

CAHILL GORDON & REINDEL LLP
EIGHTY PINE STREET
NEW YORK, NY 10005-1702

FLOYD ABRAMS
L. HOWARD ADAMS
ROBERT A. ALESSI
HELENE R. BANKS
LANDIS C. BEST
SUSAN BUCKLEY
KEVIN J. BURKE
JAMES J. CLARK
BENJAMIN J. COHEN
CHRISTOPHER T. COX
STUART G. DOWNING
ADAM M. DWORKIN
RICHARD E. FARLEY
PATRICIA FARREN
JOAN MURTAGH FRANKEL
JONATHAN J. FRANKEL
BART FRIEDMAN
CIRO A. GAMBONI

WILLIAM B. GANNETT
CHARLES A. GILMAN
STEPHEN A. GREENE
ROBERT M. HALLMAN
WILLIAM M. HARTNETT
CRAIG M. HOROWITZ
DOUGLAS S. HOROWITZ
DAVID G. JANUSZEWSKI
ELAI KATZ
THOMAS J. KAVALER
DAVID N. KELLEY
CHÉRIE R. KISER*
EDWARD P. KRUGMAN
JOEL KURTZBERG
ALIZA R. LEVINE
JOEL H. LEVITIN
GEOFFREY E. LIEBMANN
MICHAEL MACRIS

TELEPHONE: (212) 701-3000
FACSIMILE: (212) 269-5420

1990 K STREET, N.W.
WASHINGTON, DC 20006-1181
(202) 862-8900
FAX: (202) 862-8958

AUGUSTINE HOUSE
6A AUSTIN FRIARS
LONDON, ENGLAND EC2N 2HA
(011) 44.20.7920.9800
FAX: (011) 44.20.7920.9825

WRITER'S DIRECT NUMBER

ANN S. MAKICH
JONATHAN I. MARK
BRIAN T. MARKLEY
GERARD M. MEISTRELL
MICHAEL E. MICHETTI
WILLIAM J. MILLER
ATHY A. MOBILIA
NOAH B. NEWITZ
MICHAEL J. OHLER
KENNETH W. ORCE
DAVID R. OWEN
JOHN PAPACHRISTOS
LUIS R. PENALVER
DEAN RINGEL
JAMES ROBINSON
THORN ROSENTHAL
TAMMY L. ROY
JONATHAN A. SCHAFFZIN

JOHN SCHUSTER
MICHAEL A. SHERMAN
DARREN SILVER
HOWARD G. SLOANE
SUSANNA M. SUH
JONATHAN D. THIER
JOHN A. TRIPODORO
GLENN J. WALDRIP, JR.
MICHAEL B. WEISS
S. PENNY WINDLE
COREY WRIGHT
DANIEL J. ZUBKOFF
ADAM ZUROFSKY

*ADMITTED IN DC ONLY

February 11, 2011

Chairman Patrick Leahy
Ranking Member Chuck Grassley
Senator Orrin Hatch
Senate Judiciary Committee
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

Re: COICA

Dear Chairman Leahy, Ranking Member Grassley and Senator Hatch,

I write with regard to the Combating Online Infringement and Counterfeits Act ("COICA"), which this Committee unanimously approved on November 18, 2010.¹ I represent the Directors Guild of America, the American Federation of Television and Radio Artists, the Screen Actors Guild, the International Alliance of Theatrical and Stage Employees, and the Motion Picture Association. I write to you at their request to offer my view that COICA is consistent with the First Amendment and to set forth the basis for that conclusion.

¹ Throughout this letter, I refer to the final version of the bill passed by the Judiciary Committee in the 111th Congress, S. 3804 (Reported in Senate), in anticipation of the Senate considering the bill during the 112th Congress.

In this letter, I will summarize the provisions of the statute briefly and then turn to its constitutionality under the First Amendment. I think it useful, however, to begin with some observations about copyright law and the First Amendment in the age of the Internet.

I start with what should not be controversial. The Internet is one of the greatest tools of freedom in the history of the world. That is why, as Secretary of State Clinton observed last month, there is an “urgent need” to protect freedom of expression on the Internet throughout the world. At the same time, however, she pointed out that “all societies recognize that freedom of expression has its limits,” observing specifically that those who use the Internet to “distribute stolen intellectual property cannot divorce their online actions from their real world identities” and that our ability to “safeguard billions of dollars in intellectual property [is] at stake if we cannot rely on the security of our information networks.”

It is no answer to this challenge to treat loose metaphors—the Internet as “the Wild West,” for example—as substitutes for serious legal analysis. It is one thing to say that the Internet must be free; it is something else to say that it must be lawless. Even the Wild West had sheriffs, and even those who use the Internet must obey duly adopted laws.

It is thus no surprise that libel law applies to material that appears on the Internet. *Milum v. Banks*, 642 S.E.2d 892 (Ga. Ct. App. 2007) (holding that defendant published libelous statements by posting them on his website) *cert. denied* (June 4, 2007). Or that libel precedents regarding printing information on paper are given comparable meaning as to information posted online. *Nationwide Bi-Weekly Administration, Inc. v. Belo Corp.*, 512 F.3d 137 (5th Cir. 2007) (holding that the “single publication rule” for the statute of limitations in libel suits applies to Internet publication). Or that principles of privacy law are applied to personal information posted online with the same animating principles that apply in more traditional media. *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34 (Minn. Ct. Ap. 2009) (holding that posting information from a patient’s medical file on a social networking website constitutes the “publicity” element of invasion of privacy); *Benz v. Washington Newspaper Publishing Co.*, 2006 WL 2844896 (D.D.C. Sept. 29, 2006) (holding that false information posted on independent websites provided reasonable claim for defamation, invasion of privacy and false light against private party defendant, in addition to claims regarding publication of related information by a newspaper).

Copyright law is no different. It is not disputable that “[a]ll existing copyright protections are applicable to the Internet.” Edward H. Rosenthal, *J.D. Salinger and Other Reflections on Fair Use*, 1003 PLI/Pat 35, 42 (2010). See *Video Pipeline, Inc. v. Buena Vista Home Entertainment, Inc.*, 342 F.3d 191 (3d Cir. 2003) (upholding preliminary injunction against website compiling video clips of copyrighted movies for commercial use); *UMG Recordings, Inc. v. Stewart*, 461 F. Supp. 2d 837 (S.D. Ill. 2006) (finding *prima facie* case of liability in support of default judgment against Internet user who downloaded, reproduced and distributed copyrighted audio recordings online). The seizure provisions of copyright laws are applied to seize and stop the use of online property to facilitate infringement, such as domain names, just as offline property can be seized to stop its use to facilitate infringement. *United States v. The Following Domain Names: TVShack.net et al.*, 2010 WL

2666284 (S.D.N.Y. June 29, 2010) (treating domain names hosting infringing videos as forfeitable property under 18 U.S.C. §§ 2323(a) and ordering their seizure, locking domain names at registry level, replacing registrar information to identify the government as the domain names' owner, and compelling the registry to route traffic to the domain names to a government IP address notifying the public that the domain name was seized).

Copyright law has existed throughout our Nation's history. The Constitution itself authorizes Congress to adopt copyright legislation (Art. I, Sec. 8, Clause 8) and the first such legislation was enacted in 1790, a year before the First Amendment was approved by Congress. Ch. 15, 1 Stat. 124 (1790) (repealed). From the start, injunctions were one form of relief accorded to victims of copyright infringement. (Courts applied the 1790 Act, and its later amendments, to grant injunctions "according to principles of equity." Act of Feb. 3, 1831, ch. 16, 4 Stat. at 438 (1831) (repealed 1870) (cited in Kristina Rosette, "*Back to the Future: How Federal Courts Create a Federal Common Law Copyright Through Permanent Injunctions Protecting Future Works*," 2 J. Intell. Prop. L. 325, 340 (1994)). However, since injunctions in non-copyright cases have frequently been held to be unconstitutional prior restraints on speech, *Near v. Minnesota*, 283 U.S. 697 (1931); *New York Times Co. v. United States*, 403 U.S. 713 (1971), and for other reasons, the subject has arisen as to the application, if any, of the First Amendment to copyright principles. See generally, Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* § 19E (2010).

The issue of whether and, if so, how certain elements of the Copyright Act should be read to accommodate various First Amendment interests remains open. The law could hardly be clearer, however, that injunctions are a longstanding, constitutionally sanctioned way to remedy and prevent copyright violations. Indeed, that premise was explicit in the critical concurring opinion in the Supreme Court's most famous prior restraint case, assessing publication of the Pentagon Papers, which noted that "no one denies that a newspaper can properly be enjoined from publishing the copyrighted works of another." *New York Times Co.*, 403 U.S. at 731 n.1 (White, J. and Stewart, J., concurring). Current treatises reflect this judicial consensus. "[C]ourts have found no constitutional obstacle to enjoining, pursuant to federal legislative mandate, the unlawful use of a registered trademark or copyright." Floyd Abrams & Gail Johnston, *Communications Law in the Digital Age 2010: Prior Restraints*, 1026 PLI/Pat 247, 261 (2010); James L. Oakes, *Copyrights and Copyremedies: Unfair Use and Injunctions*, 38 J. Copyright Soc'y 63, 71 (1990) ("A pirated or copied edition, record, movie, song or other work . . . cries out for an injunction").

The Supreme Court's most detailed treatment of the interrelationship between the First Amendment and copyright, the seminal case of *Harper & Row Publishers, Inc. v. Nation Entpr.*, 471 U.S. 539, 560 (1985), stressed that far from conflicting with the First Amendment, the Copyright Act actually furthers the very interests which the First Amendment protects. "First Amendment protections," the Court noted, are "already embodied in the Copyright Act's distinctions between copyrightable expression and uncopyrightable facts and ideas." The Constitution supports the explicit protection of such expression and creativity, the Court stated, within a framework that defends *both* the right to speak *and* the ability to profit from speech. "[T]he Framers intended copyright itself to be the engine of free expression," explained the Court, and "[b]y establishing a market-

able right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas." *Id.* at 558. Copyright law thus fortifies protections for speakers and creators, in a First Amendment context, while stimulating future creativity.

The evident constitutionality of injunctive relief for copyright violations does not mean, to be sure, that injunctions must automatically or always be issued in response to a copyright violation. The Supreme Court has recently held to the contrary, warning against the error of a "categorical grant" of injunctive relief for patent infringement in *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 394 (2006), and the Second Circuit has applied that conclusion in a recent, celebrated copyright case, *Salinger v. Colting*, 607 F.3d 68 (2d Cir. 2010). What *no* court has ever denied is that injunctions are a valuable and constitutional response to copyright violations.

Legislative Summary

I turn to a discussion of the bill itself. COICA is designed to enforce federal copyright and trademark law in the age of the Internet. It aims to combat the "theft of American intellectual property" on a scale that costs "American creators and producers billions of dollars per year," as this Committee's Legislative Report documented, and which results in "hundreds of thousands of lost jobs annually." S. Rep. No. 111-373, at 2 (2010).

COICA does so by strengthening the measures that the Attorney General may pursue, with court approval, to address infringing content. The bill buttresses injunctive relief to not only order offending websites to cease breaking the law, but also to compel domain names, advertising companies, financial transaction providers and Internet service providers to cease cooperating with websites that are breaking the law.

The bill does not address all types of infringement online. It focuses only on websites that are *dedicated* to profiting from infringing content or activities. COICA would establish a statutory category of websites that are "dedicated to infringing activities." This term is defined as a website that is "marketed" or "primarily designed" for infringement, or has no other "commercially significant purpose or use" besides infringement, as defined under current copyright and trademark law, and which would otherwise be "subject to civil forfeiture." Thus for copyright violations under COICA, a website must be "dedicated to infringing activities" and offering goods or services in violation of title 17 U.S.C., or facilitating such violations by means such as downloading, streaming, transmitting or linking. For trademark violations under COICA, a website must be "dedicated to infringing activities" and offering, selling or distributing goods, services or counterfeit materials in violation of section 34(d) of the Lanham Act (15 U.S.C. 1116(d)).

COICA does not alter the available remedies for private parties seeking to redress infringement. Nor does it limit the defenses that may be offered, including but not limited to that of fair use. What the bill does, beyond the current copyright framework, is add to the remedies available to the Attorney General, who would be authorized to commence actions against websites "dedicated to infringing activities." Under COICA, a federal district court "may" issue a temporary re-

straining order, a preliminary injunction or an injunction “in accordance with rule 65 of the Federal Rules of Civil Procedure.” By incorporating Rule 65, COICA applies the procedural protections that federal law currently affords all litigants in civil actions in the United States.

Under Rule 65, courts “may issue a preliminary injunction only on notice to the adverse party.” For temporary restraining orders to be issued without notice, Rule 65 requires that two conditions must be met. “[S]pecific facts in an affidavit or verified complaint [must] clearly show that immediate and irreparable injury, loss, or damage will result . . . before the adverse party can be heard in opposition.” And “the movant’s attorney certifies in writing any efforts made to give notice and the reasons why it should not be required.” Hearings for orders without notice are to be held “at the earliest possible time, taking precedence over all other matters,” under Rule 65, and the adverse party may move to dissolve or modify an order on two days’ notice to the moving party. All these protections are incorporated into COICA.

For websites registered in the United States, COICA provides for *in rem* actions to be commenced located in the judicial district where a domestic website’s domain name registrar is doing business. Once court orders are issued against domestic domains, a federal law enforcement officer shall serve the registrar, or if the registrar is abroad, then the registry. A registrar or registry receiving such an order is required to suspend or lock the domain name.

For foreign websites, COICA provides for *in rem* actions in the District of Columbia against the domain names of such websites, provided that the Attorney General simultaneously sends notice to the registrant of the domain name by postal mail and email, (using the addresses that the registrant provided to the domain name registrar), and provided that the Attorney General publishes notice of the action, as a court may direct, after its filing. Once court orders are issued against foreign domains, a federal law enforcement officer may serve such orders on three entities that work with the website in question. First, the order may be served on advertising services companies, which shall take “reasonable measures” to prevent their networks from providing advertisements to the website named in the order. Second, the order may be served on financial transaction providers, which shall stop payment transactions between U.S. customers and the website named in the order, and which shall inform the website that it is not authorized to use the transaction provider’s trademark. Third and finally, the order may be served on Internet service providers (“ISPs”), which shall take “technically feasible and reasonable steps” to block the domain name in the United States. COICA enumerates several protections for ISPs in this process, stipulating that they “shall not be required” to modify their network or facilities to comply with such orders; nor to take steps involving “domain name lookups” that are performed by entities other than their “own domain name system server”; nor to continue taking preventive actions under the order once access to the domain name has been “disabled by other means.” Under COICA, all three such entities may decide, at their discretion, how to communicate their actions to users or customers. In the event of a willful and knowing failure to comply with such orders, the Attorney General may seek injunctive relief directly against the entity in question. In such actions, COICA provides that the technological inability to comply with the underlying orders shall serve as a defense.

Entities taking actions reasonably designed to comply with court orders issued under COICA are granted immunity from causes of action based on such compliance. They are also exempted from liability for voluntarily taking the actions stipulated against websites dedicated to infringing activity in COICA, provided that such actions are taken based on the reasonable belief that the websites are dedicated to infringing activity.

First Amendment Considerations

Having discussed the broad constitutional and copyright framework for COICA, and described what the bill does in basic terms, I now turn to two potential First Amendment issues in analyzing COICA: the breadth of the regulatory framework's impact on speech, and its procedural protections in a First Amendment context.

Potential Overbreadth

It is a fundamental principle of First Amendment jurisprudence that government restrictions on speech should be narrowly tailored to avoid unnecessarily burdening protected speech. Courts apply strict scrutiny to statutes that potentially interfere with protected speech, with special attention for rules that may sweep too broadly. Like any statute impacting speech, Congress must consider the potential overbreadth of COICA's statutory structure and remedies in light of these First Amendment considerations.

COICA is not constitutionally overbroad. First, it sets a rather high bar in defining when a website or domain is eligible for potential actions by the Attorney General. Second, its remedies are focused on preventing infringing content at the distribution point where website operators choose to infringe. Finally, the application of Federal Rule 65 serves as a check on overbreadth.

COICA is not designed to regulate the entire Internet. Nor is it designed to counter the vast array and forms of online infringement, which are subject to various laws already on the books. COICA focuses, instead, on a narrow category of entities which are not simply trafficking in some infringing content, or occasionally breaking federal laws, but which are primarily and continuously devoted to providing and selling infringing content in the United States. Since COICA specifically defines a rigorous standard of websites that are "dedicated to infringing activities," actions under COICA require a showing that a target website is both violating federal law and operating with the main function of continuous infringement. Therefore, any website devoted to legal activities, such as commentary, socializing or commerce, cannot be pursued under COICA if it occasionally or even repeatedly practices infringement.

For websites and domains that meet COICA's definition, injunctive relief would be issued to address infringement at its distribution point. Thus an individual choosing to use a website or domain to practice infringement faces relief at the point of infringement, be that a particular website address or a domain name devoted to infringement. This approach constitutes a narrowly tai-

lored means to prevent future infringement, with a court making the final determination as to whether and how to craft injunctive relief “against the domain name used by an Internet site . . . to cease and desist from undertaking any further activity in violation” of COICA, S. 3804 (Reported in Senate) at 17. Such relief tracks equitable remedies in traditional copyright law, such as forfeiture or impoundment. 17 U.S.C. § 506(b) (forfeiture); 17 U.S.C. § 503 (impoundment). In the online context, distribution may occur only at a single website address, in which case injunctive relief may block that address via orders served on the domain name registrar, registry or ISP. Or distribution may occur across a domain, in which case injunctive relief may block the domain via orders served on the domain name registrar, registry or ISP. Some protected and non-infringing content may be implicated in this process, but such content would have to be hosted in conjunction with an entity that is dedicated to infringement. Even without such a high bar, of course, the presence of non-infringing speech generally does not provide a copyright violator with immunity from enforcement actions. The First Amendment allows government regulations to prevent piracy that clearly have an incidental impact on non-infringing speech. *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1129 (N.D. Cal. 2002) (noting that the First Amendment allows the government to pursue online infringement with an “incidental restriction” on First Amendment freedoms, so long as the traditional test is met that the “means chosen do not burden substantially more speech than is necessary to further the government’s legitimate interests.”) (internal citations omitted). Furthermore, and independent of a potential statutory framework such as that set forth in COICA, courts already approve, on a case-by-case basis, copyright seizures of domain names that can result in the blockage of some non-infringing content. Indeed, some such seizures apply current forfeiture laws to permanently seize a domain name as property. *United States v. TVShack.net et al.*, 2010 WL 2666284 (S.D.N.Y. June 29, 2010) (treating domain names hosting infringing videos as forfeitable property under 18 U.S.C. §§ 2323(a) and ordering their seizure).

If an order under COICA does result in blocking some non-infringing content, COICA is sufficiently narrow to accommodate the immediate publication of that content elsewhere and the future publication of the content on the same domain. First, by definition, any non-infringing content is not specifically enjoined by the order, so it may still be legally posted anywhere else online. Second, such content can be unblocked or reposted *on the same* website or domain name in the future, once the infringing content at issue is removed. Indeed, the content can be unblocked or reposted precisely because the domain name itself, as property, is not forfeited by an order pursuant to COICA. Thus after the infringement issue is resolved and the site operator is in compliance with federal law, the domain name can post its archived non-infringing content.

In addition, it is worth noting that a website may meet COICA’s “dedicated to infringement” standard based on its links to other websites providing infringing content, apart from whether or not the linking website technically hosts infringing content on its own site or servers. COICA provides that such websites may be dedicated to infringement by providing “aggregated links to other sides or Internet resources for obtaining” infringing content. Just as with posting infringing content, however, such a site must meet the high bar of being “marketed” or “primarily designed” for infringement, or having no other “commercially significant purpose or use” besides infringement. This is consistent with caselaw regarding online copyright infringement, since

“[l]inking to infringing material” can create liability, 1003 PLI/Pat 35 at 43. When a website links to infringing content, or links to technology to facilitate infringement, courts look to whether the website operator knowingly linked to facilitate violations of the law. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (holding defendant violated Digital Millennium Copyright Act by linking to program to unlock DVDs for unauthorized copying, and requiring knowing linking for the purpose of disseminating the program); *Bernstein v. JC Penney, Inc.*, 50 U.S.P.Q.2d 1063 (C.D. Cal. 1998) (plaintiff did not have a claim for mere linking to website without knowledge of infringing material on the site). Injunctions issued specifically against linking, in order to thwart copyright infringement, have also been held to be consistent with the First Amendment. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). Furthermore, in recent enforcement actions against domain names, the U.S. Department of Homeland Security specifically seized “‘linking’ websites” that provide “links to files on third party websites that contain illegal copies of copyrighted content.” (Aff. ¶ 13) *United States v. The Following Domain Names: HQ-Streams.com et al.*, 2011 WL 320195 (S.D.N.Y. Jan 31, 2011). Given these precedents, potential actions pursuant to COICA against websites dedicated to infringing content based on extensive and continuous linking to facilitate infringement appear to rest on a solidly constitutional foundation. As for overbreadth in the linking context, it appears clear that neither a few inadvertent links to infringing material on an otherwise lawful website, nor some links to infringing websites for the purposes of public information or education, could be held to meet COICA’s threshold.

Procedural Protections

The procedural protections under COICA are so strong, uniform and constitutionally rooted that it is no exaggeration to observe that any complaints in this area are not really with the bill, but with the Federal Rules of Civil Procedure itself, which governs all litigants in U.S. federal courts.

COICA incorporates Rule 65 to provide the process governing how a judge “may” issue a temporary restraining order, preliminary injunction, or permanent injunction. Thus website operators subject to COICA would benefit from the same procedural safeguards afforded litigants in all other U.S. civil actions. For preliminary injunctions, those safeguards require notice in advance. For temporary restraining orders, the safeguards include first, the requirement that temporary restraining orders issued without notice must be based on specific facts showing the prospect of immediate and irreparable damage “before the adverse party can be heard in opposition” (emphasis added); and second, a written certification by, in this case, the U.S. government’s attorney, explaining efforts made to give notice and the reasons it should not be required in this instance. Subsequent hearings for orders without notice are a first priority under Rule 65, which also grants the adverse party the option of moving to dissolve an order with two days’ notice.

In addition to those well-established procedures, COICA also explicitly requires the Attorney General to conduct service of process by sending notice of an intent to proceed under COICA to the domain name registrant. Consistent with the objectives of Rule 65, this requirement

provides an opportunity to operators of allegedly infringing websites to defend themselves before an order is issued. In the event that operators prefer to respond later, or only learned of injunctive action later because they did not provide accurate contact information to their registry, they also retain their rights to seek later relief from the order by disputing the allegations or appealing to the interests of justice. It is worth noting that federal copyright law disfavors the submission of false contact information to a domain name registrar, treating the knowing provision of “materially false contact information to a domain name registrar” as a rebuttable presumption of willful infringement. 17 U.S.C.A § 504(c); *Chanel, Inc. v. Cui*, 2010 WL 2835749 (S.D.N.Y. July 7, 2010) (entering default judgment for permanent injunction against product trademark infringement and finding willful conduct based, in part, on defendant’s repeated submissions of “false information in registering domain names” used for infringement). Indeed, the rules for registration of domain names require the provision of accurate contact information. Registrar Accreditation Agreement, section 3.7.7.1 (May 21, 2009), available at <http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3> (registrants required to provide registrar accurate and reliable contact details). Finally, since COICA states that courts “may” issue preliminary injunctions or injunctions, the range of available remedies includes the prospect of a final—not preliminary—resolution of the dispute.

Once COICA’s required procedural protections are satisfied, it is still possible that some operators of allegedly infringing websites will knowingly decline to participate in U.S. court proceedings. Such a choice, after legitimate notice and procedural safeguards are provided, can lead to *ex parte* proceedings and default judgments. Courts routinely enter default judgments in civil lawsuits, including comparable online copyright cases. After initial notice has been served, courts grant permanent injunctive relief for copyright violations in default judgments without additional attempts at notice. *Disney Enterprises, Inc. v. Farmer*, 427 F.Supp. 2d 807 (E.D. Tenn. 2006) (issuing permanent injunction barring infringement of copyright by website distributing copyrighted movies over peer-to-peer network, with default judgment entitled without additional service of notice on defendant); *Priority Records, LLC v. Bradley*, 2007 WL 465754 (E.D. Mich. Feb. 8, 2007) (issuing permanent injunction in default judgment against defendant using online distribution system to download and distribute copyrighted recordings).

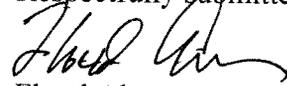
Conclusion

I am aware that COICA has been criticized on First Amendment-related grounds by organizations such as the American Civil Liberties Union and certain human rights groups, organizations for which I have the highest regard. The core of their concern about the bill seems anchored in the view that the United States would be less credible in its criticism of nations that egregiously violate the civil liberties of their citizens if Congress adopts COICA.

I disagree. Copyright violations are not protected by the First Amendment. Entities “dedicated to infringing activities” are not engaging in speech that any civilized, let alone freedom-oriented, nation protects. That these infringing activities occur on the Internet makes them not less, but more harmful. The notion that by combating such acts through legislation, the United States

would compromise its role as the world leader in advancing a free and universal Internet seems to me insupportable. As a matter of both constitutional law and public policy, the United States must remain committed to defending both the right to speak and the ability to protect one's intellectual creations. This legislation does not impair or overcome the constitutional right to engage in speech; it protects creators of speech, as Congress has since this Nation was founded, by combating its theft.

Respectfully submitted,



Floyd Abrams*

cc: Directors Guild of America
American Federation of Television and Radio Artists
Screen Actors Guild
International Alliance of Theatrical and Stage Employees
Motion Picture Association

* I thank my associate and colleague, Ari Melber, for his assistance in all aspects of the preparation of this submission.

February 15, 2011

Rogue Sites are Stealing American Jobs and Hurting Consumers!

To the Members of the United States Congress:

The more than 80 undersigned businesses and professional and labor organizations, representing over **1.5 million jobs and workers**, and more than 50 trade associations representing thousands of companies, urge you to make it a priority to enact legislation that will provide the government with enhanced tools to disrupt the efforts of those who use websites to make illegal profits by stealing the intellectual property (IP) of America's innovative and creative industries. These rogue websites are part of a network of counterfeiting and piracy that a recent study found cost 2.5 million jobs in the G20 economies.

Many of these sites pose as legitimate businesses, luring consumers with sophisticated and well-designed websites. But, in reality, the counterfeit and pirated products these sites distribute are often of poor quality, harmful, and promote fraud. Further, consumers put themselves at risk of identity theft and malicious computer viruses by visiting these sites. Legislation to disrupt these efforts is a major step to make the Internet safer and protect consumers from the dangers of buying in the online marketplace.

IP-intensive industries are a cornerstone of the U.S. economy, employing more than 19 million people and accounting for 60 percent of our exports. Rampant online counterfeiting and piracy presents a clear and present threat that we must do more to address. A recent study examined about 100 rogue websites and found that these sites attracted more than 53 billion visits per year. That averages about 9 visits for every man, woman, and child on Earth. It is not surprising that global sales of counterfeit goods via the Internet from illegitimate retailers reached \$135 billion in 2010. What's more, as a consequence of global and U.S.-based piracy of copyright products, the U.S. economy lost \$58.0 billion in total output in 2007.

The United States cannot and should not tolerate this criminal activity. As the studies show, the theft of American IP is the theft of American jobs. And rogue sites negatively impact the health and safety of American citizens. Last year, Senator Patrick Leahy and Senator Orrin Hatch introduced S. 3804 to combat rogue sites and were joined by an impressively bipartisan group of 18 additional Senators. That bill was approved by the Senate Judiciary Committee 19-0. In the House of Representatives, Judiciary Committee Chairman Lamar Smith and Ranking Member John Conyers have long recognized the harm from IP theft and supported efforts to address it. We urge you to support bicameral introduction and enactment of carefully balanced rogue sites legislation this year and look forward to working with you in support of that goal.

Sincerely,

1-800-PetMeds
ABRO Industries, Inc.
Acushnet Company
adidas America

Advanced Medical Technology Association (AdvaMed)
Alliance of Automobile Manufacturers
Alliance of Visual Artists (AVA)
American Association of Independent Music
American Board of Internal Medicine
American Federation of Musicians
American Made Alliance
American Society of Composers, Authors and Publishers (ASCAP)
American Society of Media Photographers
Anti-Counterfeiting and Piracy Initiative (ACAPI)
Association of American Publishers (AAP)
Association of Equipment Manufacturers
Association of Test Publishers
Autodesk, Inc.
Beachbody, LLC
Beam Global Spirits & Wine
Bose Corporation
Brigid Collins Family Support Center
Broadcast Music, Inc. (BMI)
Cascade Designs Incorporated
Cengage Learning
CFA Institute
Chanel USA
Christian Music Publishers Association
Coalition Against Counterfeiting and Piracy (CACCP)
Commercial Photographers International
Copyright Clearance Center (CCC)
Country Music Association
Electronic Components Industry Association (ECIA)
Entertainment Software Association (ESA)
ERAI, Inc.
The Estee Lauder Companies
Evidence Photographers International Council
Ex Officio
Exxel Outdoors
Far Bank Enterprises
Fashion Business Incorporated
Federation of State Boards of Physical Therapy
Ford Motor Company
Fortune Brands, Inc.
Gemvision Corporation
Gospel Music Association
Governors America Corp.
Graduate Management Admission Council
Greeting Card Association (GCA)
Harry Fox Agency

Hastings Entertainment, Inc.
IDS Publishing
Imaging Supplies Coalition (ISC)
Independent Distributors of Electronics Association (IDEA)
Innate-gear
Intellectual Property Owners Association
International Trademark Association (INTA)
John Wiley & Sons, Inc.
Kekepana International Services
Leatherman Tool Group, Inc.
Lexmark International, Inc.
LVMH Moët Hennessy Louis Vuitton
Major League Baseball
Marmot
The McGraw-Hill Companies
Messy Face Designs, Inc.
MicroRam Electronics, Inc.
Monster Cable Products, Inc.
Motion Picture Association of America, Inc. (MPAA)
Music Managers Forum-U.S.
Nashville Songwriters Association International
National Association of Broadcasters
National Association of Manufacturers
National Association of Recording Merchandisers
National Association of Theatre Owners (NATO)
National Basketball Association (NBA)
National Football League (NFL)
National Music Publishers' Association (NMPA)
NBCUniversal
Nervous Tattoo Inc., dba Ed Hardy
New Era Cap Co Inc
News Corporation
Nike, Inc.
Nintendo of America Inc.
Oakley, Inc.
OpSec Security, Inc.
Outdoor Industry Association
Outdoor Power Equipment Institute (OPEI)
Outdoor Research, Inc
Pacific Component Xchange, Inc.
Pearson Education
Personal Care Products Council
Petzl America
Picture Archive Council of America (PACA)
PING
Professional Photographers of America

Quality Float Works, Inc.
The Recording Academy (National Academy of Recording Arts and Sciences)
Recording Industry Association of America (RIAA)
Reebok International Ltd.
Reed Elsevier Inc.
Romance Writers of America (RWA)
Rosetta Stone Inc.
Schneider Electric
SESAC, Inc.
SG Industries, Inc.
Small Business & Entrepreneurship Council
SMT Corp.
Society of Sport & Event Photographers
Software & Information Industry Association (SIIA)
Sony Music Entertainment
Sony Pictures Entertainment
SoundExchange
Specialty Equipment Market Association (SEMA)
Sports Rights Owners Coalition
Spyder Active Sports, Inc
Stock Artist Alliance
Stuart Weitzman Holdings, LLC
Student Photographic Society
SunRise Solar Inc.
Taylor Made Golf Company, Inc.
Tiffany & Co.
The Timberland Company
Time Warner Inc.
Toshiba America Business Solutions, Inc.
U.S. Chamber of Commerce
Ultimate Fighting Championship
Underwriters Laboratories Inc.
Universal Music Group
Viacom
Vibram USA, Inc
W.R. Case & Sons Cutlery Co.
The Walt Disney Company
Warner Music Group
Winestem Company
Xerox Corporation
Zippo Manufacturing Company

Written Testimony Submitted for the Record of

Daniel Castro

Senior Analyst, Information Technology and Innovation Foundation (ITIF)

on

“Targeting Websites Dedicated To Stealing American Intellectual Property”

before the

Senate Committee on the Judiciary

U.S. Senate

February 12, 2011

Legislation introduced in Congress in 2010, such as S. 3804, the “Combating Online Infringement and Counterfeits Act” (COICA), would take an aggressive and needed stand against online piracy and counterfeit goods, a growing problem that hurts American consumers and costs Americans jobs. Critics of the legislation argue that this bill would hurt free speech, encourage censorship in foreign countries, and cripple the technological infrastructure on which the Internet runs. Not only is this criticism untrue, but more robust enforcement of digital copyrights would likely lead to a stronger Internet ecosystem and more innovative content and services for consumers.

The Problem of Digital Piracy

Software, video games, movies, music, books, photos, and other media are increasingly available to users online. Many users go online and pay for digital content or applications through sites like Amazon, iTunes or Netflix. And the advent of new services like Google TV suggests that consumers will increasingly use the Internet to enjoy video programming on their PCs, in their living rooms and on their mobile devices. But all too many Internet users are choosing to download pirated digital content from illegal sites or peer-to-peer (P2P) networks. The problem has become so pervasive that at least 1 in 4 bits of traffic on the Internet is related to infringing content.¹ The Information Technology and Innovation Foundation (ITIF) has previously documented how Internet users can easily go online and, with just a few clicks, find pirated copies of full-length Hollywood movies or television programming to watch for free or software programs to use on their computers.² Many of these sites earn advertising dollars from major companies. For example, in ITIF’s 2009 review of the websites The Pirate Bay and isoHunt, we found brands such as Amazon.com, Blockbuster, British Airways, and Sprint appearing on these sites.³

Online piracy has a significant impact on the U.S. economy. While the exact cost of piracy is difficult to measure, the impact is substantial, with one estimate finding that the U.S. motion picture, sound

recording, business software, and entertainment software/video game industries lost over \$20 billion dollars in 2005 due to piracy, and retailers lost another \$2 billion, for a combined loss of over \$22 billion.⁴ Online piracy harms the artists, both the famous and struggling, who create content, as well as the technicians—sound engineers, editors, set designers, software and game programmers—who produce it. Piracy ultimately also hurts law-abiding consumers who must pay higher prices for content, enjoy less content or relatively lower quality content, or pay higher prices for Internet access to compensate for the costs of piracy.

Potential Legislative Responses

In December 2009, ITIF proposed a number of policies to help reduce online copyright infringement, especially in countries that turn a blind eye to copyright enforcement.⁵ These recommendations include the following:

- Create a process by which the federal government, with the help of third parties, can identify websites around the world that are systemically engaged in piracy
- Enlist ISPs to combat piracy by blocking websites that offer pirated content
- Enlist search engines to combat piracy by removing websites that offer infringing content from their search results
- Require ad networks and financial service providers to stop doing business with websites providing access to pirated content
- Create a process so that the private sector can consult with government regulators on proposed uses of anti-piracy technology
- Fund anti-piracy technology research, such as content identification technology
- Pursue international frameworks to protect intellectual property and impose significant pressure and penalties on countries that flout copyright law

Many of these recommendations have been considered in recent legislation, such as COICA, introduced by Senators Patrick Leahy (D-VT) and Orrin Hatch (R-UT) in 2010. COICA would provide important new tools to crack down on online infringement of intellectual property. The legislation would not target minor violations of copyright, but rather would target “Internet sites dedicated to infringing activities” which it defines as a site that is “primarily designed, has no demonstrable, commercially significant purpose or use other than, or is marketed by its operator...to offer” unauthorized access to copyright-protected content.

Response to Criticism of Legislation

Critics of COICA make three general objections: 1) that the legislation would impair free speech; 2) that the legislation would encourage censorship in foreign countries; and 3) that the legislation would cripple the technological infrastructure on which the Internet runs. All of these objections are unfounded.

Freedom of Speech

First, some critics oppose the legislation on the grounds that it would hurt free speech, a groundless accusation. Not all free speech is protected. As Justice Holmes in *Schenck v. U.S.* famously argued, freedom of speech does not include the freedom to falsely yell “Fire” in a crowded theater (or more recently “Bomb!” on an airplane).⁶ Nor does it entail a freedom to establish a website for the sole purpose of enabling online piracy, even if the site posts a few statements expressing the owners’ political views.

Neither does the idea of a “free and open” Internet mean that every website has the right to exist. Certainly, most people would agree that some websites should not be permitted to remain online, such as sites devoted to hosting child pornography or illegal scams. The purpose of this legislation is not to shut down a personal website that accidentally links to a copyrighted image or websites that use material protected by fair use, but to shut down websites whose principal purpose is to engage in egregious infringement of intellectual property.

Yet critics of the legislation, such as the Electronic Frontier Foundation (EFF), complain that free speech will be hurt if the government blocks “a whole domain, and not just the infringing part of the site.”⁷ While certainly most infringing sites will contain at least some non-infringing content, it is not an injustice to block the entire site. As noted, the legislation only applies to sites where the principal purpose of the site is to engage in digital piracy. Such frivolous complaints are equivalent to arguing that the justice system would be unfair to shut down a bar found to be repeatedly serving alcohol to minors even if some of its customers were of legal age or a pawn shop that serves as a front for moving stolen goods even if a few of its items were acquired legally.

Others present a similar criticism of the legislation under the guise of protecting free speech when their objection is really to an expansion of government authority. This mentality is exemplified by Bruce Schneier who as a matter of course argues against virtually any action by government to police abuses on the Internet.⁸ These kinds of objections come from a purely anti-government ideology that rejects any attempt to give government more power, even if that is appropriate power to enforce laws against criminals.

Foreign Censorship

Critics also claim that COICA would set a negative precedent and harm the United States internationally by giving political cover to the “totalitarian, profoundly anti-democratic regimes that keep their citizens from seeing the whole Internet.”⁹ Critics, such as the 87 Internet engineers who signed EFF’s letter to the Judiciary Committee, argue that the legislation would “seriously harm the credibility of the United States in its role as a steward of key Internet infrastructure.” Others, including groups like the American Library Association, Consumer Electronics Association, NetCoalition and Public Knowledge, argue that “COICA’s blacklist may be used to justify foreign blacklists of websites that criticize governments or royalty, or that contain other ‘unlawful’ or ‘subversive’ speech.”¹⁰ Again, these criticisms do not stand up to a serious analysis. This is equivalent to arguing that the United States should not put rioters who engage in wholesale property destruction and violence in jail because it simply encourages totalitarian governments to use their police to suppress their citizens.

More narrowly, some critics, such as Wendy Seltzer at Princeton University's Center for Information Technology Policy, argue that other countries would use anti-piracy efforts as a ruse for cracking down on political dissidents.¹¹ Such activities are not without precedent—Russian police have raided advocacy groups and opposition newspapers that have spoken out against the government in the name of searching for pirated software.¹² Yet while certainly some unscrupulous countries might claim their actions are equivalent to that of the United States, it would be demonstrably untrue. There is simply no comparison between a country using clear and transparent legal means to enforce intellectual property rights online and a country censoring political speech online, even under the guise of protecting copyrights. Moreover, to argue that abusive regimes operating without the rule of law would somehow act more abusively because the United States cracks down on cyber crime is a stretch at best. If this were the case, we should have seen a dramatic increase in Internet censorship after nations like France and the U.K recently passed laws to crack down on online copyright theft.

In fact, if this law would have any effect on foreign nations it would be to embolden them to take stronger steps to crack down on digital piracy, a problem that is even worse in many foreign nations and one that contributes to a deteriorating balance of trade for the United States as foreign consumers steal U.S. software, music, video games, movies, books, photos, and other digital content.

Weaken the Internet

Finally, some opponents of stricter online IP enforcement argue that this legislation “will risk fragmenting the Internet's global domain name system (DNS).”¹³ To understand the debate, you must understand how DNS works. DNS is like a global phonebook for the Internet providing users a number that corresponds to each name. Before a user can visit a domain name (e.g. www.itif.org), his or her computer must first discover the IP address associated with that web address (e.g. 69.65.119.60). DNS servers provide this service to users by translating domain names into IP addresses through a recursive process. Most users rely on the DNS servers of their local ISP for this service and it is these DNS servers that are the principle target of COICA. If a site appeared on the government blacklist, e.g. www.watch-pirated-videos.tv, then the DNS servers would be instructed to no longer resolve an IP address for that domain. And without this IP address, users cannot visit these infringing websites.

Groups like EFF claim this will “undermine basic Internet infrastructure” and lament that it will keep ISPs from “telling you the truth about a website's location.”¹⁴ While such fiction may be useful in generating fear about COICA, the simple fact is that using DNS to block access to websites or servers is not new or particularly challenging—it has been used for blocking spam and protecting users from malware, for example, for many years. In addition, many DNS resolvers routinely return different answers to users as part of a service, such as to provide parental filters, correct typos in URLs, or to provide search results in lieu of a basic “domain not found” error.¹⁵

Other critics, such as the Center for Democracy and Technology, argue that COICA will set a precedent where ISPs will be required to block other “illegal or unsavory content” creating “a controlled, ISP-policed medium.”¹⁶ Such an end result is antithetical to the worldview of CDT (and other opponents of this legislation) that the Internet should be free of private-sector control regardless of the consequences. This “slippery slope” argument is fundamentally illogical. The analogy would be like

saying that if we pass laws against a person committing physical assault on another person, then it is only a matter of time before we pass laws against people bumping into each other rudely on the street. Such stubborn and entrenched views do not reflect the kind of flexible policymaking that most people agree is necessary for the fast-paced world of the evolving Internet. Rather than relying on tradition to justify Internet policy, a better approach would be to look at the practical implications of specific policy proposals in the present.

Why the Criticism?

So what's really behind these criticisms? They all reflect these groups' and individuals' overarching view of the Internet as a medium whose chief function is to liberate individuals from control by, or dependence on, big organizations. For these groups, the Internet is first and foremost about individual freedom, not about collective responsibility. They see the Internet as a special place, above and beyond the reach of the kinds of rules that govern the offline world. Yet, for most of the rest of us, the Internet is no different than the rest of society where we have rights and responsibilities and where laws against certain behaviors exist. We play by the rules and we expect others to do the same, and when they do not, we expect society (through the actions of democratically elected governments) to step in and punish those who commit crimes. All of these objections listed here reflect this fundamental Internet exceptionalist ideology, and as such are largely attacks not so much on this particular legislation, but on any legislation that would put limits on Internet freedom, even if it's the freedom to falsely yell "fire!" in a crowded theatre.

Because of their overriding focus on individual freedom and not on collective benefit, critics of the legislation fail to understand that stronger enforcement of intellectual property would be beneficial to American consumers and businesses. For example, delivering video content to the TV is expected to be the next driver of broadband access and services but for this business model to work, content owners and creators should be able to ensure their rights are protected. Online piracy not only results in the unauthorized distribution of content, it hurts the ability of content producers to create legitimate business models for selling digital content. As the saying goes, "It's hard to compete with free." While many companies have rallied to the challenge and created compelling businesses to sell content legally, on the whole, illegal content still remains widely available and commonplace.

Conclusion

COICA is important because it recognizes that online piracy is no longer about college students trading files in their dorm room, but instead it has grown in to a multi-million dollar international business. Sites hosting pirated content or linking to pirated content can generate a significant amount of revenue from online advertising and sales. COICA would provide a mechanism to not only cut off access to these sites, but also cut off their funding mechanisms to make operating online piracy sites unprofitable.

Should we throw out freedom of speech and long-held legal protections like due process just to protect intellectual property online? Of course not. But neither should we abandon the Constitutional provisions which support protecting intellectual property. As with any law enforcement initiative, efforts at

reducing online piracy involve balancing costs and benefits. While street crime could be reduced by doubling the number of police, most communities find an equilibrium where the marginal cost of an additional police officer does not outweigh the corresponding reduction in crime. With regard to Internet piracy, it is hard to argue that this equilibrium has been reached and that society would not be better off with greater efforts to stop digital piracy. While not all anti-piracy efforts should be embraced—for example, policymakers are wise to shy away from expensive digital rights management (DRM) technology mandates—the government should make a serious effort to combat piracy through reasonable approaches like COICA. The extent of piracy is so large, and the costs of enforcement quite reasonable, that it is clearly in the public interest to take more aggressive steps to curb it. Legislation such as COICA provides an opportunity for the U.S. government to get serious about enforcing intellectual property rights online.

-
- ¹ David Price, “An Estimate of Infringing Use of the Internet,” *Envisional* (2011), http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.
 - ² Daniel Castro, Richard Bennett, and Scott Andes, “Steal These Policies: Strategies for Reducing Digital Piracy,” *Information Technology and Innovation Foundation* (Washington, DC: 2009), <http://www.itif.org/files/2009-digital-piracy.pdf>.
 - ³ *Ibid.*
 - ⁴ Stephen Siwek, “The True Cost of Copyright Industry Piracy to the U.S. Economy,” *Policy Report 189*, The Institute for Policy Innovation, September 2007.
 - ⁵ Castro, Bennett and Andes, “Steal these Policies.”
 - ⁶ “The man who said ‘bomb’ on an airplane,” *San Francisco Chronicle*, August 6, 2010, http://www.sfgate.com/cgi-bin/blogs/crime/detail?entry_id=69558 and “Woman accused of airport bomb threats,” *United Press International*, April 21, 2008, http://www.upi.com/Top_News/2008/04/21/Woman-accused-of-airport-bomb-threats/UPI-38521208794796/.
 - ⁷ Richard Esguerra, “Censorship of the Internet Takes Center Stage in ‘Online Infringement’ Bill,” *Electronic Frontier Foundation*, September 21, 2010, <http://www.eff.org/deeplinks/2010/09/censorship-internet-takes-center-stage-online>.
 - ⁸ For example, with regards to the Obama Administration’s plans to expand wiretapping online Schneier writes, “it’s bad civic hygiene to build technologies that could someday be used to facilitate a police state.” Bruce Schneier, “Web snooping is a dangerous move,” *CNN.com*, September 29, 2010, <http://www.cnn.com/2010/OPINION/09/29/schneier.web.surveillance/index.html>.
 - ⁹ Esguerra, “Censorship of the Internet Takes Center Stage in ‘Online Infringement’ Bill.”
 - ¹⁰ Letter from Public Knowledge et al. on “S. 3804, Combating Online Infringement and Counterfeits Act (COICA), September 27, 2010, <http://www.publicknowledge.org/files/docs/JointLetterCOICA20100929.pdf>.
 - ¹¹ Wendy Seltzer, “Copyright, Censorship, and Domain Name Blacklists at Home in the U.S.,” *Freedom to Tinker*, September 21, 2010, <http://www.freedom-to-tinker.com/blog/wseltzer/copyright-censorship-and-domain-name-blacklists-home-us>.
 - ¹² Clifford Levy, “Russia Uses Microsoft to Suppress Dissent,” *New York Times*, September 11, 2010, <http://www.nytimes.com/2010/09/12/world/europe/12raids.html>.
 - ¹³ Peter Eckersley, “An Open Letter From Internet Engineers to the Senate Judiciary Committee,” *Electronic Frontier Foundation*, September 29, 2010, <http://www.eff.org/deeplinks/2010/09/open-letter>.
 - ¹⁴ Esguerra, “Censorship of the Internet Takes Center Stage in ‘Online Infringement’ Bill.”
 - ¹⁵ For a more detailed rebuttal of some of the technical fears about COICA, see Daniel Castro, “No, COICA Will Not Break the Internet,” *Innovation Policy Blog* (2011), <http://www.innovationpolicy.org/no-coica-will-not-break-the-internet>.
 - ¹⁶ “The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet’s Open Architecture,” *Center for Democracy and Technology*, September 28, 2010, http://cdt.org/files/pdfs/Leahy_bill_memo.pdf.

AMERICAN FEDERATION OF LABOR AND CONGRESS OF INDUSTRIAL ORGANIZATIONS



815 SIXTEENTH STREET, N.W.
WASHINGTON, D.C. 20006

RICHARD L. TRUMKA
PRESIDENT

ELIZABETH H. SHULER
SECRETARY-TREASURER

ARLENE HOLT BAKER
EXECUTIVE VICE-PRESIDENT

LEGISLATIVE ALERT!

(202) 637-5057

February 15, 2011

The Honorable Patrick Leahy, Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy:

On behalf of the AFL-CIO, I want to thank you for holding a hearing on “Targeting Websites Dedicated to Stealing American Intellectual Property.” This hearing demonstrates that, despite being unfairly attacked for introducing S.3804, the “Combating Online Infringement and Counterfeits Act” (COICA) in the last Congress, you remain appropriately focused on combating the torrent of digital theft that robs U.S. jobs while threatening the health and safety of U.S. citizens. American workers greatly appreciate the courage and leadership you have once again displayed.

This Congress must pass legislation to provide more effective tools against “rogue websites” operated by unscrupulous individuals who use the Internet as a platform to sell counterfeit and pirated goods. As you know, many of these rogue websites look legitimate and have become increasingly sophisticated in both design and operation. They deceive consumers into believing they are legitimate, threaten American jobs, and as we have seen with the recent instances of fake products such as toothpaste, pharmaceuticals and auto parts, represent a severe health and safety risk to U.S. citizens. This hearing will help Congress decide which additional tools would be most appropriate and effective for combating such “rogue websites.”

The AFL-CIO will stand by you as you try to halt the destruction of American jobs by rogue websites. Last fall, more than a dozen unions and guilds, representing hundreds of thousands of workers in industries ranging from entertainment to firefighting, wrote you in support of S. 3804. I assure you that these unions and guilds were not outliers; the labor community as a whole understands that digital intellectual property (IP) theft affects not only jobs in the entertainment industry, where lost profits in music and motion picture production put tens of thousands of good-paying jobs at risk, but also jobs in manufacturing, such as pharmaceuticals, apparel, luxury goods, and auto parts. In all, counterfeiting and piracy of intellectual property has an impact on millions of American workers in IP-sensitive industries.

The Honorable Patrick Leahy
February 15, 2011
Page 2

We thank you again for your efforts to fight for workers and their families, and to protect both their jobs and their safety. We look forward to continuing to work with you and your Senate colleagues to enact COICA.

Sincerely,

A handwritten signature in black ink, appearing to read "William Samuel". The signature is fluid and cursive, with the first name "William" and last name "Samuel" clearly distinguishable.

William Samuel, Director
Government Affairs Department



Statement of the U.S. Chamber of Commerce

ON: "Targeting Websites Dedicated To Stealing American Intellectual Property"

TO: United States Senate Committee on the Judiciary

DATE: Wednesday, February 16, 2011

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96 percent of the Chamber's members are small businesses with 100 or fewer employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business -- manufacturing, retailing, services, construction, wholesaling, and finance -- is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber of Commerce's 115 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross-section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 business people participate in this process.

Testimony of Steven M. Tepp
Senior Director, Internet Counterfeiting and Piracy
Global Intellectual Property Center
U.S. Chamber of Commerce

Chairman Leahy, Ranking Member Grassley, Senator Hatch, and Members of the Judiciary Committee; thank you for your recognition of the problems created by rogue websites and the need for Congressional action in this area. The U.S. Chamber of Commerce appreciates your leadership and the opportunity to submit this testimony.

Recognizing the fundamental importance of intellectual property (IP) protection and enforcement to the future of American business, the Chamber's Global Intellectual Property Center (GIPC) leads a world-wide effort to protect innovation and creativity by promoting strong intellectual property rights and norms around the world. We recognize that these rights are vital to creating jobs, saving lives, advancing global economic growth, and generating breakthrough solutions to global challenges. The GIPC represents a broad spectrum of intellectual property-intensive companies and leads the over 700-member Coalition Against Counterfeiting and Piracy, the largest business coalition dedicated to fighting the growing threat of counterfeiting and piracy to the economy, jobs, and consumer health and safety.

The Harm from Rogue Websites

Rogue websites, those dedicated to counterfeiting and piracy, are harming our economy, depriving America of jobs and tax revenues, and exposing American consumers to harm and fraud. By perverting the incredible power of the Internet as a tool of legitimate distribution of goods and services, the operators of rogue sites have expanded their criminal enterprises to heretofore unthinkable levels. The existence of online piracy and counterfeiting is well-known, as is its massive scope. But several recent studies lay out the problem in numbers that have stunned even the most jaded.

Last month, the brand protection firm MarkMonitor issued an independent report that identified the traffic to a sample of Internet sites that are notorious for selling counterfeit goods and distributing infringing content. The MarkMonitor report concluded that:

- 26 of the sites selling counterfeit prescription drugs (separate from the counterfeit physical goods analysis) generated 51 million visits per year.
- The combined traffic to 48 of the sites selling counterfeit physical goods is more than 87 million visits per year.
- 43 sites that were classified as sources of 'digital piracy' generated over 146 million visits per day, representing **more than 53 billion visits per year** – nearly 9 visits for every human being on earth.

But that was just the beginning. Just a few weeks later, a study released by Envisional found that **nearly one fourth of all online traffic worldwide is infringing IP**. In the course of this study,

Envisional closely examined numerous sites. Among them was a peer-to-peer site that was comprised of **98.8% copyrighted content**. And an analysis of the most popular content on the OpenBitTorrent tracker, found that **only one file in 10,000 was non-copyrighted**.

The harm from this appalling amount of IP infringement was made clear in the stark findings of a report by Frontier Economics just two weeks ago—counterfeiting and piracy have stolen **2.5 MILLION jobs** from the G20 economies. The report also found that:

- The global economic value of counterfeiting and piracy is **\$650 billion** a year.
- International trade in counterfeit and pirated products is **\$360 billion** a year.
- Counterfeiting and piracy robbed G20 governments of **\$125 billion** a year in lost tax revenue and other benefits.

At a time when America's need for jobs is so great and our Federal budget deficit is such a major concern, the case for improving IP protection and enforcement has never been clearer: Effectively combatting piracy and counterfeiting saves jobs and promotes legitimate commerce.

Enhanced Legal Tools are Needed to Cut Off Rogue Sites

The enforcement of IP online is complicated by many practical factors, but it is not impossible and it would be a grievous error not to try.

One of the great recent success stories has been the actions of U.S. Immigration and Customs Enforcement (ICE) under Director John Morton. Over the past ten months, and most recently on Monday, ICE, in cooperation with the Justice Department and the IPR Center, has seized the domain names of more than a hundred websites involved in counterfeiting and piracy. While some of these sites have resurfaced with different domain names, many of them have not. This represents a clear win for American consumers, job-seekers, innovators, and creators. The Chamber congratulates the Administration on these past and ongoing efforts and offers its sincere thanks to Director Morton and all the others who have contributed to Operation In Our Sites.

As we know, the Internet knows no national boundaries, but the jurisdictional limits of Federal enforcement agencies do. Thus, the effectiveness of seizing rogue site domain names is limited for addressing counterfeiting and piracy on wholly foreign websites. And many rogue sites are based outside the United States.

Ideally, all countries would improve their IP protection and enforcement systems with the result that the number and reach of rogue sites globally would diminish substantially. Until such time, the United States has a duty to protect its market and consumers from these sites.

Mr. Chairman, your introduction of S. 3804 and its unanimous approval by this Committee was a critical step forward. As we all know, that legislation would have authorized the Justice Department to bring suits in Federal court. Those courts could, upon sufficient proof that a site met the definition of "dedicated to infringement," issue orders to the strategic partners in the fight against online theft – Internet service providers, payment processors, and advertisers – to

stop linking and/or doing business with the site. The fundamental premise of that bill, cutting rogue sites off from the American market to protect consumers against fraud and harm and to stem the flow of American dollars to counterfeiters and pirates, is a creative approach to the foreign rogue site problem. As you know, the Chamber enthusiastically supported S. 3804.

Yesterday, we delivered to all Members of Congress a letter on behalf of over 80 businesses and professional and labor organizations, representing over **1.5 million jobs and workers**, and over 50 trade associations representing thousands of companies. The signatories to this letter represent a uniquely broad and deep coalition, featuring companies of all sizes and across many sectors of our economy, the entirety of which recognizes the threat and harm of rogue sites and the need for Congressional action. The letter is appended to this testimony.

Mr. Chairman, the Chamber looks forward to working with you, Senator Hatch, Chairman Smith and Ranking Member Conyers on the House Judiciary Committee to help craft the best possible legislation and to enact that legislation this year.

Thank you.

February 13, 2011

Dear Chairman Leahy and Members of the Senate Judiciary Committee,

I strongly support Bill 3804.

Piracy eats away not only at the income of writers, but at the fabric of intellectual property. This blatant disregard for copyright not only devalues us, the creators, but the work we labor to create.

In discussions with people who feel piracy is simply the cost of doing business, or worse, that it's their right as a consumer, I've been told I should be flattered so many people want to read my work--for free--that they probably wouldn't have bought the book anyway, so it's not really a lost sale, that there's nothing I can do about it, so why fight it. They tell me they can't afford to actually buy the book, but they want to read it. When I suggest the library as an alternative, I'm told the library's too far away or the wait for the book from a library too long.

I'm told not to call it stealing or those who engage in the practice thieves because it annoys them.

It annoys them.

I say respectfully it annoys me when what we, as writers, have created out of our individual minds, hearts, guts is taken without compensation. When it's taken without our consent. We do not consent to piracy. We do not consent to being devalued out of existence.

The internet is an extraordinary tool, and with it, we can access information with a few keystrokes. But there is a difference, wide and deep, between information and creative property. We use words to express our imaginations, to tell stories that entertain, that bring comfort, offer amusement or solace. Melding that imagination with words to create a book takes work, time, effort, talent. The storyteller and the book that comes from her through that work, that talent, must be valued and respected. If piracy continues to devastate a writer's income, to erode the ability of the publishers to make the profit necessary to bring those books to the public, where will the next generation of storytellers come from? How can they live if their individual creativity has no value?

The novelist, the novel, the publisher as the gate-keeper can't stand against the growing assault of piracy.

Freedom is essential to us, as people, as Americans. But freedom must co-exist with the rule of law. And the law must address progress along with the benefits and complications it brings with it.

We look to you to make the laws that protect us, that protect our work, that protect and respect creative property. We look to you to stand up for us and against piracy and its growing sense of entitlement.

Without writers there will be no stories. Without stories, the world will be a smaller and much less vibrant place. Please don't let that happen.

Nora Roberts

**STATEMENT OF MOTION PICTURE ASSOCIATION OF
AMERICA, INC.**

BEFORE THE SENATE JUDICIARY COMMITTEE

**DIRKSEN SENATE OFFICE BUILDING, ROOM 226
WASHINGTON, D.C.**

FEBRUARY 16, 2011, 10 A.M.

A. Background and Introduction

We want to thank the Committee for this opportunity to submit this Statement regarding rogue Internet sites on behalf of the MPAA and its member companies. The MPAA is the primary voice and advocate for the American motion picture, home video and television industries in the U.S. and around the world. MPAA's members are the leading producers and distributors of filmed entertainment: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLP; and Warner Bros. Entertainment Inc.

Motion picture and television production is a major private sector industry in all 50 states, directly employing over 296,000 people across the United States. These are high quality jobs—both in front of the camera and behind the scenes—with an average salary of nearly \$76,000, 72 percent higher than the average salary nationwide. Our on-location production activity also supports more than 115,000 small businesses across the country—over 90% of which employ fewer than 10 people—with film productions infusing on average \$225,000 per day into a local economy. Nationwide, the motion picture industry generates in excess of \$15 billion in public revenues, and we consistently boast a positive balance of trade in every country in which we do business.

**B. Rogue Websites Create Consumer Confusion and Damage the Motion
Picture and Television Industry**

While high-speed broadband networks bring immense opportunities for the exchange of information and ideas, the inappropriate use of the networks can facilitate the anonymous theft and rapid, ubiquitous illegal distribution of

copyrighted works. It is not an overstatement to say that, the rampant theft of IP strikes at the heart our nation's economy, our core values of reward for innovation and hard work, and our ability to compete globally. In short, Internet theft puts at risk one of America's great export industries.

The most pernicious forms of digital theft occur through the use of websites. The sites, whose content is hosted and whose operators are located throughout the world take many forms, but have in common the simple fact that all materially contribute to, facilitate and/or induce the distribution of copyrighted works, such as movies and television programming.

"Rogue" websites, as they are frequently called, typically engage in one or more of the following forms of online theft of copyrighted content:

- Streaming an unauthorized copy of a copyrighted video;
- Downloading an unauthorized copy of a copyrighted video;
- Streaming or downloading of an unauthorized copy of a copyrighted video by linking to a torrent or other metadata file that initiates piracy;
- Linking to a specific offer to sell an unauthorized copy of a copyrighted video;
- Hosting an unauthorized copy of a copyrighted video.

These rogue websites are increasingly sophisticated and take on many attributes of legitimate content delivery sites, creating additional enforcement challenges and feeding consumer confusion. Among the steps taken by rogue websites to deceive consumers into believing they are legitimate are:

- The use of credit card companies, such as Visa and MasterCard, to facilitate payments to rogue websites.
- The use of "e-wallet" or alternative payment methods such as PayPal, Moneybrokers, AlertPay and Gate2Shop to allow for the receipt of payment from the public for subscriptions, donations, purchases and memberships.
- The use of advertising, often for mainstream, Blue Chip companies, on the websites.
- Reward programs for frequent purchasers.

All of these elements combine to create a feeling of legitimacy that results in unknowing consumers purchasing illegal content and enriching the criminals profiting from these rogue sites.

The impact of this activity is documented in a recently published report by Envisional, an independent Internet consulting company. Envisional's "Technical Report: An Estimate of Infringing Use of the Internet" estimates that almost a quarter of global Internet traffic and over 17 percent of U.S. Internet traffic is copyright infringing. This is a staggering level of theft that cannot be sustained without significant damage to the motion picture industry and the workforce it supports.

C. Action by the Congress and the Administration Will Curtail the Negative Economic Impact of Online Theft

We have enjoyed a long history of working with the Committee and have been encouraged by the emphasis that the Administration has placed on intellectual property rights and enforcement. Since Victoria Espinel was confirmed by the Senate over 13 months ago we have seen increasing cooperation from our partners in the private sector intermediaries—whether pay processors, ad brokers, or ISPs. The combined efforts of the Department of Justice, ICE and the IPR Center have not only put rogue sites out of business but have raised awareness with the public, deterred bad actors, and resulted in many websites voluntarily ceasing criminal activity or going legal.

In fact, an MPAA evaluation of ICE's "Operation In Our Sites, v.1.0" demonstrated the positive effects of the Administration's involvement. Of the top 304 infringing websites that were monitored during the 2010 calendar year, including both sites that compile links to stolen content and sites that allow unauthorized streaming, nine were seized during both phases of "Operation in Our Sites". An additional 81 websites, over one quarter of the landscape (26%) voluntarily stopped offering illegal content or completely shut down, and of the 81 sites, 12 transitioned to legal movies or TV, or became promotional websites that do not offer illegal content. This is a significant development.

Last week the IPEC released its first annual report to Congress pursuant to the PRO-IP Act and the report reiterated not only the detrimental impact of copyright infringement on the economy but also the need to work with the Congress to

update intellectual property law to improve law enforcement effectiveness. To quote:

“The digital environment is at its core an economy of intellectual property. Digitalization of goods, services, data, ideas and conversations creates intrinsically new assets, often built on or derived from assets for which there are existing protections. The application of intellectual property rules to the digital environment are therefore essential to enabling creators to be rewarded for their work. Lack of intellectual property enforcement in the digital environment, by contrast, threatens to destabilize rule-of-law norms, with severe effects on jobs and economic growth. Undermining respect for rule-of-law values impacts a range of other policy goals affected by the Internet (e.g., privacy). In short, criminal laws and intellectual property laws that apply in the physical world are based on a tradition of rules, checks and balances that must be applied to and tailored to the digital world.”

We believe that rogue sites legislation, combined with the Administration’s work with intermediaries and enforcement by the IPR Center, will go a long way towards shutting down the unauthorized distribution of copyrighted works and close a gap in the intellectual property law.

Again, we thank Chairman Leahy on behalf of our member companies for the opportunity to provide this Statement. We look forward to working with you, Ranking Member Grassley, Senator Hatch and other members of the Committee on crafting legislation to deal with this criminal activity.



A UNIT OF FOX FILMED ENTERTAINMENT

BLUE SKY STUDIOS, INC.
ONE AMERICAN LANE
GREENWICH, CT 06831
PHONE: 203-992-6313
FAX: 203-992-6002
www.blueskystudios.com

BRIAN A. KEANE
CHIEF OPERATING OFFICER, EVP

The Honorable Richard Blumenthal
United States Senate
Washington, DC 20510

February 15, 2011

Dear Senator Blumenthal:

Last year, Senator Leahy and Senator Hatch along with 18 cosponsors introduced bipartisan legislation that would combat online copyright infringement and the sale of counterfeit goods, S.3804, the "Combating Online Infringement and Counterfeits Act." Knowing that you have been a leader on protecting consumers from online harms, I hope that you will be an original co-sponsor of Senator Leahy's legislation when it is reintroduced this year.

Blue Sky Studios is located in Greenwich, CT and currently employs 400, mostly high skilled animators and engineers. The financial success of our movies like Ice Age, Horton Hears a Who, and our soon to be released movie Rio, is threatened when Rogue sites – many of which are hosted outside the U.S. and not reachable by current U.S. law – entice people to illegally download or stream our movies. These Rogue sites have become increasingly sophisticated in both design and operation, and often deceive consumers into believing they are legitimate. In addition to undermining the growth and stability of companies like Blue Sky and threatening American jobs, many of these sites represent a severe safety risk to consumers who unwittingly purchase dangerous and illegal products. We believe that the legal tools the Rogue site legislation would provide to the Department of Justice are essential to helping address these illegal websites and ensuring that the Internet is a safe and vibrant marketplace.

Senator Leahy's bill was carefully crafted to adhere to constitutional requirements that protect free speech and provide appropriate due process for all affected parties. We therefore urge you to become an original co-sponsor of this legislation when it is introduced and we look forward to working with you in support of its enactment.

Sincerely,

Brian Keane
Blue Sky Studios