Statement of
Maria A. Pallante
Acting Register of Copyrights

Before the
Subcommittee on Intellectual Property, Competition, and the Internet
Committee on the Judiciary
United States House of Representatives
112th Congress, 1st Session

March 14, 2011

"Promoting Investment and Protecting Commerce Online:
Legitimate Sites v. Parasites, Part I"

Chairman Goodlatte, Ranking Member Watt, and Members of the Subcommittee, I appreciate the opportunity to appear before you this afternoon to testify about the importance of providing incentives for legitimate commerce in the online environment by protecting against the parasites who compete with it. We also deeply appreciate the support of Chairman Smith and Ranking Member Conyers on these issues.

As you know, the Copyright Office is the agency charged with administering the copyright law. Our duties include advising Congress and other government entities on matters of domestic and international copyright policy, including legislative proposals, participating in intergovernmental meetings and negotiations, and conducting studies, public inquiries, roundtables and rulemakings, as appropriate. We do not carry out enforcement activities, but are regularly consulted on copyright enforcement issues by Congress and the executive branch.

Copyright law, which originates in the U.S. Constitution[1] and is codified today in Title 17 of the United States Code, promotes innovation by extending to owners of creative works a panoply of exclusive rights, including reproduction, distribution, the right to prepare derivative works, and, in certain instances, the right of public performance and display. Though these rights are granted by law, they are of little value to the copyright owner if they cannot be meaningfully enforced.

The issues presented by parasites and so-called "rogue websites" raise complex legal questions but also present an opportunity for Congress to manage the relationship between technology and intellectual property, as it has done many times before. In the course of our research on this issue, we have met with a variety of stakeholders in the Internet ecosystem and will continue to do so in the weeks ahead. We welcome the opportunity to assist Congress in its continued examination of the need for legislation in this area. While we recognize the significant concerns related to trademark infringement and counterfeiting, my comments today focus on copyright law and practice.

ROGUE WEBSITES

The Copyright Office believes the United States has a problem with a category of bad actors that build online businesses by infringing copyright and engaging in related illegal activity. Indeed, based on our discussions with a wide array of stakeholders, there appears to be widespread, although not universal, consensus on this point.

The operators of rogue websites exploit copyrighted works with impunity because, in part, there is no expectation of enforcement; they have no real fear of being brought to justice. With the global reach of the Internet, rogue websites can be located anywhere in the world and still have a devastating effect on the market for legitimate copyrighted works created by U.S. book authors, composers, recording artists, filmmakers, software companies and other creators.

While many agree on the broad outlines of the problem, the precise contours remain elusive. There are a variety of views about how to frame the issue and how to develop effective

[1] Art. I, § 8 ("The Congress shall have Power . . . To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").

solutions that respect our core American values of due process and free expression of ideas. Moreover, there is a wide spectrum of piratical, counterfeiting, and otherwise infringing activity on the Internet, making a solution difficult. Many sites contain some infringing content alongside lawfully distributed materials, while others contain nothing but infringing content. Still other sites – most commonly referred to as "cyberlockers" – allow users to store and share digital files. Although many users employ cyberlockers for entirely lawful purposes, some have used them as a mechanism to distribute infringing content.

We appreciate that the Subcommittee's stated focus is the proliferation of websites built almost entirely on the business of making and/or distributing unauthorized materials. Such websites violate trademark law, engage in unfair competition and, in the case of copyright law, undermine the exclusive rights of reproduction, distribution, and/or the public performance or display of legitimate copyrighted materials.

These "worst of the worst" flagrantly engage in illegal activities. They offer consumers the sale, download, streaming of or linking to highly creative movies, music, books, and software. They may also offer devices, software and services used to circumvent access or copy controls in violation of Title 17.

Many rogue website operators make money through direct transactions with Internet consumers. In some cases, they charge a fee for the purchase of a product or service. In other cases, they charge subscription fees. In either instance, they may utilize well-known payment processors (e.g. credit cards) to facilitate the actual exchange of money, or they may falsely state that they have relationships with such payment processors and then, when a consumer actually attempts to pay, redirect consumers to other, alternative payment methods that may or may not be secure. Those rogue websites that do not engage in direct financial transactions with customers may rely on online advertising placement to fund their illegal activities.

Aside from being illegal, the existence of such websites undermines the incentives and the ability of legitimate companies to engage in the production, sale, licensing and other dissemination of copyrighted content to compete in the marketplace. For good faith companies whose livelihoods are based on the creation and exploitation of intellectual property, rogue websites present a significant threat to their core business model.

At the same time, unlike traditional brick-and-mortar infringers, rogue website operators can be extremely difficult to identify or locate, especially if they are based outside the United States. As a result, pursuing them can be hopelessly frustrating for copyright owners and law enforcement agencies alike, including because it is everybody's goal to target those whose primary purpose is to profit from intellectual property they do not own and have no reasonable basis for exploiting. (The circumstances clearly exceed a finding of "fair use" or other defenses available under the law.) Nevertheless, one of the key challenges for policy makers will be to define carefully those bad actors who are the target of additional enforcement measures, so as to avoid inadvertently capturing good faith actors.

CURRENT LEGAL AND BUSINESS ENVIRONMENT

As a backdrop for the issues, I will provide a brief overview of current U.S. law related to enforcement of copyright on the Internet.

Civil Enforcement and the Digital Millennium Copyright Act: With respect to civil actions for online copyright infringement, the forms of relief provided by the Copyright Act in appropriate cases include actual damages, statutory damages, injunctive relief, costs and attorneys fees, and impoundment. The well-established doctrines of direct and secondary liability for copyright infringement have developed through case law. Copyright owners have a significant role in enforcing their interests using civil law mechanisms. Indeed, the vast majority of copyright enforcement cases are brought by copyright owners themselves, though fewer and fewer small copyright owners can afford the costs of litigation. In the context of rogue websites, the cause of action is typically direct infringement and the availability of damages and injunctive relief would vary with the specific facts at hand.

Additionally, in 1998 Congress passed the Digital Millennium Copyright Act (DMCA),[2] which was intended to foster the expansion of electronic commerce by reducing legal uncertainties of conducting business on the Internet while, at the same time, establishing mechanisms for combating online infringement. As part of the DMCA, Section 512 of the Copyright Act provides certain "safe harbors" and limits the liability of online service providers for copyright infringement when engaging in certain types of activities. For example, Section 512(a) provides Internet service providers (ISPs) with a limitation on liability for acting as "mere conduits" and providing transitory digital network communications, Section 512(c) provides online service providers that host material on their servers or networks at the direction of third parties with a limitation on liability, and Section 512(d) provides search engines with a limitation on liability for providing information location tools.

To be eligible for these limitations under the law, online service providers (other than mere conduits) must take certain responsible steps as participants in the Internet ecosystem, including responding to the notifications of copyright owners. In general, an on-line service provider may be notified that it is providing access to infringing material. The copyright owner may request a "take-down," but must also supply to the provider a degree of factual data specified in Section 512 (such as identifying the copyright at issue, the infringing work, and the owner's contact information, among other things). If the provider removes the infringing material, the copyright owner will not be able to bring an action against the provider for allowing access to the infringing material. A similar provision applies to search engines that direct users to infringing material. Section 512 thus provides a streamlined method for copyright owners to have infringing material taken down without first having to go to court.

Criminal Enforcement: Criminal copyright infringement is a federal cause of action. The Department of Justice often takes the lead on criminal copyright prosecutions, but several other U.S. government agencies have a role in investigations and law enforcement under various statutes that protect intellectual property rights, including copyright. For example, the Federal

[2] *See* 17 U.S.C. § 512, § 1201 *et seq*.

Bureau of Investigation (FBI), the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and other agencies all work to enforce our copyright law.[3] In recent months, ICE has used existing civil forfeiture remedies available against criminal activity to seize the domain names of websites involved in extensive infringing copyright and trademark activities.[4]

We note that part of what ICE is doing is providing a level of comfort to consumers with respect to the legitimate operation of the top-level domains most commonly used in the United States. That is, ICE cannot reach all the secondary or foreign domains that lure consumers to infringing content or unsafe medicine, but they can try to make the big three (.com, .org and .net) safe for the American public. Unfortunately, we understand (and are concerned) that once a domain name has been seized, it eventually returns to the pool of domains available to the public for registration unless it is purchased by the government. We question this result. We would also note that to the extent ICANN plans to increase the number of top-level domains available for commerce in the United States, as has recently been discussed, one consideration should be how the use of multiple domains would affect existing enforcement capabilities and objectives for customer protection.

Takedowns and the Domain Name System (DNS): One particular enforcement measure that is especially relevant in this context is the takedown or blocking of Internet domain names that are associated with rogue websites. As mentioned above, U.S. law enforcement has used existing civil forfeiture provisions to obtain warrants to seize domain names, and the service of these warrants is usually aimed at a domain name registry, and, in some cases, ISPs. These entities also respond to orders or requests from courts and law enforcement to disable or block access to domain names and websites that are used for criminal activity. DNS blocking targets the domain name itself; it does not block the Internet protocol (IP) address, which is comprised of a series of numbers that identifies a domain name on the Internet and that ultimately leads the user to the desired website.

Current Voluntary Practices: Voluntary practices to combat online copyright infringement have been developing in a number of areas. For instance, we understand that there is increasing cooperation between payment processors, which include credit card companies (e.g., MasterCard) and online payment services (e.g., PayPal), and rightsholders to combat online infringement of copyrighted works including films and music. In addition to cooperation in the

---

[3] A summary of recent efforts by law enforcement in the intellectual property arena has been compiled by the Office of the Intellectual Property Enforcement Coordinator, which recently issued its first Annual Report. *See* Office of the Intellectual Property Enforcement Coordinator, *2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement*, Feb. 2011, *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf.

[4] These actions led by ICE have been conducted under 18 U.S.C. § 2323. The Prioritizing Resources and Organization for Intellectual Property Act of 2008 strengthened existing forfeiture provisions for use in cases involving copyright infringement and trademark counterfeiting. Pub. L. No. 110-403, 122 Stat. 4256. ICE has indicated to us that approximately 140 domain names have been targeted in four operational sweeps since the summer of 2010. According to a recent conversation with ICE, to date, not a single owner of the targeted domain names has contested these seizures.

United States, we understand that there is progress on voluntary cooperation with law enforcement by payment processors and certain copyright owners in the United Kingdom.[5]

We have also been told that some domain name system registrars voluntarily cooperate with individual rightsholder requests to block access to domain names that are associated with rogue websites because these registrars have broad terms of service prohibiting use of domain names for various types of illegal activity, including intellectual property violations. We understand that at least one registrar is actively – and voluntarily – helping rightsholders when a domain name is being used in connection with infringing goods and services.[6]

DEFICIENCIES IN CURRENT LEGAL AND BUSINESS ENVIRONMENT

In analyzing the legal issues relevant to rogue websites, it has become clear to us that websites based outside the United States are especially problematic. In many cases, they lack sufficient ties to the United States to be compelled to appear before U.S. courts and to allow the enforcement of a judgment against them. The detrimental effect of this fact on U.S. creators and innovators is one of the major reasons we applaud the attention this Subcommittee is giving to this topic.

Indeed, the pressing issue is how to tackle rogue websites based in foreign jurisdictions. Copyright owners have few options to pursue websites that are based abroad and that do not take advantage of U.S.-based Internet registrars or registries.[7] Finding methods to address the illegal activities of foreign websites and non-U.S.-based actors who may not be subject to U.S. jurisdiction can be a challenge in many areas of U.S law enforcement, and the same challenge applies to civil efforts to combat copyright infringement. In this context, the question becomes how to get at the off-shore rogue websites. We have seen the "pop up" effect of Internet piracy, as operators of rogue websites whose domain names have been seized have simply moved to top-

---

[5] Earlier this month, the international recording industry announced a project with two payment processing companies and the City of London Police's Economic Crime Directorate. *See* IFPI press release, "Recording industry welcomes support by payment providers to tackle illegal online sale of unlicensed music," March 2, 2011, *available at* http://www.ifpi.com//content/section_news/20110302.html. So far, the details of 24 copyright infringing music services have been given to the London police.

[6] We are also aware of voluntary efforts addressing Internet pharmacies and establishing standards for addressing trademark counterfeiting on the Internet. On December 14, 2010, the White House announced that American Express, eNom, GoDaddy, Google, MasterCard, Microsoft, Network Solutions, Neustar, PayPal, VISA and Yahoo! agreed to start a non-profit group to educate the public and begin to take voluntary enforcement action against illegal Internet pharmacies. *See* Office of the Intellectual Property Enforcement Coordinator, *Counterfeit Pharmaceutical Inter-Agency Working Group Report to the Vice President of the United States and to Congress*, March 2011, *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/Pharma_Report_Final.pdf. Voluntary guidelines also exist in the trademark counterfeiting context. *See* International Trademark Association (INTA), "Addressing the Sale of Counterfeits on the Internet," Sept. 2009, *available at* http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf. Participating payment processors include American Express, Discover, MasterCard, PayPal, and VISA, working with participating Internet providers eBay, Google and Yahoo!.

[7] Internet registrars allow individuals and organizations to register specific domain names. By contrast, Internet registries do not have direct relationships with the registering person or organization, but instead manage all domain names within a specific type of top-level domain name such as ".com" or ".net."

level domains administered in other countries (e.g., ".info" and ".ru"), which may serve as more "hospitable" jurisdictions that allow them to operate, usually with impunity, or at least untouched for a significant amount of time.[8]

Copyright law is territorial and copyright owners must manage significant jurisdictional questions when attempting to pursue infringement actions against foreign actors. Copyright owners could attempt to bring suit in the United States for copyright infringement by a foreign website if there are sufficient contacts (e.g., significant advertising and sales to U.S. consumers) but it can be difficult to litigate against uncooperative foreign entities and/or to enforce a judgment abroad. The intersection of U.S. and foreign law is an appropriate topic for Congress to consider, including how these jurisdictional issues affect the remedies in successful infringement cases.

We do believe that enhanced international cooperation can play a positive role, that is, international cooperation both by law enforcement authorities and by private sector groups and Internet intermediaries. However, while voluntary efforts should be pursued whenever possible, the continued evidence of widespread global Internet copyright infringement suggests that cooperation alone cannot be the only solution to this complex problem. Cooperation on an international scale is at best a gradual process and to date has not stopped these websites from continuing to wreak havoc on the marketplace of legitimate commerce.

Finally, we note that, although copyright owners may have more options to pursue domestic rather than foreign rogue websites, domestic sites also continue to pose challenges. The parasites who operate rogue websites in the United States often do not provide sufficient contact information to allow a copyright owner to identify or locate them and can create obstacles to moving forward with potential litigation. Additionally, even if a copyright owner targets a domestic website, there may still be the same problem as faced abroad that the website may simply – and quickly – reappear at another domain name.

MOVING FORWARD

The Copyright Office believes that copyright enforcement against the operators of rogue websites could be enhanced and improved with mechanisms that "follow the money" within the Internet ecosystem. These parasites could be cut off from payment mechanisms and advertising revenues in the United States; this could combat their very existence, or at least substantially decrease their impact on the market for legitimate copyrighted content.

In our view rogue websites are a problem that will require mutual cooperation of many stakeholders and Congress may want to consider whether all who benefit from a healthy online ecosystem should contribute to a solution. For example, ISPs play a critical role in providing Internet access, and correspondingly the means to interrupt access, to rogue websites. Domain

[8] For example, news reports indicate that the Spanish website Rojadirecta.com, a domain name that was seized by ICE in its February 1, 2011 seizure, quickly established additional domains served by registries in other countries (e.g., Spain, Montenegro, India), and continues its operations. *See, e.g.*, Trent Nouveau, *US DOJ and ICE seize additional domains*, TG Daily, Feb. 2, 2011, *available at* http://www.tgdaily.com/business-and-law-features/53884-us-doj-and-ice-seize-additional-domains.

name registries and registrars are able to block domain names. Search engines point users to rogue websites, but technology may exist that would allow them to block such sites from appearing in search results, much as search engines have eliminated child pornography from their results.

Payment Processors: Payment processors are credit card companies and payment intermediaries such as PayPal. With respect to legitimate commerce, they enable consumers and businesses to conduct transactions online. Without them, the Internet would not be the robust business enterprise it is today in the American economy.

Payment processors are structured in a variety of ways. Some have direct contractual relationships with consumers, others have relationships with merchants and banks, and yet others have mixed arrangements. They have terms of use that can be helpful in handling allegations of copyright infringement. At the same time, many rogue websites allow Internet consumers to use traditional credit cards, debit cards and other financial transaction services to purchase or access infringing materials as part of single transactions or subscriptions. Even those websites that do not rely on financial transactions can benefit from payment processors' goodwill by displaying the logos of well-known payment networks in an effort to lend credibility to the site by creating a false sense of authenticity.

Congress could grant enforcement entities such as ICE the explicit authority to request a court order requiring payment processors to stop providing these services for the website in question to consumers within the United States. If rogue websites are unable to use standard payment methods, Internet users may be less willing to use less familiar alternative payment structures, and innocent consumers might be suspicious of the absence of standard payment methods, thereby harming the financial viability of the sites.

Advertising Networks: Many rogue websites display advertising, allowing them to run lucrative businesses by providing content without a copyright owner's permission. Generally, advertising networks place advertisements on websites for merchants wishing to advertise their goods and services. Such networks typically place their clients' advertising on websites that may be relevant to the clients' goods and services or that are popular with the clients' target demographic. Some networks, however, do not specifically control where all of the advertisements appear and instead subcontract at least some of their placement services to other advertising brokers that, in turn, place advertisements on various websites.

Unfortunately, the multi-layered structure of Internet advertising placement can make it difficult to determine which entity is ultimately responsible for placing an advertisement on a specific website. At this point it is unclear to us whether all the advertising networks involved in the placement of a particular advertisement would necessarily have either knowledge that an advertisement was placed on an infringing site or the ability to prevent the advertisement's placement on that site.

Legislation that could prevent advertising networks from placing advertisements on rogue websites might reduce the profitability of these sites and deter further copyright infringement. Once again, legislation could give enforcement entities such as ICE explicit authority to request

a court order requiring U.S.-based advertising networks to stop placing advertisements on the alleged rogue website in question.

Other Parties in the Internet Ecosystem: ISPs play a critical role in providing access to and delivery of Internet-based services to consumers. Some stakeholders propose to provide enforcement authorities such as ICE with the ability to request court orders directing ISPs to block the domain names or Internet protocol addresses of specified foreign-based rogue websites for all U.S.-based customers. We have also heard concerns about the technical feasibility of implementing blocking orders, especially at the subdomain or IP address levels, as well as the potential costs that ISPs might incur if a large volume of orders were presented to them for action. We believe that these issues require further investigation and analysis.

We are aware of several other countries that have issued judicial orders requiring ISPs in their jurisdictions to block national access to specific foreign websites that seem to fall within the rogue website concept here. For example, actions have been taken in Italy, Ireland and Denmark in an effort to block the website The Pirate Bay from those nations' citizens.[9]

When attempting to seize or take down domain names to block rogue websites, law enforcement agencies and copyright owners often work with registrars and registries because they can often control where a request for a domain name from an Internet user is directed.[10] We are aware, however, of the concerns expressed by some that domain name server blocking, including that used in the recent ICE civil forfeiture proceedings and other non-copyright law enforcement activities, targets only the domain name and does *not* block the IP address, thus allowing persistent Internet users to find the rogue website using the IP address. This Subcommittee might want to give further consideration to methods to address this concern either at the registrar and registry level or through ISPs.

---

[9] The Italian Supreme Court in December 2009 ruled that ISPs could be obliged to cut access to the then-Swedish-based The Pirate Bay (TBP) domain. *See* International Federation of the Phonographic Industry (IFPI), *Italy's Supreme Court explains ruling that ISPs should block The Pirate Bay*, Jan. 8, 2010, *available at* http://www.ifpi.org/content/section_news/20100108.html. In early February 2010, Italian prosecutors ordered all national access providers to block TBP. *See Block The Pirate Bay, Italian ISPs ordered*, Feb. 10, 2010, *available at* http://www.p2pnet.net/story/35342. Action has also been taken action against TBP in Ireland and Denmark. One major Irish ISP, Eircom, blocked access to TPB in July 2009 (using both DNS and IP address blocking). *See* Austin Modine, *Eircom to block Pirate Bay*, The Register, Feb. 23, 2010, *available at* http://www.theregister.co.uk/2009/02/23/irma_demands_irish_isps_block_access_to_piracy_sites/. In Denmark, the recording industry obtained an injunction against an ISP (Tele2, now Telenor) requiring it to block access to TPB; this was confirmed on appeal, and, in May 2010 the Supreme Court upheld the injunction. *See* European Digital Rights (EDRi), *Danish supreme court upholds injunction to block the Pirate Bay*, June 2, 2010, *available at* http://www.edri.org/edrigram/number8.11/piratebay-denmark-supreme-court. The Court did not require IP address blocking, only blocking of the site's domain and sub-domains (DNS blocking).

[10] When a consumer tries to reach a website associated with a domain name, the consumer's ISP identifies and contacts the relevant registry associated with the requested domain name, such as VeriSign for ".com" top-level domain names, because the registry controls the root name servers that will direct Internet traffic to the correct website. The registry, in turn, directs the user to an authoritative domain name server, which, in most circumstances, is the registrar of the specific domain name. The registrar then sends the Internet user to the content identified by its customer, the domain name registrant, which is housed on a specific server, identified by an IP address connected with a particular domain name (or group of domain names).

Search engines are perhaps the most important player in the on-line ecosystem. Without them, the Internet would be un-navigable. Unfortunately, search engines routinely point people to rogue websites, including in situations where the customer is looking for a legitimate site. In fact, sometimes the illegitimate sites appear much higher in search results, displacing authorized sources of copyrighted content. A legitimate question is whether search engines should be involved in solving the rogue website dilemma. For example, is it reasonable and viable for search engines to suppress search results that direct Internet users to rogue websites?

The Copyright Office is very active in the realm of international intellectual property policy. In discussions and efforts with other countries, the United States seeks to be a leader in the development of standards and solutions. Moreover, our rightsholders are beneficiaries of the work done by the U.S. government globally. It would befit the leadership role of the United States to address the bad actors who undermine legitimate commerce on the Internet.

DUE PROCESS AND OTHER SAFEGUARDS

The Copyright Office strongly agrees with those who have stressed due process and related concerns in the context of legislating a solution to rogue websites. First, due process is a bedrock foundation of our nation's legal system, even for those who violate the law. Any remedy that impedes or obstructs access to a website must be consistent with this core American principle. The domain owner should receive notice as well as an opportunity to be heard.

Due process concerns are all the more pertinent in light of possible First Amendment implications of shutting down websites on the Internet. Care must be taken to ensure that noninfringing expression is not unnecessarily suppressed and that the relief is effective but narrowly tailored. This said, we do not believe that an order that shuts down websites devoted to infringing activity would violate the First Amendment (nor would it constitute "censorship"). We note that injunctions have long been used in copyright cases and courts have not held them to be inconsistent with free expression. Indeed, copyright itself is part of the construct of free expression in the United States. The exclusive rights of copyright allow authors and their licensees to disseminate creative expression to the public and provide incentives for them to contribute to important public discussions and the economy. Fair use and other exceptions under the law provide good faith actors with the means to make limited use of copyrighted works without permission in certain instances, such as using brief excerpts of works necessary for the dissemination of news.

Second, remedies for the rogue website problem cannot unnecessarily jeopardize the efficient operation of the Internet. Some Internet engineers have warned that some of the proposed remedies would "risk fragmenting the Internet's global domain name system (DNS) … and seriously harm the credibility of the United States in its role as a steward of key Internet infrastructure."[11] Such assertions require careful examination and the hearing of the Subcommittee today is a very helpful means of doing so. It might also be helpful to the dialogue among stakeholders if Congress were to seek the counsel of experts who can objectively evaluate technical facts as they relate to the rogue website problem. The Copyright Office believes that

[11] Open Letter from Internet Engineers to the Senate Judiciary Committee (Sept. 28, 2010), http://www.eff.org/deeplinks/2010/09/open-letter.

all players in the ecosystem would agree with this premise, including authors and other content owners, as the Internet is an extremely important platform for the dissemination of creative works.

CONCLUSION

The Copyright Office believes that the parasites who operate rogue websites undermine the incentives for legitimate commerce and if left unchecked, they threaten to weaken the robust, innovation-based markets that exist in the United States today. Though we have some successful mechanisms for copyright enforcement, there remain deficiencies in law and practice. We believe every player in the Internet ecosystem can play some role in remedying this problem, and we look forward to Congress's continued examination of the issues.

Mr. Chairman, thank you again for inviting me to speak here today. The mission of the U.S. Copyright Office is "[t]o promote creativity by administering and sustaining an effective national copyright system." We welcome the efforts of this Subcommittee and welcome any questions that you and the Subcommittee may have. As always, we at the Copyright Office stand ready to assist you in your work.

# # #