

Online Copyright Infringement and Counterfeiting: Legislation in the 112th Congress

Brian T. Yeh
Legislative Attorney

January 20, 2012

Congressional Research Service
7-5700
www.crs.gov
R42112

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

The global nature of the Internet offers expanded commercial opportunities for intellectual property (IP) rights holders but also increases the potential for copyright and trademark infringement. Piracy of the content created by movie, music, and software companies and sales of counterfeit pharmaceutical drugs and consumer products negatively impact the American economy and can pose risks to the health and safety of U.S. citizens. Although rights holders and law enforcement agencies currently have some legal tools to pursue domestic infringers, they face difficult challenges in enforcing IP laws against actors located abroad. Many websites trafficking in pirated copyrighted content or counterfeit goods are registered and operate in foreign countries. These foreign "rogue sites" sell subject matter that infringes U.S. copyrights and trademarks to U.S. consumers, yet the website operators remain beyond the reach of U.S. courts and authorities.

Some believe that legislation is necessary to address the jurisdictional problem of holding foreign websites accountable for piracy and counterfeiting. On May 12, 2011, Senator Leahy introduced S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act), that would allow the Attorney General to seek an injunction from a federal court against a domain name used by a foreign website that engages in, enables, or facilitates infringement; such court order may then be served on U.S.-based domain name servers, Internet advertisers, search engines, and financial transaction providers, which would be required to take actions such as preventing access to the website or suspending business services to the site. IP rights holders may also sue to obtain a cease and desist order against the operator of an Internet site dedicated to infringement (whether domestic or foreign) or the domain name itself.

On October 26, 2011, Representative Lamar Smith introduced H.R. 3261, the Stop Online Piracy Act (SOPA). SOPA is similar to the PROTECT IP Act yet is broader in scope by including several provisions not found in S. 968, such as those that increase the criminal penalties for online streaming of copyrighted content, create criminal penalties for trafficking in counterfeit drugs, and require the appointment of dedicated IP personnel in U.S. embassies.

There has been considerable public debate about the PROTECT IP Act and SOPA. Critics claim these measures amount to "Internet censorship" and that they would impair free speech. There are also concerns that the legislation will disrupt the technical integrity of the Internet. Supporters of the bills argue that in order to reduce digital piracy and online counterfeiting, new enforcement mechanisms are vital for U.S. economic growth and needed to protect public health and safety. After intense lobbying against the legislation, Senator Reid on January 20, 2012, postponed a cloture vote that had been scheduled for the PROTECT IP Act, and Representative Smith announced that the House Judiciary Committee would similarly postpone consideration of SOPA, until a compromise could be reached between supporters and opponents of the legislation.

An alternative to these bills is the Online Protection and Enforcement of Digital Trade Act (OPEN Act; S. 2029, H.R. 3782) that would authorize the International Trade Commission (ITC) to investigate foreign websites that allegedly engage in willful IP infringement. The ITC may issue a cease and desist order against the infringing foreign website; such an order may be used by the rights holder to oblige financial transaction providers or Internet advertising services to stop doing business with the website. Unlike the PROTECT IP Act and SOPA, the OPEN Act does not apply to domestic websites and also would not require search engines or domain name servers to block access or disable links to foreign websites.

Contents

Introduction 1
Brief Overview of Federal Laws That Apply to Particular Unlawful Online Activity 2
Digital Millennium Copyright Act (DMCA) 2
Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) 4
Anticybersquatting Consumer Protection Act (ACPA) 5
Unlawful Internet Gambling Enforcement Act (UIGEA) 6
Ryan Haight Online Pharmacy Consumer Protection Act 7
Legislative History of Online Copyright Infringement and Counterfeiting Legislation 7
Summary of PROTECT IP Act Provisions 9
Action by the Attorney General 9
Action by a "Qualifying Plaintiff" 10
Due Process, Safeguards, and Limitations on Liability 11
Reports to Congress 12
Summary of SOPA Provisions 12
Title I of SOPA, "Combating Online Piracy" 13
Action by the Attorney General 13
Actions by a "Qualifying Plaintiff" 15
Due Process, Safeguards, and Limitations on Liability 17
Reports to Congress 18
Title II of SOPA, "Additional Enhancements to Combat Intellectual Property Theft" 19
Streaming of Copyrighted Works in Violation of Criminal Law 19
Trafficking in Inherently Dangerous Goods or Services 19
Protecting U.S. Businesses From Foreign and Economic Espionage 19
Amendments to Sentencing Guidelines 20
Defending Intellectual Property Rights Abroad 20
Debate Over the Legislation 20
Impact on Free Speech 20
Technical Integrity of the Internet 22
Private Cause of Action 23
Conflict with the DMCA "Safe Harbors" and Potential Impact on Internet Innovation (Referring to SOPA Only) 24
Manager's Amendment to H.R. 3261 (SOPA) 26
Summary of the OPEN Act 27
International Trade Commission Enforcement 28
Applicable Scope of New Section 337A, as added by the OPEN Act 28
Violation 28
Complaint 29
ITC Determination 29
Remedies 30
Section 337 Judges 31
OPEN Act Compared to PROTECT IP Act and SOPA 31

Contacts

Author Contact Information 31
Acknowledgments 31

Introduction

The Internet has become a central part of the American economy, delivering innovative products while eliminating the need for inefficient middlemen. However, the free flow of information facilitated by the Internet has also created problems with copyright and trademark infringement. The problem is significant; as much as 6% of the U.S. gross national product is generated by industries supported by intellectual property laws.[1] A recent report contends that nearly 24% of all Internet traffic worldwide is infringing.[2] Piracy of the content created by movie, music, and software companies, and the sale of counterfeit goods that include inauthentic clothing, pharmaceutical drugs, and consumer electronics, negatively impacts the American economy.[3] Although the Government Accountability Office cautions that it is difficult to precisely quantify the economy-wide impacts of piracy, it is believed to be a serious problem.[4]

However, many websites trafficking in copyrighted content or counterfeit goods are registered and operate entirely in foreign countries. These foreign "rogue sites" often provide creative content and physical goods protected by U.S. intellectual property law to people located within the United States. S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act), and H.R. 3261, the Stop Online Piracy Act (SOPA), are legislative responses to the jurisdictional problem of holding foreign websites accountable for piracy and counterfeiting. The bills also authorize new enforcement mechanisms against domestic sites that facilitate infringing activities. These bills would create new obligations for U.S.-based domain name servers, Internet advertisers, search engines, and financial transaction providers to address such harm to intellectual property rights holders. There has been considerable public debate about the changes to existing law that are proposed by these two bills. An alternative legislative measure, the Online Protection and Enforcement of Digital Trade Act (OPEN Act; S. 2029, H.R. 3782) has been introduced in response to the concerns raised about the PROTECT IP Act and SOPA.

[1] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Frederick Huntsberry, Chief Operating Officer Paramount Pictures Corp.).

[2] *See Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (written statement of Sen. Patrick Leahy, Chairman S. Comm. on the Judiciary, *citing* a report commissioned by NBC Universal, available at http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf).

[3] As used in this report, the term "piracy" refers to the unlawful reproduction and distribution of copyrighted content, and "counterfeiting" refers to the manufacture and distribution of products that bear (without authorization) a trademark that is identical to a trademark validly registered for those goods, or that cannot be distinguished in its essential aspects from such a trademark, and that, thereby, infringes the rights of the owner of the trademark in question. These definitions are adapted from those used in the World Trade Organization (WTO)'s Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), Section 4, Article 51, footnote 14, available at http://www.wto.org/english/tratop_e/trips_e/t_agm4_e.htm#Footnote14.

[4] U.S. Government Accountability Office, *Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, 10-423, April 2010, p. 2, available at http://www.gao.gov/new.items/d10423.pdf.

Brief Overview of Federal Laws That Apply to Particular Unlawful Online Activity

Digital Millennium Copyright Act (DMCA)

Congress passed the Digital Millennium Copyright Act (DMCA) in 1998 in an effort to adapt copyright law to an evolving digital environment.[5] Title II of the DMCA added a new Section 512 to the Copyright Act (Title 17 of the U.S. Code) in order to limit the liability of service providers against claims of copyright infringement relating to online materials. This "safe harbor" immunity is available only to parties that qualify as a "service provider" as defined by the DMCA, and only after the provider complies with certain eligibility requirements. In exchange for immunity from liability, the DMCA requires service providers to cooperate with copyright owners to address infringing activities conducted by the providers' customers. The DMCA's safe harbors greatly limit service providers' liability based on the specific functions they perform.[6] The safe harbors correspond to four functional operations of a service provider that might otherwise constitute copyright infringement: (1) transitory digital network communications, (2) system caching, (3) storage of information on systems or networks at direction of users, and (4) information location tools.[7]

One safe-harbor-qualifying condition common to three of the four categories is the requirement that upon proper notification by the copyright owner of online material being displayed or transmitted without authorization, a service provider must "expeditiously" remove or disable access to the allegedly infringing material.[8] This "notice and takedown" obligation does not apply when the service provider functions as a passive conduit of information under 17 U.S.C. Section 512(a) (offering transitory digital network communications), but is a condition that must be met to obtain shelter under the remaining three safe harbor provisions. As indicated by the eligibility conditions in each subsection of Section 512(b)-(d), the notice and takedown procedure varies slightly for each. To prevent abuse of the notice and take-down procedure, Section 512(f) provides damages, costs, and attorneys' fees to any service provider that is injured by a knowing, material misrepresentation that an item or activity is infringing.[9] For example, any person who sends a "cease and desist" letter to a service provider, with the knowledge that the claims of copyright infringement are false, may be liable to the accused infringer for damages.

---

[5] For more information regarding the DMCA, *see* CRS Report RL32037, *Safe Harbor for Service Providers Under the Digital Millennium Copyright Act*, by Brian T. Yeh and Robin Jeweler, and CRS Report RL33887, *The Digital Millennium Copyright Act: Exemptions to the Prohibition on Circumvention*, by Brian T. Yeh.

[6] Ellison v. Robertson, 189 F. Supp. 2d 1051, 1064 (C.D. Cal. 2002), *aff'd in part and rev'd in part,* 357 F.3d 1072 (9th Cir. 2004). Service providers who qualify for safe harbor are protected from all monetary and most equitable relief that may arise from copyright liability. In such a situation, "even if a plaintiff can show that a safe harbor-eligible service provider has violated her copyright, the plaintiff will only be entitled to the limited injunctive relief set forth in 17 U.S.C. §512(j)." Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1098-99 (W.D. Wash. 2004) (citations omitted).

[7] 17 U.S.C. §512(a)-(d).

[8] *See* 17 U.S.C. §512(b)(E), (c)(C), and (d)(3).

[9] "'Knowingly' means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations. "'Material' means that the misrepresentation affected the ISP's response to a DMCA letter." Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2004) (citations omitted).

As noted earlier, the DMCA's safe harbor provisions do not confer absolute immunity from legal liability for copyright infringement. Although they ensure that qualifying service providers are not liable for monetary relief, they may be liable for limited injunctive relief. For example, a service provider that provides "transitory digital network communications" may be subject to the following injunctive relief:

- an order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order;
- an order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.[10]

In the case of service providers that provide either (1) system caching, (2) storage of information on systems or networks at direction of users, or (3) information location tools, the court may grant injunctive relief with respect to a service provider in one or more of the following forms:

- an order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network;
- an order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order;
- such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.[11]

One public interest group has praised the importance of the DMCA's safe harbor provisions to the development of the Internet:

> Without these protections, the risk of potential copyright liability would prevent many online intermediaries from providing services such as hosting and transmitting user-generated content. Thus the safe harbors have been essential to the growth of the Internet as an engine for innovation and free expression.[12]

Some have called for Congress to pass legislation that would expand the DMCA to include notice and takedown provisions regarding trademark infringement and other illegal conduct such as spam, phishing, and fraud.[13]

---

[10] 17 U.S.C. §512(j)(1)(B).

[11] 17 U.S.C. §512(j)(1)(A).

[12] Electronic Frontier Foundation, *Digital Millennium Copyright Act*, *at* http://www.eff.org/issues/dmca.

[13] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearings Before the House Subcomm. on Intellectual Property, Competition, and the Internet,* 112h Cong., 1st sess. (2011) (statement of Christine N. Jones, General Counsel, The Go Daddy Group, Inc.), at 8.

Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act)

The Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) strengthened existing forfeiture provisions for use in cases involving criminal copyright infringement and trademark counterfeiting.[14] The PRO-IP Act allows civil forfeiture of "[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of [criminal copyright infringement or trafficking in counterfeit goods]."[15] The Department of Justice and U.S. Immigration and Customs Enforcement (ICE) have recently begun to use this civil forfeiture authority in an innovative way—to seize and forfeit domain names of websites that are being used for criminal activity, in this case websites that are involved in selling counterfeit goods and distributing pirated merchandise and copyrighted digital materials.[16] Domain name registrars redirect traffic from the seized domains to a government website explaining that the domain name has been seized by ICE. However, the sites remain online and accessible through their Internet protocol addresses.[17]

Between June 30, 2010, and November 28, 2011, ICE seized 350 domain names[18] associated with Internet piracy in its initiative called "Operation In Our Sites."[19] Of these 350 seized domain names, 116 have been forfeited to the U.S. government.[20] In order to obtain domain name seizure warrants, ICE agents present evidence of criminal trademark violations or criminal copyright infringement that is occurring on the website to a federal magistrate judge. In order to issue the warrant, the judge must determine, by a standard of probable cause, that the domain name is being used in violation of federal criminal laws.[21] Due process protections are part of this process, as described by the ICE Director:

> As with all judicially authorized seizure warrants, the owners of the seized property have the opportunity to challenge the judge's determination through a petition. If a petition is filed, a hearing is held in a federal court to determine the validity of the affidavit supporting the seizure, at which point the government would have the burden of proof.… Under existing

[14] P.L. 110-403, 122 Stat. 4256.

[15] 18 U.S.C. §2323.

[16] For more information about this initiative, *see* Ben Sisario, U.S. Shuts Down Web Sites in Piracy Crackdown, N.Y. TIMES, November 27, 2010, at B2; *see also* U.S. Dep't of Justice, *Press Release: Federal Courts Order Seizure of 82 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ and ICE Cyber Monday Crackdown*, November 29, 2010, *available at* http://www.justice.gov/opa/pr/2010/November/10-ag-1355.html.

[17] An Internet protocol address is a series of numbers assigned to a device attached to a network. These numbers are used to indicate where the device is located on the network. For example, when a user visits http://www.google.com the user's computer is communicating with 74.125.93.147, the Internet protocol address of google.com's webserver.

[18] A domain name can be typed into a web browser to access an Internet address; it usually consists of a "top level domain" and a "second level domain"—for example, in the domain name "amazon.com," ".com" is a top level domain, and "amazon" is the second level domain. A domain name registry operates top level domains, and a domain name registrar manages the registration of domain names. See S.Rept. 111-373 at 6.

[19] U.S. Dep't of Justice, U.S. Immigration and Customs Enforcement (ICE), *Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE HIS and FBI Cyber Monday Crackdown,* November 28, 2011, *at* http://www.justice.gov/opa/pr/2011/November/11-ag-1540.html.

[20] *Id.*

[21] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearings Before the House Subcomm. on Intellectual Property, Competition, and the Internet,* 112th Cong., 1st sess. (2011) (statement of John Morton, Director, ICE), at 11.

> federal law, the website owner may also choose to demand return of the property through the law enforcement agency itself, by writing a letter to ICE.… Further, if the website owner determines he or she does not wish to pursue either of these avenues of due process, a challenge may be filed directly with the law enforcement agency conducting a forfeiture action under administrative processes.[22]

The assistant deputy director of ICE has explained that several factors are taken into account before the agency decides which domain name should be seized, including

- the popularity of the website, which often correlates with its profitability;
- whether the website is commercial in nature and earns a substantial amount of money—those that run advertisements, sell subscriptions, or sell merchandise; and
- whether seizing a site will have a substantial impact on piracy.[23]

However, the global nature of the Internet presents problems to the civil forfeiture approach used by ICE. Only domain names registered within the United States and subject to ICE's jurisdiction may be seized.

Anticybersquatting Consumer Protection Act (ACPA)

The Anticybersquatting Consumer Protection Act (ACPA)[24] includes two provisions that provide individuals with remedies against abuses of the domain name system. First, it provides a means to protect against trademark dilution through the domain name system. Second, it provides anticybersquatting protections for individuals.[25]

ACPA allows trademark owners to file a lawsuit against domain name registrants and their licensees for trademark dilution.[26] Such suits are permissible if the domain name is identical or confusingly similar to a mark that was distinctive or famous at the time the domain name was registered, or infringes upon names or insignias of the American Red Cross or United States Olympic Committee.[27] If the registrant is found to have registered the domain name in bad faith, ACPA authorizes a court to order that the domain name be forfeited, canceled, or transferred to the trademark owner.[28]

---

[22] *Id.* at 12.

[23] BNA's Electronic Commerce & Law Report, *U.S. Nexus, Website's Profit Factor Into ICE Calculus of Which Domains to Seize,* June 8, 2011 (interview between BNA's Tamlin Bason and Erik Barnett, assistant deputy director of ICE).

[24] P.L. 106-113, app. I, tit. III.

[25] Cybersquatting is defined under ACPA as registering a domain name that "consists of the name of another living person [such as a celebrity], or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name." 15 U.S.C. §8131.

[26] 15 U.S.C. §1125(d)(1)(A). For more information about trademark dilution generally, *see* CRS Report RL33393, *Protecting Famous, Distinctive Marks: The Trademark Dilution Revision Act of 2006*, by Brian T. Yeh.

[27] 15 U.S.C. §1125(d)(1)(A)(ii).

[28] 15 U.S.C. §1125(d)(1)(C).

ACPA also authorizes in rem actions directly against a domain name that infringes upon a trademark, where personal jurisdiction cannot be obtained over the owner of the infringing domain name or if the owner cannot be identified by the trademark owner.[29]

ACPA also allows individuals to sue cybersquatters, defined as one who intends to profit by registering and subsequently selling a domain name that is comprised of or confusingly similar to the first individual's name without consent.[30] The court may award injunctive relief to the plaintiff, "including the forfeiture or cancellation of the domain name or the transfer of the domain name to the plaintiff."[31]

Unlawful Internet Gambling Enforcement Act (UIGEA)

The Unlawful Internet Gambling Enforcement Act (UIGEA), which Congress passed in 2006 as Title VIII of the SAFE Port Act,[32] seeks to cut off the flow of revenue to unlawful Internet gambling businesses.[33] UIGEA prohibits gambling-related businesses from accepting checks, credit card charges, electronic transfers, and similar payments in connection with unlawful Internet gambling.[34] Anyone who violates this prohibition of UIGEA is subject to a criminal fine of up to $250,000 (or $500,000 if the defendant is an organization), imprisonment of up to five years, or both.[35] In addition, upon conviction of the defendant, the court may enter a permanent injunction enjoining the defendant from making bets or wagers "or sending, receiving, or inviting information assisting in the placing of bets or wagers."[36] The Attorney General of the United States or a state attorney general may bring civil proceedings to enjoin a transaction that is prohibited under UIGEA.[37]

UIGEA directed the Board of Governors of the Federal Reserve System and the Treasury Department to promulgate regulations that require "each designated payment system, and all participants therein, to identify and block or otherwise prevent or prohibit restricted transactions through the establishment of policies and procedures" reasonably calculated to have that result.[38] The final rule adopted by the Federal Reserve and the Treasury Department identifies five relevant payment systems that could be used in connection with, or to facilitate, the "restricted transactions" used for Internet gambling: Automated Clearing House System (ACH), card systems, check collection systems, money transmitting business, and wire transfer systems.[39] The rule defines a "restricted transaction" to mean any transactions or transmittals involving any credit, funds, instrument, or proceeds that the UIGEA prohibits any person engaged in the business of betting or wagering from knowingly accepting, in connection with the participation of

[29] 15 U.S.C. §1125(d)(2)(A).

[30] 15 U.S.C. §8131(1)(A).

[31] 15 U.S.C. §8131(2).

[32] P.L. 109-347, 120 Stat. 1952 (31 U.S.C. §§5361-5367) (2006).

[33] For a more detailed analysis and description of UIGEA, *see* CRS Report RS22749, *Unlawful Internet Gambling Enforcement Act (UIGEA) and Its Implementing Regulations*, by Brian T. Yeh and Charles Doyle.

[34] 31 U.S.C. §5363.

[35] 31 U.S.C. §5366(a).

[36] 31 U.S.C. §5366(b).

[37] 31 U.S.C. §5365.

[38] 31 U.S.C. §5364(a).

[39] 31 C.F.R. §132.3.

another person in unlawful Internet gambling.[40] The rule directs participants in the designated systems, unless exempted, to "establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions,"[41] and then provides non-exclusive examples of reasonably compliant policies and procedures for each system.[42]

Some Members of Congress have criticized UIGEA for being, in their view, ineffective at stopping Internet gambling by millions of Americans.[43]

Ryan Haight Online Pharmacy Consumer Protection Act

"Rogue" Internet pharmacies engage in practices that are illegal, such as selling unapproved or counterfeit drugs or dispensing drugs without a prescription. In response to the problem of rogue Internet pharmacies and the illegal sale of prescription controlled substances over the Internet, the 110th Congress passed the Ryan Haight Online Pharmacy Consumer Protection Act of 2008[44] (hereinafter called "Ryan Haight Act"), which amends the federal Controlled Substances Act to expressly regulate online pharmacies that dispense controlled substances by mandating that the pharmacy post specific information on its website, and that the pharmacy register with and submit certain reports to the Drug Enforcement Administration. The Ryan Haight Act requires that delivery, distribution, or dispensing of controlled substances over the Internet must be pursuant to a "valid prescription" (defined by the statute as a prescription that is issued for a legitimate medical purpose in the usual course of professional practice, by a practitioner who has conducted at least one medical evaluation of the patient in the physical presence of the practitioner). The Ryan Haight Act also clarifies and enhances the penalties for illegal distributions of controlled substances over the Internet. According to the White House 2010 National Drug Control Policy, the Ryan Haight Act has "already had a significant impact on reducing the number of illegal Internet pharmacies."[45]

Legislative History of Online Copyright Infringement and Counterfeiting Legislation

On September 20, 2010, Senator Leahy with Senator Hatch introduced the Combating Online Infringement and Counterfeits Act (COICA). The Senate Judiciary Committee voted to report COICA favorably to the Senate, with an amendment in the nature of a substitute. However, no

[40] 31 C.F.R. §132.2(y).

[41] 31 C.F.R. §132.5(a).

[42] 31 C.F.R. §132.6.

[43] *Tax Proposals Related to Legislation to Legalize Internet Gambling: Hearing Before the House Comm. on Ways and Means,* 111th Cong., 2nd sess. (2010) (statement of Rep. McDermott) ("[E]very day millions of Americans gamble on the Internet. Prohibition hasn't prevented the millions of Americans who want to gamble online from doing it. It has forced internet gambling operators to work offshore, it has put consumers at risk, and it sends billions in dollars of revenue to other nations.").

[44] P.L. 110-425.

[45] White House Office of National Drug Control Policy, *2010 National Drug Control Strategy*, at 33.

public hearing was held to consider COICA before the end of the 111th Congress, and the full Senate did not act on the legislation before the end of the congressional term.

At the request of Senator Coburn, the Senate Judiciary Committee in the 112th Congress held a hearing February 16, 2011, on the topic of "Targeting Websites Dedicated To Stealing American Intellectual Property." This hearing considered the scope of intellectual property theft over the Internet and the problem of "rogue websites" that exclusively traffic in infringing material, issues that COICA was designed to address.[46]

On May 12, 2011, Senator Leahy introduced S. 968, the PROTECT IP Act. On May 26, 2011, the Senate Committee on the Judiciary voted to report the legislation to the full Senate, with an amendment in the nature of a substitute.[47] Senator Wyden then placed a hold on the bill, indicating his intent to object to any unanimous consent request to proceed,[48] a sentiment that has been since joined by Senators Moran, Cantwell, and Paul.[49] The Senate Judiciary Committee held a hearing on June 22, 2011, entitled "Oversight of Intellectual Property Law Enforcement Efforts" that included testimony from ICE and other agencies charged with enforcement of intellectual property laws online. On July 22, 2011, Senator Leahy filed a written report.[50] On December 17, 2011, Senator Reid presented a cloture motion on a motion to proceed to S. 968, the PROTECT IP Act, with a roll call vote scheduled to be held on January 24, 2012. Senator Wyden expressed his intent to filibuster the bill.[51]

On October 26, 2011, Representative Lamar Smith, chairman of the House Judiciary Committee, introduced H.R. 3261, the Stop Online Piracy Act (SOPA). The House Judiciary Committee held a hearing on SOPA on November 2, 2011. On December 12, 2011, Representative Smith released a manager's amendment in the nature of a substitute to H.R. 3261. On December 15 and 16, the House Judiciary Committee held markup sessions in which the committee considered 60 amendments that were filed to the manager's amendment. However, the committee did not complete the markup and postponed continuation of the SOPA markup "due to House schedule."[52]

On January 14, 2012, the White House responded to an online petition submitted under the Obama Administration's "We the People" initiative that urged the President to veto the SOPA bill. In an online post written by the Intellectual Property Enforcement Coordinator Victoria Espinel, the U.S. Chief Technology Officer Aneesh Chopra, and Cybersecurity Coordinator Howard Schmidt, the White House explained that it would support online piracy legislation that "provides prosecutors and rights holders new legal tools to combat online piracy originating beyond U.S. borders." However, the White House stated that it "will not support legislation that reduces

[46] Nathan Pollard and Amy E. Bivins, *Leahy Vows to Offer Tough Anti-Piracy Bill; Senator Demands 'Accountability' From ISPs*, 16 Electronic Commerce & Law Report 257 (February 23, 2011).

[47] Sen. Leahy, Report of the Sen. Judiciary Committee, *Congressional Record*, May 26, 2011, p. S3426.

[48] Sen. Wyden, Intent to Object, *Congressional Record*, May 26, 2011, p. S3419.

[49] Letter from Senators Wyden, Cantwell, Moran, and Paul, to Senators Reid and McConnell, November 17, 2011.

[50] S.Rept. 112-39.

[51] Sen. Wyden, Congressional Record, December 17, 2011, p. S8783.

[52] U.S. House of Representatives, Committee on the Judiciary, Full Committee Markup of: H.R. 3261, the "Stop Online Piracy Act," *at* http://judiciary.house.gov/hearings/mark_12152011.html.

freedom of expression, increases cybersecurity risk, or undermines the dynamic, innovative global Internet."[53]

Several websites, including Wikipedia, Reddit, and Mozilla, participated in a 24-hour shutdown of their webpages on January 18 in order to express their opposition to the PROTECT IP Act and SOPA. The online protests, increased public awareness and negative opinions concerning the bills, and largely unfavorable media coverage, contributed to several Members of Congress withdrawing their support for the legislation in its current form.[54] On January 20, 2012, Senator Reid announced that, "in light of recent events," he was postponing the cloture vote that had been scheduled for the PROTECT IP Act on January 24, although he expressed his hope that a compromise could be reached between supporters and opponents of the legislation "in the coming weeks."[55] Moments after Senator Reid's announcement, Chairman Smith released a statement that the House Judiciary Committee would similarly postpone consideration of SOPA "until there is wider agreement on a solution" to the online piracy problem.[56]

Summary of PROTECT IP Act Provisions

The following is a brief summary of the key provisions of S. 968, as reported in the Senate.

Action by the Attorney General

S. 968 focuses on Internet sites that are "dedicated to infringing activities." An "Internet site dedicated to infringing activities," as defined by the bill, is an Internet site that has no significant use other than engaging in, enabling, or facilitating (1) copyright infringement; (2) circumvention of copyright protection systems; or (3) the sale, distribution, or promotion of goods, services, or materials bearing a counterfeit mark. The term also encompasses websites that facts or circumstances suggest are used primarily as a means for engaging in or enabling those activities.[57] The PROTECT IP Act also defines "nondomestic domain name" as a domain name for which the domain name registry is not located in the United States.[58]

The PROTECT IP Act would authorize the Attorney General to file a civil action against a person who registers a nondomestic domain name used by an Internet site dedicated to infringing activities, or against a person who owns or operates such an Internet site.[59] This provision is unlikely to be invoked often because these individuals are rarely located in the United States and are therefore difficult to prosecute domestically.

---

[53] Victoria Espinel et al., *Combating Online Piracy While Protecting an Open and Innovative Internet, at* https://wwws.whitehouse.gov/petition-tool/response/combating-online-piracy-while-protecting-open-and-innovative-internet.

[54] *See* Jonathan Weisman, *Web Rises Up to Deflect Bills Seen As Threat,* NEW YORK TIMES, January 19, 2012, at A1.

[55] Reid Statement On Intellectual Property Bill, January 20, 2012, *at* http://democrats.senate.gov/2012/01/20/reid-statement-on-intellectual-property-bill/.

[56] Statement from Chairman Smith on Senate Delay of Vote on PROTECT IP Act, January 20, 2012, *at* http://judiciary.house.gov/news/01202012.html.

[57] S. 968 as reported, §2(7).

[58] S. 968 as reported, §2(9).

[59] S. 968 as reported, §3(a)(1).

If through due diligence the Attorney General cannot find such a person, the Attorney General may commence an in rem action against a nondomestic domain name used by an Internet site dedicated to infringing activities. In such an action, a federal court may issue a temporary restraining order, a preliminary injunction, or an injunction against the domain name if the domain name is used within the United States to access the Internet site and the Internet site harms U.S. intellectual property rights holders. A federal law enforcement officer (with prior court approval) may serve a copy of such court order (to cease and desist from undertaking any further activity as an Internet site dedicated to infringing activities) to the following entities that would be required to take the specified actions:

- **Operators of non-authoritative domain name servers:** Non-authoritative domain name servers are intermediary servers used to resolve a domain name to its Internet protocol address. They do this by retaining a copy of information stored on an authoritative domain name server. Operators of these servers, generally Internet service providers, are directed to prevent access to seized domain names through the least burdensome technically feasible means.[60]
- **Financial transaction providers:** Companies that facilitate online transactions, such as credit card companies, are required to prevent their service from completing transactions between customers located within the United States and the Internet site.[61]
- **Internet advertising services:** Internet advertising services are required to stop selling advertising to and providing advertising for the Internet site.[62]
- **Information location tools:** Search engines such as Google and Yahoo must take technically feasible measures to remove or disable access to the Internet site.[63]

The PROTECT IP Act authorizes the Attorney General to bring an action for injunctive relief against any of the third parties that receive this court order and knowingly and willfully fail to comply with the obligations described above. A defendant in such an action may establish an affirmative defense by showing that it does not have the technical means to comply without incurring an unreasonable economic burden.[64]

Action by a "Qualifying Plaintiff"

A qualifying plaintiff[65] may bring suit for civil injunctive relief against a person who registered a domain name used by an Internet site dedicated to infringing activities, or the owner/operator of such an Internet site. Because this provision does not use the term "nondomestic" to limit the term "domain name," this action by a qualifying plaintiff is available against the owner/operator of any Internet site dedicated to infringement (whether domestic or foreign) or the registrant of

[60] S. 968 as reported, §3(d)(2).

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] S. 968 as reported, §3(e).

[65] A qualifying plaintiff is defined by the bill as (1) the U.S. Attorney General or (2) "an owner of an intellectual property right ... harmed by the activities of an Internet site dedicated to infringing activities occurring on that Internet site." *See* S. 968 as reported, §2(11)(B).

such domain name.[66] This provision gives a new "private right of action" to intellectual property rights holders who are harmed by the activities occurring on the domestic or foreign Internet site dedicated to infringing activities.

If through due diligence a qualifying plaintiff is unable to find such a person (or no such person has an address within the United States), the qualifying plaintiff may bring suit against a domain name used by an Internet site dedicated to infringing activities. In response, a federal court may issue a temporary restraining order, a preliminary injunction, or an injunction, against the domain name if the domain name is used within the United States to access the Internet site and the site harms U.S. intellectual property rights holders. Should the court grant the injunctive relief, the qualifying plaintiff (with prior court approval) may serve a copy of the court's cease and desist order to the following entities, which would then be responsible for taking the specified actions:

- **Financial transaction providers:** Companies that facilitate online transactions, such as credit card companies, are required to prevent their service from completing transactions between customers located within the United States and the Internet site.[67]
- **Internet advertising services:** Internet advertising services are required to stop selling advertising to and providing advertising for the Internet site.[68]

The PROTECT IP Act authorizes a qualifying plaintiff to bring an action for injunctive relief against any party receiving this court order that knowingly and willfully fails to comply with such order. A defendant in such an action may establish an affirmative defense by showing that it does not have the technical means to comply without incurring an unreasonable economic burden.[69]

Due Process, Safeguards, and Limitations on Liability

The PROTECT IP Act specifies that Rule 65 of the Federal Rules of Civil Procedure (FRCP) will govern how a federal court may issue injunctive relief in either an action brought by the Attorney General against a nondomestic entity, or an action brought by a qualifying plaintiff against domestic or nondomestic parties.[70] Rule 65 of the FRCP provides that a "court may issue a preliminary injunction only on notice to the adverse party," and that a "court may issue a temporary restraining order without written or oral notice to the adverse party or its attorney only if (1) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and (2) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required." Thus, Rule 65 requires that, prior to the issuance of a preliminary injunction, the party that is the target of the injunction is entitled to notice and an opportunity to be heard. However, an ex parte temporary restraining order (with no notice to the adverse party) may be granted if the party seeking the order satisfies the stringent requirements described above.

[66] S. 968 as reported, §4(a).

[67] S. 968 as reported, §4(d)(2).

[68] *Id.*

[69] S. 968 as reported, §4(e).

[70] S. 968 as reported, §§3(b)(1), 4(b)(1).

The Attorney General is also required by S. 968 to provide notice of the alleged violation and intent to proceed under the act to the registrant of the domain name or to the owner/operator of the Internet site, by using the postal or email address of the registrant/owner or by some other means that the court finds necessary.[71] The PROTECT IP Act places a similar notice requirement upon the quantifying plaintiff.[72]

Any person bound by a court order (registrant of the domain name, owner/operator of the Internet site, financial transaction provider, Internet advertising service) may file a motion with the court to modify, suspend, or vacate the order; the court may grant such relief if the court finds that either (1) the Internet site associated with the domain name is no longer, or never was, dedicated to infringing activities, or (2) the interests of justice require it.[73]

To encourage financial transaction providers and Internet advertising services to "self-police," the PROTECT IP Act makes them immune from liability for voluntarily taking action against an Internet site, so long as they act in good faith on credible evidence that the Internet site is dedicated to infringing activities.[74]

S. 968 provides immunity from liability to more actors when they refuse to provide services to "infringing Internet sites that endanger the public health." An "infringing Internet site that endangers the public health" is an Internet site that sells, dispenses, or distributes counterfeit prescription medicine. Domain name registries, domain name registrars, financial transaction providers, search engines, and Internet advertising services may refuse to provide services to such Internet sites when they have a good faith belief that the site is infringing.[75]

Reports to Congress

The PROTECT IP Act requires reports to Congress regarding the effectiveness of the act and its effect on Internet technologies, from the following government entities: the Attorney General, the Register of Copyrights, the Secretary of Commerce, and the Government Accountability Office.[76]

Summary of SOPA Provisions

As introduced, SOPA contains two titles: (1) Combating Online Piracy and (2) Additional Enhancements to Combat Intellectual Property Theft. Prior to the titles are savings and severability clauses. The first savings clause pronounces that "Nothing in this Act shall be construed to impose a prior restraint on free speech or the press protected under the 1st amendment to the Constitution." The second savings clause explains that nothing in Title I of this act shall be construed to enlarge or diminish copyright infringement liability for any cause of action under the Copyright Act, including any limitations on liability that the Copyright Act

[71] S. 968 as reported, §3(c)(1).

[72] S. 968 as reported, §4(c)(1).

[73] S. 968 as reported, §4(f).

[74] S. 968 as reported, §5(a).

[75] S. 968 as reported, §5(b).

[76] S. 968 as reported, §7.

provides. The severability clause explains that if any provision of this act is held to be unconstitutional, the other provisions of the act are not to be affected by that determination.

Title I of SOPA, "Combating Online Piracy"

Action by the Attorney General

Whether an Internet site may be subject to an action by the Attorney General under SOPA depends on if it qualifies as a "foreign infringing site." Section 102(a) of SOPA provides a definition of a "foreign infringing site" to mean

1. the Internet site (or portion thereof) is a U.S.-directed site and is used by users in the United States,
2. the owner/operator of such Internet site "is committing or facilitating the commission of" criminal trademark and copyright infringement, and
3. the Internet site would be subject to seizure in the United States by the Attorney General if such site were a domestic Internet site.[77]

Section 102(b) of SOPA authorizes the Attorney General to commence either an in personam action against a registrant of a domain name used by a foreign infringing site (or the owner/operator of such site), or an in rem action against a foreign infringing site or the foreign domain name used by such site. An in rem action is only permitted where, after diligence by the Attorney General, the domain name's registrant or the site's owner cannot be found.

Federal district courts are authorized by SOPA, following the commencement of these actions, to issue a temporary restraining order, a preliminary injunction, or an injunction against the registrant of the domain name used by the foreign infringing site, or the owner/operator of the foreign infringing site, to cease and desist from undertaking any further activity as a foreign infringing site.

A process server on behalf of the Attorney General, who obtains prior approval of the court, may serve a copy of the court's cease and desist order on third parties that fall within the following four categories; these parties that receive the court order are then required to take the actions specified below.

- **A service provider** is required to take "technically feasible and reasonable measures designed to prevent access by its subscribers located within the United States to the foreign infringing site (or portion thereof) that is subject to the order, including measures designed to prevent the domain name of the foreign infringing site (or portion thereof) from resolving to that domain name's Internet Protocol address. Such actions shall be taken as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order."[78]

[77] Examples of such domestic sites are those that have been seized by the U.S. Immigration and Customs Enforcement (ICE) in its "Operation In Our Sites" initiative, described at the outset of this report.

[78] H.R. 3261, §102(c)(2)(A)(i).

- **An Internet search engine** is required to "take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, designed to prevent the foreign infringing site that is subject to the order, or a portion of such site specified in the order, from being served as a direct hypertext link."[79]
- **A payment network provider** is required to "take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, designed to prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States or subject to the jurisdiction of the United States and the payment account" that is used by the foreign infringing site and through which the payment network provider would complete such payment transactions.[80]
- **An Internet advertising service** is required to "take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, designed to prevent its service from providing advertisements to or relating to the foreign infringing site that is subject to the order or a portion of such site specified in the order; cease making available advertisements for the foreign infringing site or such portion thereof, or paid or sponsored search results, links, or other placements that provide access to such foreign infringing site or such portion thereof; and cease providing or receiving any compensation for advertising or related services to, from, or in connection with such foreign infringing site or such portion thereof."[81]

SOPA authorizes the Attorney General to bring an action for injunctive relief against any party that receives this court order and knowingly and willfully fails to comply with the obligations described above. A defendant in such an action may establish an affirmative defense by showing that it does not have the technical means to comply without incurring an unreasonable economic burden.[82]

SOPA also authorizes the Attorney General to bring an action for injunctive relief against "any entity that knowingly and willfully provides or offers to provide a product or service designed or marketed for the circumvention or bypassing of measures" that were taken by any of the parties that received the court order.[83]

[79] H.R. 3261, §102(c)(2)(B).

[80] H.R. 3261, §102(c)(2)(C).

[81] H.R. 3261, §102(c)(2)(D).

[82] H.R. 3261, §102(c)(4).

[83] H.R. 3261, §102(c)(4)(A)(ii). The bill defines "a product or service designed or marketed for the circumvention or bypassing of measures" to mean a product or service that is designed or marketed to enable a domain name described in the court order to (1) resolve to that domain name's Internet protocol address notwithstanding the measures taken by the service provide to prevent such resolution, or (2) resolve to a different domain name or Internet protocol address that the provider of the product or service knows, reasonably should know, or reasonably believes is used by an Internet site offering substantially similar infringing activities as those with the infringing foreign site that is subject to the court order. H.R. 3261, §102(c)(4)(D).

Actions by a "Qualifying Plaintiff"

Whether an Internet site (that may be either domestic or foreign) may be subject to a private right of action by a "qualifying plaintiff" under SOPA depends on if the Internet site is one that is "dedicated to theft of U.S. property." An intellectual property right holder who is "harmed by" the activities of such an Internet site is classified by SOPA as a "qualifying plaintiff."[84] SOPA provides a definition of the term "Internet site is dedicated to theft of U.S. property" to mean

1. an Internet site, or a portion thereof, that is a U.S.-directed site and is used by users within the United States; **and**
2. either:
    a. "the U.S.-directed site is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator or another acting in concert with that operator for use in, offering goods or services in a manner that engages in, enables, or facilitates:" (1) copyright infringement, (2) circumvention of copyright protection systems, or (3) the sale, distribution, or promotion of goods, services, or materials bearing a counterfeit mark, **or**
    b. the operator of the U.S.-directed site:
        i. "is taking, or has taken, deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out acts that constitute" copyright infringement or circumvention of copyright protection systems, **or**
        ii. "operates the U.S.-directed site with the object of promoting, or has promoted, its use to carry out acts that constitute" copyright infringement or circumvention of copyright protection systems, "as shown by clear expression or other affirmative steps taken to foster infringement."[85]

Notification Process (No Court Involvement)

Subsection 103(b) of SOPA authorizes a qualifying plaintiff to send written notifications to payment network providers and Internet advertising services regarding an Internet site that is dedicated to the theft of U.S. property. Such notification must, among other things, include the following items:

- Identify the Internet site that is allegedly dedicated to the theft of U.S. property, including the domain name or Internet Protocol address of such site.
- Identify specific facts to support a claim that the Internet site is dedicated to theft of U.S. property, and that "clearly show that immediate and irreparable injury, loss, or damage will result to the holder of the intellectual property right harmed by the activities" of such Internet site "in the absence of timely action by the payment network provider or Internet advertising service."

[84] H.R. 3261, §103(a)(2) (definition of "qualifying plaintiff").

[85] H.R. 3261, §103(a)(1) (definition of "Internet site is dedicated to theft of U.S. property").

- "Information reasonably sufficient to establish that the payment network provider or Internet advertising service is providing payment processing or Internet advertising services for such site."
- "A statement that the holder of the intellectual property right has a good faith belief that the use of the owner's works or goods in which the right exists, in the manner described in the notification, is not authorized by the holder, its agent, or law."[86]

A payment network provider or Internet advertising service is required to "take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after" delivery of the notification, that are, respectively, "designed to prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States and the Internet site" or "prevent its service from providing advertisements to or relating to the Internet site."[87]

The owner/operator of the Internet site may file a "counter notification" to the payment network provider or Internet advertising service that states (under penalty of perjury) that the owner/operator/registrant of the Internet site "has a good faith belief that it does not meet the criteria of an Internet site dedicated to theft of U.S. property."[88]

SOPA provides liability (in the form of damages, costs, and attorneys' fees) for any provider of a notification or counter notification who, respectively, knowingly materially misrepresents that a site is an Internet site dedicated to the theft of U.S. property, or that such site does not meet the criteria of an Internet site dedicated to the theft of U.S. property.[89]

Civil Actions for Injunctive Relief

If a counter notification is filed, or if a payment network provider or Internet advertising service fails to comply with its obligations upon receiving the notification, Section 103(c) of SOPA allows the qualifying plaintiff to commence an in personam action against the registrant of the domain name used by the Internet site, or the owner/operator of the Internet site. If the qualifying plaintiff cannot find these individuals through due diligence, he or she may bring an in rem action against the Internet site or the domain name used by such site.[90]

SOPA authorizes federal district courts, following the commencement of this action by the qualifying plaintiff, to issue a temporary restraining order, a preliminary injunction, or an injunction against the registrant/owner/operator of the Internet site, to cease and desist from undertaking any further activity as an Internet site dedicated to theft of U.S. property.[91]

A qualifying plaintiff who obtains prior approval of the court may serve a copy of the court's cease and desist order on payment network providers and Internet advertising services, which are

[86] H.R. 3261, §103(b)(4)(A).

[87] H.R. 3261, §103(b)(1), (2).

[88] H.R. 3261, §103(b)(5).

[89] H.R. 3261, §103(b)(6).

[90] H.R. 3261, §103(c)(2).

[91] H.R. 3261, §103(c)(5).

then required to take the same measures as required of these parties under the action brought by the Attorney General described above. If the qualifying plaintiff demonstrates to the federal court probable cause to believe that any of these third parties that received the court order has not complied with its obligations, the court shall require the entity to explain why an order should not be issued directing it to comply with the obligations and to impose a monetary sanction.[92] An entity against whom this relief is sought may establish an affirmative defense by showing that it does not have the technical means to comply without incurring an unreasonable economic burden.

Due Process, Safeguards, and Limitations on Liability

SOPA would require courts to follow Rule 65 of the Federal Rules of Civil Procedure (FRCP) in deciding whether to issue injunctive relief in either an action brought by the Attorney General against a nondomestic entity, or an action brought by a qualifying plaintiff against domestic or nondomestic parties.[93] Rule 65 of the FRCP provides that a "court may issue a preliminary injunction only on notice to the adverse party," and that a "court may issue a temporary restraining order without written or oral notice to the adverse party or its attorney only if: (A) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required." Thus, Rule 65 requires that, prior to the issuance of a preliminary injunction, the party that is the target of the injunction is entitled to notice and an opportunity to be heard. However, an ex parte temporary restraining order (with no notice to the adverse party) may be granted if the party seeking the order satisfies the stringent requirements described above.

SOPA requires the Attorney General to provide notice of the alleged violation and intent to proceed under the act to the registrant of the domain name or to the owner/operator of the Internet site, by using the postal or email address of the registrant/owner or by some other means that the court finds necessary.[94] The bill requires qualifying plaintiffs to provide similar notice.[95]

SOPA provides immunity from liability to third parties for their actions taken to reasonably comply with the court order.[96]

Any person bound by the court order (registrant of the domain name, owner/operator of the Internet site, service provider, Internet search engine, payment network provider, Internet advertising service) may file a motion with the court to modify, suspend, or vacate the order; the court may grant such relief if the court finds that either (1) the Internet site associated with the domain name is no longer, or never was, a foreign infringing site, or (2) the interests of justice require it.[97]

[92] H.R. 3261, §103(d)(4).

[93] H.R. 3261, §§102(b)(5), 103(c)(5).

[94] H.R. 3261, §102(b)(3).

[95] H.R. 3261, §103(c)(3).

[96] H.R. 3261, §§102(c)(5), 103(d)(5).

[97] H.R. 3261, §§102(d), 103(e).

To encourage certain third parties to "self-police," SOPA provides immunity from any cause of action for service providers, payment network providers, Internet advertising services, Internet search engines, domain name registries, or domain name registrars, that voluntarily take action against an Internet site, so long as they act in the reasonable belief that (1) the Internet site is a foreign infringing site or is dedicated to theft of U.S. property, and (2) the action is consistent with the entity's terms of service or other contractual rights.[98]

SOPA also provides immunity from liability to service providers, payment network providers, Internet advertising services, advertisers, Internet search engines, domain name registries, or domain name registrars, when they, in good faith and based on credible evidence, stop providing or refuse to provide services to "an Internet site that endangers the public health."[99] "An Internet site that endangers the public health" is defined by subsection (c) to mean an Internet site that is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator for use in (1) offering/selling/dispensing/distributing prescription medicine without a valid prescription, or (2) offering/selling/dispensing/distributing prescription medicine that is adulterated or misbranded.

Reports to Congress

SOPA requires the Register of Copyrights to "conduct a study on the enforcement and effectiveness of this title and on any need to amend the provisions of this title to adapt to emerging technologies."[100]

SOPA also requires the Intellectual Property Enforcement Coordinator (IPEC), in consultation with the Secretaries of the Treasury and Commerce, the United States Trade Representative, the Chairman of the Securities and Exchange Commission, and the heads of other departments and appropriate agencies, to identify and conduct an analysis of notorious foreign infringers whose activities cause significant harm to holders of intellectual property rights in the United States.[101] The IPEC is required to submit a report to Congress that includes, among other things, "an examination of whether notorious foreign infringers have attempted to or succeeded in accessing capital markets in the United States for funding or public offerings," and "whether notorious foreign infringers that engage in significant infringing activity should be prohibited by the laws of the United States from seeking to raise capital in the United States, including offering stock for sale to the public."[102]

[98] H.R. 3261, §104.

[99] H.R. 3261, §105.

[100] H.R. 3261, §106(b).

[101] H.R. 3261, §107(a).

[102] H.R. 3261, §107(b).

Title II of SOPA, "Additional Enhancements to Combat Intellectual Property Theft"

Streaming of Copyrighted Works in Violation of Criminal Law

Section 201 of SOPA would amend the criminal copyright statutes (17 U.S.C. §506, 18 U.S.C. §2319) to provide additional criminal penalties for unlawful public performances of copyrighted works over the Internet using technology such as "streaming." This section authorizes a maximum five-year prison sentence for those who, without authorization, willfully stream commercially valuable copyrighted material for purposes of commercial advantage or private financial gain. In addition, this section would authorize misdemeanor and felony penalties for *non-commercial* willful public performance by means of digital transmission, during any 180-period, of 1 or more copyrighted works, where the total retail value of the public performance exceeds $1,000. For a detailed analysis and discussion of the changes that Section 201 would make to existing law, see CRS Report R41975, *Illegal Internet Streaming of Copyrighted Content: Legislation in the 112th Congress*, by Brian T. Yeh.

Trafficking in Inherently Dangerous Goods or Services

Section 202 of SOPA would amend 18 U.S.C. Section 2320 (the criminal offense of trafficking in counterfeit goods or services) to include the intentional importation, exportation, or trafficking of counterfeit drugs.[103] This section also provides penalties if this criminal offense involves a good or service that, "if it malfunctioned, failed, or was compromised, could reasonably be foreseen to cause" (1) serious bodily injury or death, (2) disclosure of classified information, (3) impairment of combat operations, or (4) other significant harm, to a member of the Armed Forces, law enforcement agency, or national security or critical infrastructure. In order for a person to be liable under this new provision, the person must possess "knowledge that the good or service is falsely identified as meeting military standards or is intended for use in a military or national security application, or a law enforcement or critical infrastructure application."

Protecting U.S. Businesses From Foreign and Economic Espionage

Section 203 of SOPA would increase the penalties for the criminal offense of theft of trade secrets by someone who intends or knows that the offense will benefit any foreign government (18 U.S.C. §1831(a)), from the existing 15 years in prison to 20 years, and from a $500,000 fine to "not less than $1,000,000 and not more than $5,000,000." If this offense is committed by organizations, the penalty is changed from the existing fine of "not more than $10,000,000" to "not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization (including expenses for research and design or other costs of reproducing the trade secret that the organization has thereby avoided)."

[103] Other legislation in the 112th Congress provide similar amendments to 18 U.S.C. §2320 (although with more stringent penalties), *see* Counterfeit Drug Penalty Enhancement Act of 2011 (H.R. 3468 and S. 1886).

Amendments to Sentencing Guidelines

Section 204 of SOPA directs the U.S. Sentencing Commission to review and, if appropriate, amend the Federal Sentencing Guidelines and policy statements applicable to persons convicted of intellectual property offenses, trafficking in counterfeit goods or services, and economic espionage.

Defending Intellectual Property Rights Abroad

Section 205 of SOPA directs the Secretary of State and the Secretary of Commerce, in consultation with the Register of Copyrights, to "ensure that the protection in foreign countries of the intellectual property rights of United States persons is a significant component of United States foreign and commercial policy in general, and in relations with individual countries in particular." This section also requires the Secretary of State and the Secretary of Commerce, in consultation with the Register of Copyrights, to "appoint at least one intellectual property attaché to be assigned to the United States embassy or diplomatic mission (as the case may be) in a country in each geographic region covered by a regional bureau of the Department of State."

Debate Over the Legislation

Numerous concerns have been raised about the provisions of the PROTECT IP Act and SOPA by a variety of organizations, including human rights and civil liberties groups, technology companies, law professors, public interest groups, and consumer organizations. These concerns, and the responses by the legislation's supporters (the bills' sponsors as well as organizations representing intellectual property rights holders, labor unions, and small and large businesses that manufacture and sell goods), can be organized broadly into the following categories.

Impact on Free Speech

Some commentators are concerned that the expansive definitions used by the bills to describe an Internet site that is "dedicated to infringing activity" (PROTECT IP Act) or an Internet site that is "dedicated to theft of U.S. property" (SOPA) could impact non-infringing content that is legitimate speech protected by the First Amendment.[104] Editorials from several major newspapers have also expressed serious reservations about the overly broad definitions.[105] Others claim that the legislation will give owners of copyrighted content "broad censorship powers."[106] These concerns are heightened by fears that the act provides insufficient legal process.[107]

---

[104] *See, e.g.,* Letter from Mark Lemley, Professor, Stanford Law School, et al. to Sen. Judiciary Comm. (June 27, 2011), Open Letter from Mark Lemley to the House of Representatives (November 15, 2011), and Laurence H. Tribe, *The "Stop Online Piracy Act" (SOPA) Violates the First Amendment, available at* http://www.net-coalition.com/wp-content/uploads/2011/08/tribe-legis-memo-on-SOPA-12-6-11-1.pdf.

[105] *See, e.g.,* Editorial, "Internet Piracy and How to Stop It," NEW YORK TIMES, June 9, 2011; Editorial, "Piracy vs. an Open Internet," LOS ANGELES TIMES, November 25, 2011.

[106] Mike Masnick, *Son of COICA*, Techdirt, May 10, 2011, http://www.techdirt.com/articles/20110510/13285714230/.

[107] *See, e.g., H.R. 3261, the "Stop Online Piracy Act": Hearing Before the H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Katherine Oyama, Copyright Counsel, Google, Inc.).

Opponents of the legislation argue that repressive foreign regimes could cite U.S. domain name seizures to justify online suppression of speech. Eric Schmidt, executive chairman of Google, compared the domain name blocking approach to China's attempts to stifle free speech. He warned that any legislative measure that authorizes domain name blocking could set a disastrous precedent if done the wrong way.[108] There is concern that backing away from an open and global Internet could set "a precedent for other countries ... to use DNS [domain name system] mechanisms to enforce a range of domestic policies, erecting barriers on the global medium of the Internet. Non-democratic regimes could seize on the precedent to justify measures that would hinder online freedom of expression and association."[109]

However, supporters of the legislation note that "[a]ll existing copyright protections are applicable to the Internet" and that "injunctions are a longstanding, constitutionally sanctioned way to remedy and prevent copyright violations."[110] The Register of Copyrights also has stated that she does not believe that shutting down a website that is devoted to infringing activity would violate the First Amendment or that it constitutes censorship, yet she also stressed that "[c]are must be taken to ensure that noninfringing expression is not unnecessarily suppressed and that the relief is effective but narrowly tailored."[111] Supporters also point to Supreme Court precedents in favor of injunctions for copyright infringement, even when the copyrighted material is a matter of public debate.[112] Nevertheless, these supporters concede that "the most troublesome First Amendment concerns" would be raised "where an entire website could be blocked or seized for a single, or just a few, [infringing] offenses."[113] Yet they assert that neither the PROTECT IP Act nor SOPA would permit such an result.[114]

In addition, supporters of the legislation argue that the legislation provides sufficient procedural protections by incorporating Rule 65 of the Federal Rules of Civil Procedure as the basis for governing the process by which federal judges may issue a temporary restraining order, preliminary injunction, or injunction.[115] As explained earlier in this report, Rule 65 provides

---

[108] Nathan Olivarez-Giles, "Google's Eric Schmidt: Blocking File-sharing Sites Would Make U.S., Britain like China," *Los Angeles Times,* May 18, 2011, available at http://latimesblogs.latimes.com/technology/2011/05/google-eric-schmidt-says-blocking-filesharing-sites-would-make-u-s-u-k-ike-china.html.

[109] Letter from Center for Democracy and Technology et al. to Sen. Patrick Leahy, Chairman Sen. Judiciary Comm. (May 25, 2011) available at http://www.cdt.org/files/pdfs/20110525_public_interet_968_ltr.pdf.

[110] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Floyd Abrams, Partner, Cahill Gordon & Reindel LLP).

[111] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Maria Pallante, Acting Register of Copyrights).

[112] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Floyd Abrams, Partner, Cahill Gordon & Reindel LLP *citing Harper & Row v. Nation Enters.*, 471 U.S. 539 (1985) (finding an injunction against a magazine's infringing publication of portions of Gerald Ford's memoir valid)).

[113] *Id.*

[114] *H.R. 3261, the "Stop Online Piracy Act": Hearing Before the H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Maria Pallante, Register of Copyrights); *see also* Letter of Counsel on PROTECT IP Act and SOPA, December 12, 2011, *available at* http://judiciary.house.gov/issues/Rogue%20Websites/Letter%20of%20Counsel.pdf (observing that because the bills "target only those websites that are wholly or almost entirely devoted to piracy … such illicit activities are not protected by the First Amendment.").

[115] *Id.*

certain procedural safeguards, including requiring notice to the allegedly infringing website and providing an opportunity for that party to be heard and defend themselves before an order is issued. Foreign entities would be entitled to these same procedural safeguards as U.S.-based website operators.[116]

Technical Integrity of the Internet

Opponents of the legislation have raised concerns that the bills, if either is enacted into law, may affect the integrity of the Internet.[117] They claim that "DNS blocking itself could affect the Internet's reliability, security, and performance."[118] Other commentators have called the domain name blocking approach ineffective,[119] noting that the Internet sites will still remain available through their Internet protocol addresses:

> [D]omain name address resolution takes place throughout the Internet, not just by larger ISPs and registries. Indeed, there are as many as a million worldwide domain names "resolvers," and it is unlikely U.S. courts could or would order all of them to comply with a blocking order. But incomplete blocking could seriously undermine the integrity of this key feature of the Web's architecture, incentivizing truly rogue Web site operators to use shadow registration systems or simply forgo domain names and rely solely on IP addresses.[120]

A group of Internet network engineers have argued that DNS filtering requirements under both bills "is incompatible with" implementation of the new security protocols known as DNS Security Extensions (DNSSEC), which have been promoted and supported by the federal government to further national cybersecurity goals.[121] They warn that "[a] legal mandate to operate DNS servers in a manner inconsistent with end-to-end DNSSEC would therefore interfere with the rollout of this critical security technology and stifle this emerging platform for innovation."[122]

---

[116] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Floyd Abrams, Partner, Cahill Gordon & Reindel LLP).

[117] Letter from Internet Engineers Opposed to COICA, to Sen. Judiciary Comm. (September 28, 2010) available at http://www.publicknowledge.org/files/docs/COICA_internet_engineers_letter.pdf (discussing similar provisions in a preceding bill).

[118] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Kent Walker, Senior Vice President, Google).

[119] *See e.g.* Editorial, "Internet Piracy and How to Stop It," NEW YORK TIMES, June 9, 2011, p. A26; Editorial, "Policing the Internet", LOS ANGELES TIMES, June 7, 2011, available at http://articles.latimes.com/2011/jun/07/opinion/la-ed-protectip-20110607.

[120] Larry Downes, *Leahy's Protect IP Bill Even Worse than COICA,* CNET News (June 20, 2011 2:46 p.m.), http://news.cnet.com/8301-13578_3-20062419-38.html.

[121] Steve Crocker et al., *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill,* available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf.

[122] *Id.* at 6; *see also* Letter from Leonard M. Napolitano, Jr., Sandia National Laboratories, to Representative Zoe Lofren, November 16, 2011 (concluding that "the Domain Name Service (DNS) filtering/redirection mandates in the bills 1) are likely to be effective, 2) would negatively impact U.S. and global cybersecurity and Internet functionality, and 3) would delay the full adoption of DNSSEC and its security improvements over DNS.").

Supporters respond that taking down infringing Internet sites is akin to "whac-a-mole" and that the law must provide sufficient authority to combat this problem.[123] Furthermore, supporters believe the DNS blocking provisions of the legislation are key to preventing foreign sites from infringing American intellectual property rights:

> Reaching sites originating outside the U.S. is critical to fighting a worldwide epidemic that is destroying the ability of the [content owners] to obtain the financing needed to produce future [content].... Internet sites that steal and distribute American intellectual property are often foreign-owned and operated, or reside at domain names that are not registered through a U.S.-based registry or registrar, setting them outside the scope of U.S. law enforcement. The Justice Department and rights holders are currently limited in their options for legal recourse, even when the website is directed at American consumers and steals American-owned intellectual property.[124]

Supporters also observe that site blocking and filtering technology that is often used to combat spam, malware, and viruses, have had "no adverse impact on the Internet."[125] Furthermore, they argue that there is no technical reason why DNS filtering and DNSSEC need to be incompatible; rather, network engineers can and will find a way to make the required changes to the DNSSEC code to ensure no such conflict occurs.[126]

Private Cause of Action

There is considerable consternation from opponents of the legislation that the problems they have identified will be exacerbated by including the new enforcement mechanisms available to intellectual property rights holders. They worry that content owners will use the private right of action to stifle Internet innovation and protect outdated business models.[127] "[T]he Internet and digital technologies can be highly disruptive of traditional business models for reasons having nothing to do with infringement."[128] Additionally, technology companies are concerned that they will be unable to cope with thousands of suits from content owners. They argue that these suits will overwhelm their ability to handle requests and ultimately increase costs for consumers.[129] "We believe that the currently proposed private litigation-based process will, however

---

[123] The references to "whac-a-mole" are ubiquitous. *See e.g. Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (written statement of Tom Adams, Chief Executive Officer, Rosetta Stone).

[124] Press Release, The Motion Picture Association of America, Broad Creative Industry Coalition Praises Senate Introduction of Bipartisan Legislation to fight Online Theft (May 12, 2011) available at http://mpaa.org/resources/e62fa607-8234-4120-97f2-aa4082cd691a.pdf.

[125] *H.R. 3261, the "Stop Online Piracy Act": Hearing Before the H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Michael P. O'Leary, Senior Executive Vice President, the Motion Pictures Association of America, Inc.).

[126] *Id.; see also* Daniel Castro, *PIPA/SOPA: Responding to Critics and Finding a Path Forward,* December 2011, The Information Technology & Innovation Foundation, *at* http://www.itif.org/files/2011-pipa-sopa-respond-critics.pdf.

[127] *See* Abigail Phillips, *The "PROTECT IP" Act: COICA Redux, The* Electronic Frontier Foundation (June 20, 4:31 p.m.), https://www.eff.org/deeplinks/2011/05/protect-ip-act-coica-redux (wondering whether Viacom would have quashed YouTube had the bill been law at the time).

[128] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of David Sohn, Senior Policy Counsel, Center for Democracy and Technology).

[129] See *Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (written statement of Thomas Dailey, General Counsel, Verizon).

unintentionally, become a one-sided litigation machine with rights owners mass-producing virtually identical cases against foreign domain names for the purpose of obtaining orders to serve on U.S. payment and advertising companies."[130]

Proponents of the legislation argue that online infringement is rampant and that law enforcement lacks the resources to deter infringing activities. Additionally, they point out that in an action brought by a qualifying plaintiff, the court order may only be served on payment processors and online advertisers to require them to cut off financial ties to the Internet site; therefore, content owners lack the power under either bill to block domain names or websites. In contrast, the Attorney General can serve the court order on DNS operators (PROTECT IP Act), service providers (SOPA), and search engines to require them to prevent access to infringing websites (in addition to having the authority to serve the court order on the financial intermediaries). As the Register of Copyrights has explained, the enforcement structure provided by the bills:

> appropriately provides much broader tools and flexibility to the Attorney General than it provides to copyright owners. This is a sound policy choice at this time. The Department of Justice has experience fighting online infringers, will use resources carefully, must exercise prosecutorial discretion in bringing actions, and must plead its case to the court and obtain a court-issued order before proceeding. Put another way, while the copyright industries are extremely important (and certainly a point of pride with respect to the U.S. economy), [the legislation] recognizes that many sectors rely on, invest in, and contribute to the success of the Internet.
>
> It is for this reason that [the legislation] puts only limited tools in the hands of copyright owners, and provides the Attorney General with the sole authority to seek orders against search engines and Internet service providers.[131]

Conflict with the DMCA "Safe Harbors" and Potential Impact on Internet Innovation (Referring to SOPA Only)

Section 512(m) of the Digital Millennium Copyright Act (DMCA) (17 U.S.C. §512(m)) explains that a service provider that seeks a safe harbor from liability (as described earlier in this report) is not required to "monitor[] its service or affirmatively seek[] facts indicating infringing activity" as a condition of enjoying such safe harbor.

Critics of SOPA note that, unlike the PROTECT IP Act, SOPA appears to effectively repeal 17 U.S.C. Section 512(m) and erode the safe harbor protections available to many Internet companies under the DMCA with its definition of an "Internet site [] dedicated to theft of U.S. property" (applicable to actions by qualifying plaintiffs). Such definition includes an operator of a U.S.-directed site that "is taking, or has taken, deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out acts that constitute" copyright infringement or circumvention of copyright protection systems.[132] In the view of SOPA's critics, this definition would mean that companies that host user-generated content websites (such as

[130] Letter from American Express et al. to Sen. Patrick Leahy, Chairman, Sen. Judiciary Comm. (May 25, 2011) available at http://www.publicknowledge.org/letter-opposing-PIPA-privaterightofaction.

[131] *H.R. 3261, the "Stop Online Piracy Act": Hearing Before the H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Maria Pallante, Register of Copyrights).

[132] H.R. 3261, §103(a)(1)(B)(ii)(I).

YouTube) and operators of cloud computing storage services (such as Dropbox) would need to monitor, filter, and otherwise police user behavior for infringing activities, in order to avoid being covered by the definition.[133] In addition, while SOPA does not directly modify the DMCA safe harbor provisions, SOPA "creates uncertainty about whether court orders issued against 'foreign infringing sites' and 'sites dedicated to theft' might disqualify an online service provider from the DMCA safe harbors."[134] This "legal uncertainty for Internet companies" means that "SOPA will significantly deter current and future Internet businesses from investing in new ventures."[135]

Others point out that although the "notice and takedown" provisions of the DMCA may be abused by content owners making erroneous claims, the consequence is the blocking or removal of such content, whereas under SOPA's notification process available to qualifying plaintiffs, the consequence for false claims is that the money to the website is stopped.[136] They note that such funds (that the website may depend on to exist) may be cut off merely "based on an allegation of harm that falls short of an allegation of infringement."[137]

Supporters of SOPA observe that while the DMCA has worked well for copyright holders and service providers to address online infringement, the DMCA's "notice and takedown" procedures are ineffective against foreign rogue sites; furthermore, the DMCA does not apply to trademark infringement and does not address the use of financial intermediaries such as payment processors and Internet advertising services.[138] Other supporters contend that SOPA's notification process is less likely to be misused than the DMCA's "notice and takedown" procedure, because under the latter, a service provider has an incentive to remove infringing content in order to preserve its safe harbor from liability. In contrast, Internet advertisers and payment processors "don't have business incentives to comply with bad faith notices under SOPA. Each site they are ordered to block is, presumably, a paying customer or revenue source."[139] Thus, not many such companies would be willing to "rubber-stamp any and every order that cuts into their bottom line without some way of making sure the site at issue is one that genuinely falls within the scope of" SOPA.[140]

Other supporters disagree that SOPA will diminish investment in new technology ventures or stifle innovation. They believe that "strong copyright law promotes innovation," and observe that

---

[133] Corynne McSherry, *SOPA: Hollywood Finally Gets a Chance to Break the Internet,* Electronic Frontier Foundation, October 28, 2011, *at* https://www.eff.org/deeplinks/2011/10/sopa-hollywood-finally-gets-chance-break-internet.

[134] *H.R. 3261, the "Stop Online Piracy Act": Hearing Before the H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Katherine Oyama, Copyright Counsel, Google, Inc.).

[135] *Id.*

[136] Mike Masnick, *The Definitive Post on Why SOPA and PROTECT IP are Bad, Bad Ideas,* Techdirt, November 22, 2011, *at* http://www.techdirt.com/articles/20111122/04254316872/definitive-post-why-sopa-protect-ip-are-bad-bad-ideas.shtml.

[137] Rashmi Rangnath, *SOPA and the DMCA Safe Harbors,* Public Knowledge, November 3, 2011, *at* http://www.publicknowledge.org/blog/sopa-and-dmca-safe-harbors ("Thus far, a copyright holder has had to allege that her copyright was infringed before she can take action under the law. Under SOPA, however, a copyright owner could argue that because a site allows users to upload material, and indeed many have uploaded infringing material, she is harmed by the site's activities. After all, her work could be in imminent danger of being uploaded without her permission.").

[138] Statement of Judiciary Committee Chairman Lamar Smith, *Hearing on H.R. 3261, the "Stop Online Piracy Act,"* November 16, 2011.

[139] Terry Hart, *How the Stop Online Piracy Act Will Hit What It Aims At,* Copyhype, October 31, 2011, *at* http://www.copyhype.com/2011/10/how-the-stop-online-piracy-act-will-hit-what-it-aims-at/.

[140] *Id.*

"[m]any of the loudest voices opposing rogue sites legislation are the same critics who predicted disaster in the wake of the DMCA, the NET Act (No Electronic Theft Act),[141] and the unanimous Supreme Court decision in *Grokster*.[142] Yet since those events occurred, the Internet has grown by leaps and bounds, innovation is off the charts and access to technology is at an all time high."[143]

Manager's Amendment to H.R. 3261 (SOPA)

As noted earlier in this report, House Judiciary Chairman Lamar Smith released a manager's amendment in the nature of a substitute to H.R. 3261 on December 12, 2011. The manager's amendment offers several substantial changes to SOPA, several of which would more closely align the provisions of SOPA with those in the PROTECT IP ACT, including the following:

- Adds additional savings clauses, including one that clarifies that nothing in title I of SOPA shall be construed to impose a duty on service providers to monitor activity on their network or service. Another savings clause specifies that service providers are not required take actions that would impair the security or integrity of the domain name system.
- Removes the non-judicial "written notification procedure" that was originally available to rights holders, leaving only one private enforcement mechanism for rights holders under SOPA (the same one provided by the PROTECT IP Act)– they must seek the authorization of a court in order to create a legal obligation on the part of payment processors and Internet advertisers to cease doing business with the offending website.
- Revises SOPA's definition of a "U.S.-directed site" to expressly require that the website be a foreign Internet site, thus removing domestic websites from the scope of the act's provisions. (Note that the PROTECT IP Act permits private plaintiff actions against domestic websites).
- Changes the definition of "foreign infringing site" (which applies to the Section 102 action by the Attorney General) to remove the requirement that the owner/operator of the site is committing or facilitating the commission of criminal trademark and copyright infringement. Instead, the definition of a "foreign infringing site" is a website that "is being operated in a manner that would, if it were a domestic Internet site, subject it (or its associated domain name) to seizure or forfeiture in the United States" under exiting law.

[141] The No Electronic Theft Act, P.L. 105-147, 111 Stat. 2678 (1997), was enacted to enable criminal prosecution of certain peer-to-peer file-sharing of copyrighted works. For a detailed discussion of this law, *see* CRS Report R41975, *Illegal Internet Streaming of Copyrighted Content: Legislation in the 112th Congress*, by Brian T. Yeh.

[142] The Supreme Court in its 2005 opinion *Metro-Goldwyn-Mayer Studios v. Grokster* held that one who distributes a device "with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties." For more information, *see* CRS Report RL31998, *File-Sharing Software and Copyright Infringement: Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, by Brian T. Yeh and Robin Jeweler.

[143] *H.R. 3261, the "Stop Online Piracy Act": Hearing Before the H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Michael P. O'Leary, Senior Executive Vice President, the Motion Pictures Association of America, Inc.).

- Changes the definition of an "Internet site dedicated to theft of U.S. property" (which applies to the Section 103 action by private plaintiffs) to require that in order for a website to meet such definition, the website's violation of copyright must be for purposes of commercial advantage or private financial gain. (The PROTECT IP Act does not contain such a requirement). In addition, the revised definition eliminates SOPA's original language that would have encompassed a website offering goods or services in a manner that "engages in, enables, or facilitates" infringement. (The PROTECT IP Act uses these three verbs in its definition of an Internet site dedicated to infringing activities.). Finally, the revised definition drops language that would have included a website that "is taking, or has taken, deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out acts that constitute" copyright infringement or circumvention of copyright protection systems.
- Provides a new section (Section 104) that states: "In any case in which only a specifically identified portion of an Internet site is identified by the court as a foreign infringing site or as an Internet site dedicated to theft of U.S. property, and made subject to an order [under section 102 and 103], the relief granted under such subjection, and the obligations of any entity served with a copy of an order … shall be confined to that specified portion so identified and made subject to the order. Nothing in the order shall be interpreted to impose obligations on any entity served with a copy of the order with respect to any other portion of an Internet site not specified in the order."
- Deletes SOPA's original requirement that service providers take "measures designed to prevent the domain name of the foreign infringing site (or portion thereof) from resolving to that domain name's Internet Protocol address." Instead, the manager's amendment allows a service provider to take "such measures as it determines to be the least burdensome, technically feasible, and reasonable means designed to prevent access by its subscribers located within the United States to the foreign infringing site that is subject to the order."
- Deletes SOPA's "5 day" time limit within which third parties would have had to satisfy their obligations to take actions against the foreign infringing site; rather, the manager's amendment provides that "[s]uch actions shall be taken as expeditiously as possible."

Summary of the OPEN Act

On December 17, 2011, Senator Wyden, along with Senators Cantwell and Moran, introduced S. 2029, the Online Protection and Enforcement of Digital Trade Act (OPEN Act), to serve as an alternative to the PROTECT IP Act and SOPA. S. 2029 has been referred to the Senate Committee on Finance. On January 18, 2012, Representative Darrell Issa introduced a version of the OPEN Act in the House, H.R. 3782, which is nearly identical to S. 2029. H.R. 3782 has been jointly referred to the House Ways and Means Committee and to the House Judiciary Committee.

The following is a brief summary of the key provisions of the OPEN Act.

International Trade Commission Enforcement

Section 337 of the Tariff Act of 1930 (19 U.S.C. §1337), as amended, prohibits unfair methods of competition or other unfair acts in the importation of products into the United States. It also prohibits the importation of articles that infringe valid U.S. patents, copyrights, processes, trademarks, or protected design rights. The International Trade Commission (ITC) is an independent, quasi-judicial federal government agency responsible for investigating and arbitrating complaints of unfair trade practices under section 337. The primary remedy employed by the ITC is to order the U.S. Customs and Border Protection (CBP) to stop imports from entering the border. Additionally, the ITC may issue cease and desist orders against individuals determined to be violators of intellectual property rights. The majority of unfair competition acts asserted under Section 337 involve allegations of patent infringement.[144]

The OPEN Act would amend the Tariff Act of 1930 to insert after Section 337 a new section 337A, entitled "Unfair Trade Practices Relating to Infringement of Copyrights and Trademarks By Certain Internet Sites."

Applicable Scope of New Section 337A, as added by the OPEN Act

The OPEN Act defines "infringing activity" to mean an activity that constitutes copyright infringement; circumvention of copyright protection systems; or the sale, distribution, or promotion of goods, services, or materials bearing a counterfeit mark.[145] It defines an "Internet site dedicated to infringing activity" to mean an Internet site that is (1) foreign, (2) conducts business directed at U.S. residents, and (3) "has only limited purpose or use other than engaging in infringing activity and whose owner or operator primarily uses the site" to **willfully** commit copyright infringement, circumvent copyright protection systems, or use counterfeit marks on products and services (emphasis added).[146] The OPEN Act provides several exclusions from this definition of an "Internet site dedicated to infringing activity," including (1) if the Internet site has a practice of complying with DMCA notice and takedown requests, (2) if the Internet site qualifies for a Section 512 DMCA safe harbor from liability, or (3) if the Internet site distributes content and goods that do not infringe a copyright or trademark.[147]

Violation

The OPEN Act declares that it is an unfair practice in import trade, and thus a violation of the new section 337A that it would add to the Tariff Act of 1930, for an Internet site dedicated to infringing activity to facilitate imports into the United States.[148] The ITC would be empowered to make the determination as to whether there has been such a violation. The only websites that may be investigated by the ITC are ones that have a nondomestic domain name; if the ITC discovers that the accused domain name is a domestic one, the ITC is required to terminate or not initiate

[144] For more information about Section 337 proceedings, *see* CRS Report RS22880, *Intellectual Property Rights Protection and Enforcement: Section 337 of the Tariff Act of 1930*, by Shayerah Ilias.

[145] S. 2029, §2, adding new §337A(a)(4).

[146] *Id.,* adding new §337A(a)(8)(A).

[147] *Id.,* adding new §337A(a)(8)(C).

[148] *Id.,* adding new §337A(b).

the investigation and then refer the matter to the Attorney General for further proceedings as the Attorney General determines is appropriate.[149] In addition, the OPEN Act requires the ITC to terminate, or not initiate, an investigation of a domain name if the operator of the associated Internet site provides a legal notice on the site that states that the operator consents to the jurisdiction and venue of the U.S. district courts.[150]

Complaint

The OPEN Act charges the ITC with the power and duty to investigate an alleged violation on its own initiative or upon receiving a complaint filed by a rights holder. An owner of a copyright or trademark that is the subject of the infringing activity on a nondomestic website may file a complaint with the ITC alleging, under oath, that the Internet site dedicated to infringing activity is being operated or maintained in violation of section 337A.[151] The OPEN Act requires the complainant to send a notice of the complaint to the registrant of the domain name at its postal and e-mail addresses, if they are reasonably available. In addition, the OPEN Act specifies that the complaint must identify (and notify) any financial transaction provider or Internet advertising company that may be required to take measures against the offending website, if the ITC determines that there has been a section 337A violation.

ITC Determination

The OPEN Act requires the ITC to determine, with respect to each section 337A investigation, whether or not the Internet site is operated or maintained in violation of section 337A. Final ITC determinations may be appealed to the U.S. Court of Appeals for the Federal Circuit.

The Senate version of the OPEN Act also provides the President with an opportunity to disapprove of any ITC determination "for policy reasons" no later than 60 days after the determination is made; such presidential disapproval nullifies the determination.[152] In contrast, the House version of the OPEN Act allows the President to disapprove of any ITC determination "for policy reasons" *at any time* after the ITC has made a determination regarding a foreign website.[153]

The OPEN Act permits the ITC, in administering a section 337A proceeding, to allow the submission of information electronically, hold hearing electronically or obtain testimony electronically, or "by such means as the Commission determines allows participation in proceedings … at as low a cost as possible to participants in the proceedings."[154]

[149] *Id.,* adding new §337A(c)(4).

[150] *Id.*, adding new §337A(c)(5).

[151] *Id.,* adding new §337A(d).

[152] *Id.,* adding new §337A(e)(4).

[153] H.R. 3782, adding new §337A(e)(4)(B).

[154] S. 2029, adding new §337A(e)(5)(B).

Remedies

The OPEN Act provides the ITC with the power to issue an order against the Internet site dedicated to infringing activity to cease and desist such activity, after the ITC makes the determination that such Internet site is in violation of the new section 337A.[155] The ITC may grant a temporary or preliminary cease and desist order against the Internet site if the complainant files with the ITC chairperson (or his designee) a petition requesting such order. The OPEN Act mandates that the ITC chairperson, prior to issuing a temporary or preliminary cease and desist order, must give the owner/operator of the Internet site an opportunity to be heard (which may include submitting information electronically). The ITC chairperson may issue such an order if he determines that "there is reason to believe" that an Internet site dedicated to infringing activity is operated or maintained in violation of section 337A.[156] The OPEN Act specifies that the ITC chairperson follow the provisions of rule 65 of the Federal Rules of Civil Procedure in deciding whether to issue the temporary or preliminary cease and desist order. If the complainant makes a showing of "extraordinary circumstances," the ITC chairperson may make a determination regarding the petition for a temporary cease and desist order on an expedited basis;[157] otherwise, the ITC chairperson is required to make a determination within 30 days.[158] The cease and desist order may last no longer than 14 days after its issuance, although the ITC chairperson may extend the order for additional periods of 14 days for good cause or with consent of the entity against which the order is issued. In order to discourage the filing of frivolous petitions for temporary or preliminary cease and desist orders, the ITC chairperson may require the complainant to post a bond; such bond may be forfeited to the owner of the Internet site if the ITC later determines that the Internet site was not in violation of section 337A.[159]

If the ITC "reasonably believes that a financial transaction provider or an Internet advertising service" is supplying services to an Internet site that is subject to a cease and desist order, the ITC may allow the complainant to serve a copy of the order upon the financial transaction provider or Internet advertising service.[160] Upon receipt of the order, financial transaction providers must take measures, as expeditiously as reasonable, to prevent or prohibit completion of payment transactions by the provider to the Internet site, and Internet advertising services must take technically feasible measures, as expeditiously as reasonable, to cease serving advertisements to the Internet site. The OPEN Act confers immunity from civil actions for these third parties that take any act reasonably designed to comply with these obligations (or that make a good faith effort to comply).

The Attorney General may bring an action for injunctive relief against any person subject to a cease and desist order who knowingly and willfully fails to comply with the order.[161] A defendant in such an action may assert an affirmative defense that the defendant lacks the technical means to comply with the order without incurring an unreasonable economic burden.

[155] *Id.,* adding new §337A(f)(1).

[156] *Id.,* adding new §337A(f)(2).

[157] *Id.,* adding new §337A(f)(2)(E)(i).

[158] *Id.*, adding new §337A(f)(2)(F)(i).

[159] *Id.*, adding new §337A(f)(2)(G).

[160] *Id.,* adding new §337A(g).

[161] *Id.,* adding new §337A(h).

The OPEN Act also confers immunity from liability (under any federal or state law) to a financial transaction provider or Internet advertising service for ceasing or refusing to provide services to an Internet site that the providers believe (in good faith and based on credible evidence) to be an Internet site that is primarily designed for the purpose of offering, selling, dispensing, or distributing any prescription medication without a valid prescription. (The PROTECT IP Act and SOPA contain a similar provision, although the two bills would extend such immunity to service providers, search engines, domain name registries and registrars in addition to financial transaction providers and Internet advertising companies.).

Section 337 Judges

The OPEN Act allows the ITC to appoint hearing officers, to be called "section 337 judges," to preside at the taking of evidence at section 337 and 337A hearings and to make initial and recommended decisions in investigations brought under section 337 and 337A of the Tariff Act of 1930. [162] A section 337 judge is required to possess a minimum of seven years of legal experience and be licensed to practice law; the OPEN Act allows the ITC to promulgate regulations regarding other qualifications of the section 337 judges, including technical expertise and experience in IP matters.

OPEN Act Compared to PROTECT IP Act and SOPA

While the PROTECT IP Act and SOPA rely primarily on the authority of federal judiciary for their enforcement measures, the OPEN Act places the responsibility of addressing online piracy and counterfeiting upon the International Trade Commission. In addition, the OPEN Act does not apply to Internet service providers and search engines and thus does not require or encourage domain name system filtering as a potential action against offending websites. The OPEN Act also only applies to foreign websites, whereas the PROTECT IP Act (as reported) and SOPA (as introduced) could apply to domestic websites in certain circumstances. Finally, the OPEN Act does not provide rights holders with a private right of action against rogue websites in federal courts; rights holders instead must seek relief through the ITC.

Author Contact Information

Brian T. Yeh
Legislative Attorney
byeh@crs.loc.gov, 7-5182

Acknowledgments

Portions of this report were prepared by Jonathan H. Miller, Law Clerk, American Law Division.

[162] *Id.,* §3, adding new 337B(a).