement be extended for a reasonable period during which NTIA can monitor Verisign's compliance with the directive that it enter into Trusted Notifier arrangements with responsible and expert third parties.

On behalf of COA, , I respectfully request that the NTIA take a pro-active role in addressing these growing online threats in a concrete manner. As party to the Cooperative Agreement, NTIA acts in effect as a steward of U.S. national interests in a safe and secure Internet where the rule of law is respected. In fulfillment of that role, NTIA should not let the Cooperative Agreement expire absent concrete and enforceable undertakings by Verisign, or any potential successor registry to the .com domain, to enter into effective Trusted Notifier arrangements.

Thank you for considering our views and please let me know of any questions. I would be happy to meet with you or any of your staff (either in person or by phone) to discuss these issues.

Respectfully submitted,

Dean S. Marks
Executive Director and Legal Counsel
Coalition for Online Accountability ("COA")
E-mail: ed4coa@gmail.com

cc: Fiona M. Alexander, NTIA

10 Great Queen Street, London, WC2B 5DG

18th October 2018

Honourable David Redl
Assistant Secretary for Communications and Information
Administrator, National Telecommunications and Information Administration
United States Department of Commerce
Washington, DC 20230

Dear Administrator Redl,

I am writing to you to request that the National Telecommunications and Information Administration take whatever actions are necessary in order to secure substantial improvements by Verisign in reducing the levels of serious abuse, particularly the trafficking in child sexual abuse imagery, occurring on websites operated under top level domain names administered by them.

Since we were formed back in 1999, the coalition of children's organizations which I represent and work with has had a major interest in finding ways to restrict or eliminate the distribution of child sex abuse material over the internet

As with many other illegal activities, the trafficking in child sexual abuse imagery online continues to grow at alarming rates. We are witnessing increases of nearly 40% in child sexual abuse urls and 60% in the number of domains that are used to display images or videos of children being sexually abused. Unfortunately, the overwhelming majority of these domains are located within .com and .net, both of which are administered by Verisign. The latest Annual Report of the Internet Watch Foundation meticulously documents these troubling statistics.

Over the years we have made several attempts to contact Verisign seeking to discuss how we might collaborate to combat the child sexual abuse imagery that is rampant on their domains. I have only ever had one response and that was three months ago when their PR agency, Weber Shandwick, contacted me to ask for a document I had written. I sent it, tried to follow up. Zero response.

Verisign is uniquely unforthcoming. We have regularly worked and had conversations with just about every internet company you can think of and quite a few you are unlikely to know. Only Verisign has been so utterly uncommunicative. This is a very poor show and runs completely contrary to the spirit of multistakeholderism.

Enlisting the active and effective voluntary cooperation of domain name Registries is now more important than ever to combat online illegal activity. As you are undoubtedly aware, since ICANN implemented a Temporary Specification in response to the European General

Data Protection Regulation, access to WHOIS information about domain name registrants has been effectively removed from a number of parties who previously played an important part in keeping crime off the internet. I have written about this separately and have concluded that this situation will not be resolved soon.

Given that context it is particularly critical for online platforms and intermediaries to take on greater responsibility in the fight against this singularly tragic form of abuse. Some other Registries, notably NOMINET, have shown that things can be done. For example, every day, using a lexicon of terms provided to them by the Internet Watch Foundation, NOMINET runs a check on each new registration to ensure it is not likely to be used to distribute child sex abuse material. NOMINET is not a small Registry. It shows things can be done at scale, if there is a will to do them. Verisign appears not to have that will so we must look to others with the power to persuade or compel them.

To put the matter plainly, it is immoral for a business to attempt to deflect responsibility by arguing these matters are the sole provenance of law enforcement and courts. As the dominant Registry in the global system, Verisign should be taking a leadership position, adopting voluntary procedures to combat online child sexual abuse. It should put in place clear and transparent processes to ensure the swift suspension of domains within their purview that are involved in distributing child sexual abuse imagery and take steps to reduce the prospects of new domains being established and used in like manner in future.

I strongly urge the NTIA and the rest of the United States Government to use whatever leverage is at its disposal to push Verisign to do the right thing and stop dragging their feet. The lives and well-being of children are at stake.

Yours sincerely,

John Carr OBE
Secretary