

Calendar No. 70

112TH CONGRESS }
1st Session }

SENATE

{ REPORT
112-39

PREVENTING REAL ONLINE THREATS TO ECONOMIC
CREATIVITY AND THEFT OF INTELLECTUAL PROPERTY
ACT OF 2011

JULY 22, 2011.—Ordered to be printed

Mr. LEAHY, from the Committee on the Judiciary,
submitted the following

R E P O R T

[To accompany S. 968]

The Committee on the Judiciary, to which was referred the bill (S. 968), to prevent online threats to economic creativity and theft of intellectual property, and for other purposes, having considered the same, reports favorably thereon, with an amendment in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

| | Page |
|---|------|
| I. Background and Purpose of the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 | 1 |
| II. History of the Bill and Committee Consideration | 11 |
| III. Section-by-Section Summary of the Bill | 16 |
| IV. Congressional Budget Office Cost Estimate | 21 |
| V. Regulatory Impact Evaluation | 21 |
| VI. Conclusion | 21 |
| VII. Changes to Existing Law Made by the Bill, as Reported | 22 |

I. BACKGROUND AND PURPOSE OF THE PREVENTING REAL ONLINE
THREATS TO ECONOMIC CREATIVITY AND THEFT OF INTELLECTUAL
PROPERTY ACT OF 2011

A. BACKGROUND

Intellectual property is the engine of the American economy and critical for job growth. According to independent studies, IP-reliant companies account in America for more than \$7.7 trillion and em-

ploy more than 19 million workers.¹ Protecting American intellectual property from theft is therefore critical to our Nation's prosperity, welfare, and job creation.²

The theft of American intellectual property threatens that prosperity.³ While estimates of the harm caused to the American economy by counterfeit products and the theft of copyrighted works differ and are difficult to confirm, copyright piracy and the sale of counterfeit goods is reported to cost American creators and producers billions of dollars per year.⁴ Intellectual property theft also reportedly results in hundreds of thousands of lost jobs annually, and severely reduces the income of those who are employed.⁵ Sim-

¹Nam D. Pham, "Employment and Gross Output of Intellectual Property Companies in the United States," NDP Consulting Research Paper, January 2011, at 2, available at http://www.theglobalipcenter.com/sites/default/files/reports/documents/employment_gross_output_of_ip_companies_in_the_us_-_jan_2011_low_res.pdf; see also *Oversight of the Office of the Intellectual Property Enforcement Coordinator Before the U.S. Senate Committee on the Judiciary*, S. Hrg. 111th Cong. 2 (2010) (written statement of David Hirschmann, President and CEO, Global Intellectual Property Center, U.S. Chamber of Commerce) at 4; *Targeting Websites Dedicated To Stealing American Intellectual Property Before the U.S. Senate Committee on the Judiciary*, S. Hrg. 112th Cong. 1 (2011) (written statement of Tom Adams, CEO, Rosetta Stone Inc.) at 1 ("Intellectual property industries are a cornerstone of the U.S. economy, employing more than 19 million people and accounting for 60 percent of our exports"); *Oversight of the Office of the Intellectual Property Enforcement Coordinator Before the U.S. Senate Committee on the Judiciary*, S. Hrg. 111th Cong. 2 (2010) (written statement of Paul E. Almeida, President, Department for Professional Employees, AFL-CIO) at 2, 4.

²"Strong intellectual property enforcement saves American jobs, it creates American jobs, it protects American ideas and it invigorates our economy." *Oversight of the Office of the Intellectual Property Enforcement Coordinator Before the U.S. Senate Committee on the Judiciary*, S. Hrg. 111th Cong. 2 (2010) (written statement of Victoria Espinel, Intellectual Property Enforcement Coordinator, Office of Management and Budget) at 2.

³"The revenue lost to American businesses from intellectual property theft carries with it lost funding for public services to compound the harm caused to our economy." *Id.* at 2.

⁴See *Targeting Websites Dedicated To Stealing American Intellectual Property Before the U.S. Senate Committee on the Judiciary*, S. Hrg. 112th Cong. 1 (2011) (written statement of Tom Adams, CEO, Rosetta Stone Inc.) at 2 ("The global sales of counterfeit goods via the Internet from illegitimate retailers reached \$135 billion in 2010. As a consequence of global and U.S.-based piracy of copyright products, the U.S. economy lost \$58.0 billion in total output in 2007"); Press Release, FBI, The Federal Bureau of Investigation and the U.S. Customs Service today announced the National Intellectual Property Rights Coordination Center's first conference for members of Congress and the industry in Washington (July 16, 2002), available at <http://www.fbi.gov/news/pressrel/press-releases/the-federal-bureau-of-investigation-and-the-u.s.-customs-service-today-announced-the-national-intellectual-property-rights-coordination-centers-first-conference-for-members-of-congress-and-industry-in-washington> ("Losses to counterfeiting are estimated at \$200-250 billion a year in U.S. business losses"); Press Release, U.S. Customs and Border Protection section of the Department of Homeland Security, U.S. Customs Announces International Counterfeit Case Involving Caterpillar Heavy Equipment (May 29, 2002) available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/52002/05292002.xml ("Customs estimates that businesses and industries lose about \$200 billion a year in revenue . . . due to the counterfeiting of merchandise"); Stephen E. Siwek, "The True Cost of Copyright Industry Piracy to the U.S. Economy," Institute for Policy Innovation, IPI Policy Report No. 189, October 3, 2007, at 1, available at [http://www.ipi.org/ipi/IPIPublications.nsf/PublicationLookupFullTextPDF/02DA0B4B44F2AE9286257369005ACB57/\\$File/CopyrightPiracy.pdf?OpenElement](http://www.ipi.org/ipi/IPIPublications.nsf/PublicationLookupFullTextPDF/02DA0B4B44F2AE9286257369005ACB57/$File/CopyrightPiracy.pdf?OpenElement) ("[E]ach year, copyright piracy from motion pictures, sound recordings, business and entertainment software and video games costs the U.S. economy \$58 billion in total output, cost American workers 375,375 jobs and \$16.3 billion in earnings, and costs Federal, State, and local governments \$2.6 billion in tax revenue"); MEMA Brand Protection Council, "Stop Counterfeiting Automotive and Truck Parts," available at www.mema.org/cmspages/getAttach.php?id=50. For a view that online infringement is a significant problem, but estimates of harm are difficult to quantify, see United States Government Accountability Office Report to Congressional Committees on "Intellectual Property, Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods" (2010) (hereinafter referred to as "Report on Economic Effects of Counterfeit and Pirated Goods"), at 18-19.

⁵See Press Release, U.S. Customs and Border Protection section of the Department of Homeland Security, U.S. Customs Announces International Counterfeit Case Involving Caterpillar Heavy Equipment (May 29, 2002) available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/52002/05292002.xml ("Customs estimates that businesses and industries lose . . . 750,000 jobs due to the counterfeiting of merchandise"); *Oversight of the Office of the Intellectual Property Enforcement Coordinator Before the U.S. Senate Committee on the Judiciary*, S. Hrg. 111th Cong. 2 (2010) (written statement of Paul E. Almeida, President, Department for Professional Employees, AFL-CIO) at 4 ("The losses of income arise because entertainment professionals depend on compensation at two points: first when professionals do the work, and later when others use and reuse the intellectual property that the professionals created. . . . For AFTRA recording artists in 2008, 90 percent of income derived from sound record-

ply put, this form of infringement impacts companies of all types and sizes and the people who work there.⁶

The growth and success of the Internet as a medium for commerce has given businesses the opportunity to connect with consumers throughout the world in ways they never could before. Unfortunately, along with the success of legitimate commerce, the distribution and sale of counterfeit products and pirated content online has also increased dramatically. According to the Director of Immigration and Customs Enforcement, “nearly 100 million people shopped [online] on Cyber Monday last year,” yet “[c]ounterfeiters are prowling the back alleys of the Internet, masquerading, duping, and stealing: masquerading as legitimate retailers, duping shoppers, stealing from real businesses and their workers.”⁷

Copyright infringement in particular, in the form of peer-to-peer networks, cyber lockers, streaming sites, and one-click hosting services, has grown rampant on the Internet. Since digital products are not tangible, they can be reproduced at very low cost, and have the potential for immediate delivery through the Internet across virtually unlimited geographic markets. The GAO reports that “sectors facing threats from digital piracy include the music, motion picture, television, publishing, and software industries,”⁸ but piracy impacts virtually any online industry that relies on copyright protection.

Similarly, the sale of counterfeit goods via Internet sites that appear professional and can quickly deliver items in sophisticated packaging is thriving on the Internet. In many cases, these Internet sites are able to conceal the inauthentic nature and low quality of the product being purchased. The footwear, clothing, consumer electronics and pharmaceutical industries, among others, are frequent victims of counterfeiting.⁹ Preventing counterfeit sales is therefore not only important to our economy and job creation, but it protects unsuspecting consumers from inferior and often dangerous products.

The online theft of American intellectual property is a growing criminal enterprise both because of the ease by which it can be done online and the ability of the sellers and distributors to remain anonymous, operate from overseas, and avoid traditional methods for protection.¹⁰ Operators of rogue Internet sites, which do nothing but traffic in infringing goods, can act with impunity from abroad.¹¹

The rogue Internet sites that operate as virtual stores for the infringing products are well designed and give the appearance of le-

ings was directly linked to royalties from physical CD sales and paid digital downloads. SAG members working under the feature film and TV contract that same year derived 43 percent of their total compensation from residuals. Residuals derived from sales to secondary markets funded 65 percent of the IATSE [Motion Picture Industry] Health Plan and 36 percent of the SAG Health and Pension Plan”).

⁶ See “Report on Economic Effects of Counterfeit and Pirated Goods,” at 9–10.

⁷ John Morton, Director of Immigration and Customs Enforcement, U.S. Department of Homeland Security Prepared Remarks: Operation In Our Sites v. 2.0—Cyber Monday (November 29, 2010) available at <http://www.ice.gov/doclib/news/library/speeches/112910morton.pdf>.

⁸ See “Report on Economic Effects of Counterfeit and Pirated Goods,” at 8.

⁹ *Id.* at 7.

¹⁰ *Id.* at 8–9.

¹¹ The Council of Europe Convention on Cybercrime, to which the United States is a signatory, requires signatories to have in place criminal copyright laws that apply to copyright infringement on the Internet. See Convention on Cybercrime, November 23, 2001, TIAS 13174, available at <http://www.state.gov/documents/organization/131807.pdf>. This Act provides an additional mechanism in the fight against online infringement occurring overseas.

gitimacy.¹² They are easily accessible by entering domain names that sound legitimate into the users' Internet browser or typing common search terms into Internet search engines; they often accept payment through well respected credit card companies; and they often run advertisements from trusted companies. All of this presents an appearance of legitimacy to the virtual store, even though the products being sold are illegal, and in the case of counterfeits are often inferior or even dangerous. And, in many cases, American consumers may unwittingly be giving their credit card information to overseas organized crime syndicates when visiting rogue Internet sites.¹³

If these rogue Internet sites operated in the physical world, rather than online, the perpetrator would be the subject of civil lawsuits and criminal penalties.¹⁴ But because this theft is veiled by the complexities of the online world and many of the perpetrators are located overseas, the task of enforcing U.S. intellectual property laws on the Internet is a difficult one. Too often our Government, as well as the businesses and consumers who are harmed by online infringement, are forced to sit idly by while this theft continues undeterred.¹⁵

The Committee notes that protecting intellectual property in the form of copyrighted material is not only important to our economy and jobs, but is also important for advancing the goals of the First Amendment. The United States Supreme Court has long held that copyright protection advances the goals of the First Amendment by "supply[ing] the economic incentive to create and disseminate

¹²For an example of the unfortunate ease with which operators of rogue Internet sites can clone legitimate Internet sites to trick consumers, see <http://www.bbc.co.uk/news/business-11372689>. The National Electrical Manufacturers Association has exposed similar examples. See, e.g., <http://blog.nema.org/blogs/currents/archive/2008/04/06/a-letter-from-the-counterfeit-wars.aspx> (counterfeit hair irons).

¹³Eric Holder, Attorney General of the United States, remarks at the Rio De Janeiro Prosecutor General's Office (February 14, 2010) ("Unfortunately, the success of this worldwide, digital marketplace has also attracted criminals who seek to exploit and misappropriate the intellectual property of others. The same technologies that have created unprecedented opportunities for growth in legitimate economies have also created global criminal organizations that are eager to steal the creativity and profits from our domestic industries and workers. . . . These groups, who do not respect international boundaries or borders, have developed sophisticated, efficient and diverse methods for committing almost every type of intellectual property offense imaginable, including: widespread online piracy of music, movies, video games, business software and other copyrighted works; well-funded corporate espionage; sales of counterfeit luxury goods, clothing and electronics, both on street corners and through Internet auction sites; and increased international trade in counterfeit pharmaceuticals and other goods that pose a substantial risk to the health and safety of our consumers"); see also *Protecting Intellectual Property Rights In A Global Economy: Current Trends and Future Challenges Before the Subcommittee on Gov't Management, Organization, and Procurement of the H. Committee on Oversight and Gov't Reform*, 111th Cong. 1 (2009) (written statement of Jason M. Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice) at 5 ("Because intellectual property crime is perceived as a low-risk criminal enterprise with the potential for high profit margins, it is not surprising that the sale of counterfeit and pirated goods is also becoming an attractive revenue source for traditional organized crime groups"); General James L. Jones, National Security Advisor to the President of the United States, Remarks at the Sochi Security Council Gathering, Sochi Russia (October 5, 2010) available at <http://www.whitehouse.gov/the-press-office/2010/10/05/remarks-gen-james-l-jones-national-security-advisor-sochi-security-counc> (Criminal syndicates "generate[] trillions of dollars annually from illicit activities such as money laundering, trafficking, counterfeiting, environmental crime, and financial fraud. . . . many of these criminal syndicates operate globally; they are comprised of loose networks that cooperate intermittently but maintain their independence; and they employ sophisticated technology and financial savvy").

¹⁴See, e.g., 17 U.S.C. § 506; 18 U.S.C. § 2319; 18 U.S.C. § 2320.

¹⁵In her recent hearing before the Senate Committee on the Judiciary, Victoria Espinel, U.S. Intellectual Property Enforcement Coordinator, stated that "legislative action may be required in order to fulfill our goals" of effective intellectual property protection. *Oversight of the Office of the Intellectual Property Enforcement Coordinator Before the U.S. Senate Committee on the Judiciary*, 111th Cong. 2 (2010) (written statement of Victoria Espinel, Intellectual Property Enforcement Coordinator, Office of Management and Budget).

ideas.”¹⁶ The “clause [of the Constitution] empowering Congress to grant patents and copyrights is [based] in the conviction that encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors in ‘Science and useful Arts.’”¹⁷

Further, Justice O’Connor wrote that copyright law is the very “engine of free expression.”¹⁸ It exists not to prevent free speech, but to promote it. Justice O’Connor went on to recall that “freedom of thought and expression ‘includes both the right to speak freely and the right to refrain from speaking at all.’”¹⁹ As rogue Internet sites evade U.S. intellectual property laws, they not only cause economic harm, but they trample on these First Amendment values.²⁰

In sum, the theft of intellectual property by rogue Internet sites is harmful in several ways. First, online infringement harms the content and trademark owners themselves in the form of lost sales, lost brand value, increased costs to protect their intellectual property, and decreased incentives to invest in research and development. Second, online infringement harms consumers who receive lower quality products, inauthentic products, or, in a worst case scenario, products that cause physical harm or health risks. Third, online infringement harms Federal and State Governments in the form of lost tax revenues, higher law enforcement costs, and the harm caused by the effects of the Government’s own purchase of counterfeit products. Fourth, online infringement harms U.S. trade by lessening its ability to partner with countries that have weaker intellectual property enforcement regimes.²¹ Fifth, online infringement reduces the incentives to create and disseminate ideas which, as the United States Supreme Court has recognized, harms the free expression principles of the First Amendment. Finally, as Victoria Espinel, U.S. Intellectual Property Enforcement Coordinator (IPEC), noted in a hearing before the Senate Committee on the Judiciary, online infringement supports international organized crime syndicates, which pose risks to our national security.²²

¹⁶See *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 558 (1985); *Sony Corp. of Amer. v. Universal City Studios, Inc.*, 464 U.S. 417 (“[T]he limited grant is a means by which an important public purpose may be achieved. It is intended to motivate the creativity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired”); *Herbert v. Shanley Co.*, 242 U.S. 591, 595 (1917) (“If music did not pay, it would be given up. If it pays, it pays out of the public’s pocket. Whether it pays or not, the purpose of employing it is profit, and that is enough”).

¹⁷See *Mazer v. Stein*, 347 U.S. 201, 219 (1954).

¹⁸See *Harper & Row Publishers, Inc.*, 471 U.S. at 558.

¹⁹See *id.* at 559 (quoting *Wooley v. Maynard*, 430 U.S. 705 (1977) (Burger, C.J.)). Additionally, in a recent letter to members of the U.S. Senate Committee on the Judiciary, First Amendment practitioner Floyd Abrams wrote: “Copyright violations are not protected by the First Amendment. Entities ‘dedicated to infringing activities’ are not engaged in speech that any civilized, let alone freedom-oriented nation protects. That these infringing activities occur on the Internet makes them not less, but more harmful.” Letter from Floyd Abrams, Senior Partner, Cahill, Gordon, and Reindel LLP, to Senator Patrick Leahy, Chairman of the Senate Judiciary Committee, Senator Chuck Grassley, Ranking Member of the Senate Judiciary Committee, Senator Orrin Hatch, United States Senate (May 24, 2011) (on file with the U.S. Senate Committee on the Judiciary’s Majority staff.)

²⁰This right to be compensated for their work is not simply a creation of U.S. law. Our Constitution provides for this in the Copyright Clause, U.S. CONST. ART. I §8, and the United Nations’ Universal Declaration of Human Rights, which has become a model for treaties and constitutions around the world, proclaimed this “right of authors” as inalienable. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc A/810 at Art. 27 ¶2 (December 10, 1948).

²¹*Id.* at 9–10.

²²*Oversight of the Office of the Intellectual Property Enforcement Coordinator Before the U.S. Senate Committee on the Judiciary*, S. Hrg. 111th Cong. 2 (2010) (written statement of Victoria

B. PURPOSE OF THE LEGISLATION

Today, law enforcement officials and rights holders have limited effective remedies available to fight the purveyors of infringing goods on the Internet when they operate overseas and in hiding.²³ Federal legislation is needed to provide a tailored mechanism for combating rogue Internet sites.

The Committee bill, as reported, gives the Department of Justice and rights holders an expedited process for cracking down on rogue Internet sites by targeting the domain names associated with those sites through injunctive relief. By making it more difficult for a domain name to be used for illicit purposes, and limiting the profitability of the underlying Internet site, the legislation will allow law enforcement to disrupt the criminal enterprises using domain names—and American infrastructure—to steal American intellectual property and profit off American consumers. The legislation will deter criminals from building up the success and visibility of rogue websites, because by doing so they will more likely become the target of law enforcement. The Committee bill, as reported, also addressed concerns raised by various parties since similar legislation was introduced in the 111th Congress, but the Committee understands that there remain outstanding concerns.

1. Department of Justice actions

The Committee bill, as reported, authorizes the Justice Department to file a civil action against the registrant or owner of a foreign registered domain name that accesses an Internet site that is “dedicated to infringing activities,” or the foreign-registered domain name itself, and to seek a cease and desist order from the court. The Justice Department should bring the action against the owner or registrant of any foreign-registered domain name where practicable. However, in cases in which the Department is unable to find the owner or registrant, or that person has no address within the United States, the bill authorizes the Department to bring an *in rem* action against the non-domestic domain name itself. This process is modeled on the Anticybersquatting Consumer Protection Act.²⁴

A domain name is the alphanumeric designation conventionally used to access a specific Internet address. The domain name typically comprises at least a top level domain and a second level domain. For instance, in the domain name senate.gov, “.gov” is the top level domain; “senate” is the second level domain. By typing

Espinell, Intellectual Property Enforcement Coordinator, Office of Management and Budget) at 2. See also *supra*, n. 13.

²³The Department of Justice, in conjunction with Immigration and Customs Enforcement, has recently used its forfeiture authority to seize domestic domain names that were being used for criminal activity. See <http://www.ice.gov/news/releases/1105/110525washingtondc.htm>; see also *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II Before the H. Committee on the Judiciary*, H. Hrg. 112th Cong. 1 (2011) (written statement of John Morton, Director, U.S. Immigration and Customs Enforcement, Department of Homeland Security) at 9–11. This authority cannot be used to combat foreign-based websites accessed by foreign-registered domain names.

²⁴The Anticybersquatting Consumer Protection Act (“ACPA”), 15 USC § 1125(d), authorizes a trademark owner to file an *in rem* action against a domain name. See *Caesars World, Inc. v. Caesars-Palace.com*, 112 F.Supp.2d 502, 504 (E.D. Va. 2000) (“There is no prohibition on a legislative body making something property. Even if a domain name is no more than data, Congress can make data property and assign its place of registration as its situs”) (emphasis added). See also *Heathmount A.E. Corp. v. Technodome.com*, 2000 WL 33666935, at *3–4 (E.D. Va. 2000) (unpublished). Further, the Federal Government’s recent domain name seizures, discussed *supra* at n.23, recognizes domain names as property.

“senate.gov” in a web browser, the Internet user’s domain name server will find the Internet address associated with the domain name senate.gov. Each top level domain is operated by a domain name registry which, through registrars, allows registrants to register domain names.²⁵

The Committee bill, as reported, authorizes the Justice Department to seek relief from a Federal district court in the form of a temporary restraining order, a preliminary injunction, or an injunction, in accordance with rule 65 of the Federal Rules of Civil Procedure. For an order to issue against the owner, registrant, or domain name itself, the Justice Department must demonstrate to the court that the Internet site accessed by the domain name is “dedicated to infringing activities.” In addition, the Internet site must be used within the United States, conduct business directed to residents of the United States, and harm holders of United States intellectual property rights.²⁶

If the court issues an order against the domain name or its registrant, owner, or operator, the legislation authorizes law enforcement officers to serve the court order on specified third parties, including operators of nonauthoritative domain name system servers (“DNS operators”),²⁷ search engines, payment processors, and online advertising network providers.²⁸ These parties monetize the Internet site by enabling U.S. consumers to access the infringing website, to purchase content and products off the website, and to view advertisements on the website. Without partnering with these entities, the financial incentive to run an infringing Internet site is greatly diminished. The bill requires these third parties to take appropriate action to, respectively, prevent a domain name from resolving to its Internet protocol address,²⁹ prevent a search result from linking to an Internet site, prevent payment processing for purchases on the underlying Internet site, or prevent its network from providing advertisements to the underlying Internet site.

The Committee bill, as reported, affords due process to both defendants and third parties compelled to action by the legislation. The Justice Department must send notice of the alleged violation and intent to proceed under the legislation to the registrant of the domain name that is the subject of the action. Additionally, the Justice Department must provide notice to any third party that

²⁵The legislation defines a domain name by cross-referencing section 45 of the Lanham Act. Pursuant to that definition, a domain name is the combination of the top level domain and the second level domain, which is what domain name registries and registrars assign, and does not include third level domains of files or subfiles.

²⁶These factors are derived from the World Intellectual Property Organization recommendations for determining whether the “use of a sign on the Internet has a commercial effect in a Member State.” See *Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights In Signs On The Internet*, adopted by the Assembly of the Paris Union for the Protection of Industrial Property and the General Assembly of the World Intellectual Property Organization, October 3, 2001, available at http://www.wipo.int/about-ip/en/development_iplaw/pub845-04.htm#P134_6837.

²⁷Most Internet service providers operate a DNS server that they offer to their subscribers, but subscribers can use DNS services that are not affiliated with their Internet service provider. The Committee bill applies to all DNS operators.

²⁸The Act includes a requirement that a plaintiff serve this order on “similarly situated” third parties. This provision is intended to avoid any competitive disparity that could result from selectively imposing burdens on some entities within a given class, but not others.

²⁹The actions required of an operator of a domain name system server is limited by the Act to those designed to prevent the domain name from resolving. The Act defines a domain name by reference to the Lanham Act, see *supra* note 25, and therefore orders issued pursuant to this Act would not require such operators to block particular subdomains or subdirectories.

might be required to take action as the result of a resulting court order.

The Committee bill, as reported, includes safeguards to allow the domain name or Internet site owner, operator, registrant, registry or registrar to petition the court to modify, suspend or vacate the order where the Internet site operator takes effective steps to exclude infringing or counterfeiting activity from the site, or where the interests of justice require. The bill also authorizes any third party receiving an order to petition the court. Similarly, as Internet site operators subject to the order transition their Internet sites to new domain names, the bill authorizes a plaintiff to bring a related action against the additional domain name in the same judicial district.

2. *Qualifying plaintiff actions*

The Committee bill, as reported, similarly authorizes a “qualifying plaintiff,” defined as either the Attorney General or a rights holder, to file an action for civil injunctive relief against the registrant or owner of any domain name that accesses an Internet site that is “dedicated to infringing activities”—or the domain name itself—and to seek a cease and desist order from the court. That action can be brought regardless of whether the domain name at issue is registered in the United States or abroad. Such an action is subject to the same due process and notice requirements described in Part I.B.1.

The mechanism is identical to that reserved for the Justice Department in non-domestic actions; however the resulting remedies are more limited. A qualifying plaintiff may only seek the court’s permission to serve a court order resulting from an action brought under this provision on a payment processor or online advertising network. Neither a DNS operator nor a search engine can be required to take action as the result of an order issued under this provision.

3. *Internet site “Dedicated to Infringing Activities”*

The definition of an Internet site “dedicated to infringing activities” in the legislation is narrowly tailored to implicate only the most egregious rogue websites that are trafficking in infringing goods. For an Internet site to fall within the definition, the legislation requires a party bringing an action, whether against a domestic or non-domestic domain name, to make one of two showings. The plaintiff can show that the Internet site has no significant use other than engaging in, enabling, or facilitating the (1) reproduction, distribution, or public performance of copyrighted works in violation of title 17, (2) violation of section 1201 of title 17, or (3) sale, distribution, or promotion of counterfeits under the Lanham Act. Alternatively, the plaintiff can show that the Internet site is designed, operated, or marketed primarily as a means for engaging in, enabling, or facilitating the (1) reproduction, distribution, or public performance of copyrighted works in violation of title 17, (2) violation of section 1201 of title 17, or (3) sale, distribution, or promotion of counterfeits under the Lanham Act.³⁰

³⁰The Combating Online Infringement and Counterfeits Act (“COICA”), S.3804, introduced and reported by the Committee on the Judiciary in the 111th Congress, used a far broader definition of an Internet site dedicated to infringing activities. COICA’s definition included sites

Importantly, in targeting only the “worst of the worst” Internet sites, the definition maintains the protection of fair use. The Committee intends for the legislation to target only those Internet sites clearly profiting from stolen American intellectual property, and not to be used where there is fair use or where there is an objectively reasonable interpretation of an express license to use intellectual property.

4. *Protections for third parties*

The Committee bill, as reported, contains protections for those third parties required to take action under the Act, to ensure that any party acting pursuant to an order is held harmless for having taken the appropriate action. This immunity extends to any acts reasonably designed to comply with an order or reasonably arising from an order. Additionally, no third party is required to take action to comply with an order beyond what is technically feasible and reasonable. It is also not the Committee’s intent that compliance with an order issued under this legislation create an ongoing duty on the part of a third party to affirmatively monitor its systems to ensure that it does not allow access to an Internet site or transact with an underlying merchant that is the subject of an order, where the site or merchant has reconstituted under an alias.

The Committee bill, as reported, also encourages voluntary action by payment processors and online advertising network providers, by providing a safe harbor if these third parties voluntarily take action authorized by the legislation relating to an Internet site that it reasonably believes is dedicated to infringing activities.³¹ Further, the bill encourages voluntary action by domain name registries, registrars, search engines, financial transaction providers, and online advertising network providers against Internet sites that endanger the public health, either where the site is “dedicated to infringing activities” relating to controlled or non-controlled prescription medicines, or has no significant use other than, or is used primarily as a means for, the distribution of prescription medicines without a valid prescription, or the distribution of misbranded or adulterated medicines.

The Committee bill, as reported, authorizes the plaintiff to bring an action to compel compliance from any third party required to take action under this section that knowingly and willfully fails to comply with a court order. The Committee anticipates that these actions will be used only in those situations where a third party does not fulfill its legal obligation under the Act. These provisions do not open the door to fishing expeditions in the form of frivolous litigation brought simply to initiate broad discovery. A third party

that satisfy the criteria for forfeiture under section 2323 of title 18. The Committee heard concerns that this definition had the potential to include Internet sites with a significant amount of protected speech. The Committee responded to those concerns in the Committee bill by crafting a narrower definition, although the Committee recognizes that it means there will be rogue Internet sites whose operators may be violating criminal law that are nonetheless beyond the scope of this legislation. The Committee also recognizes that even with the new, narrower definition, there may still be some minimal amount of lawful content accessed through the domain name. The Supreme Court has upheld similar ancillary restraints for content neutral regulations. *See Arcara v. Cloud Books, Inc.*, 478 U.S. 697 (1986).

³¹This safe harbor should not be construed to imply that there is liability for other entities that undertake voluntary action to combat online infringement and counterfeiting, or for payment processors or online advertising networks undertaking other actions against rogue websites, outside of those prescribed in this section.

would not be monetarily liable for any action or inaction under this Act.

5. Impact of the legislation

The Committee understands that when access to an Internet site is blocked by a DNS operator or a search engine, the Internet site is still accessible to a user who takes certain affirmative steps. For example, where the Internet site is blocked by the DNS operator, a user can access the Internet site by changing the Domain Name Server to which the Internet service provider communicates to an alternative Domain Name Server. In the Committee's view, however, a substantial portion of users are not intending to commit or facilitate an intellectual property-related crime. Rather, many consumers are being lured to the illegal Internet sites as discussed above. These consumers will be protected as a result of the remedies outlined in the Act and will, instead, visit Internet sites offering legitimate content or products.

Similarly, the Committee understands that when a payment processor or advertising network suspends a particular merchant account in compliance with the Act, that website may in fact find a way to process payments through another alias. The Act requires payment processors and advertising networks to make reasonable efforts to stop payment transactions from merchants associated with the Internet site at issue, and the Committee believes that this will substantially diminish the financial viability of that site.

The Committee does not intend the Act to deter voluntary action otherwise taken by third parties against rogue websites, nor does the Committee intend the Act to serve as a substitute for such voluntary action. Voluntary, cooperative action taken by private parties to prevent infringement and the sale of counterfeits over the Internet can be an effective approach to combat online infringement.

6. Savings clauses

The Committee bill, as reported, may not be construed to limit or expand the civil or criminal remedies available under any other Federal or State laws for infringing activities on the Internet. The legislation does not enlarge or diminish vicarious or contributory liability for any cause of action under the Lanham Act or title 17, including any limitation on liability under section 512 of title 17. Finally, nothing in this legislation shall serve as a basis for determining the application of section 512 of title 17 to any party.

7. Guidelines and reports

The Committee bill, as reported, requires the Attorney General to publish certain procedures for implementation of this Act. The bill also requires the Attorney General to develop a deconfliction process with other law enforcement agencies, including U.S. Immigration and Customs Enforcement, for implementation of this Act.

The Committee bill, as reported, also requires the Secretary of Commerce, the Register of Copyrights, the Attorney General, and the Comptroller General to issue reports. The Secretary of Commerce is required to report to the Committees on the Judiciary in both the Senate and House on the ability to deploy Domain Name Security Extensions. The Register of Copyrights is required to re-

port to the Committees on the Judiciary in both the Senate and House on the effectiveness and burden of carrying out this legislation. The Attorney General is required to report to the Committees on the Judiciary in both the Senate and House on actions brought under this legislation. The Comptroller General is required to report to the Committees on the Judiciary in both the Senate and House on actions brought by a rights holder under this legislation.

8. Importation of counterfeit products and infringing devices

The Committee bill, as reported, provides that Customs and Border Protection (“CBP”) may identify and prevent counterfeit products from being imported into the United States by clarifying that, notwithstanding the Trade Secrets Act, the Secretary of Homeland Security is authorized to share samples or photos of suspected counterfeit products and their packaging or labels with the relevant rights holders to determine whether the shipment should be seized at the border. Similarly, it ensures that the Secretary of Homeland Security can share information and samples relating to anti-circumvention devices that have been seized with affected parties. These provisions are intended as clarifying in nature and do not imply that anything in the Trade Secrets Act currently prohibits the sharing of such information and should not limit or affect what specific information CBP may be required to or prevented from disclosing through subsequent legislation or rulemaking.

II. HISTORY OF THE BILL AND COMMITTEE CONSIDERATION

A. INTRODUCTION OF THE BILL

On September 20, 2010, in the 111th Congress, Chairman Leahy introduced the Combating Online Infringement and Counterfeits Act, S. 3804, along with Senator Hatch. Senator Bayh, Senator Durbin, Senator Feinstein, Senator Klobuchar, Senator Kohl, Senator Schumer, Senator Voinovich, and Senator Whitehouse, were original cosponsors of the bill. Senator Alexander, Senator Cardin, Senator Coburn, Senator Gillibrand, Senator Graham, Senator Grassley, Senator Inhofe, Senator McCaskill, and Senator Menendez later joined as cosponsors. This bill was referred to the Senate Committee on the Judiciary.

The bill was on the agenda for the September 23, 2010 business meeting, but was held over. On November 18, 2010, the Committee on the Judiciary considered S. 3804. Chairman Leahy offered a substitute amendment, which was adopted by unanimous consent. That was the only amendment considered during this debate. Senator Coburn submitted a statement for the record that indicated certain Internet service providers, search engines, Federal agencies in charge of intellectual property enforcement, and other interested parties had outstanding concerns over some provisions in the legislation, and noted the need for further discussion of those issues in the form of a hearing prior to the final passage of the legislation. The Committee then voted to report the Combating Online Infringement and Counterfeits Act, with an amendment in the nature of a substitute, favorably to the Senate by a roll call vote of 19–0.

On May 12, 2011, Chairman Leahy introduced the Preventing Real Online Threats to Economic Creativity and Theft of Intellec-

tual Property Act, S. 968, along with Senator Hatch and Senator Grassley. Senator Blumenthal, Senator Coons, Senator Feinstein, Senator Franken, Senator Graham, Senator Klobuchar, Senator Kohl, Senator Schumer, and Senator Whitehouse were original cosponsors. Senator Alexander, Senator Ayotte, Senator Blunt, Senator Boozman, Senator Cochran, Senator Corker, Senator Durbin, Senator Gillibrand, Senator Hagan, Senator Lieberman, Senator Rubio, Senator Shaheen, and Senator Tom Udall joined as cosponsors. The bill was referred to the Senate Committee on the Judiciary.

B. HEARINGS

On June 23, 2010, in the 111th Congress, the Senate Committee on the Judiciary held a hearing on “Oversight of the Office of the Intellectual Property Enforcement Coordinator.” This hearing was attended by Chairman Leahy, Senator Coburn, Senator Franken, Senator Grassley, Senator Hatch, Senator Klobuchar, and Senator Whitehouse. Testifying on Panel I was the Honorable Victoria A. Espinel, Intellectual Property Enforcement Coordinator, Office of Management and Budget. Testifying on Panel II were Barry M. Meyer, Chairman and CEO, Warner Bros. Entertainment Inc.; Paul E. Almeida, President, Department for Professional Employees, AFL–CIO; David Hirschmann, President and CEO, Global Intellectual Property Center, U.S. Chamber of Commerce; and Caroline Bienstock, President and CEO, Carlin America. The following materials were submitted for the record: Letter from the Copyright Alliance to Chairman Leahy dated June 23, 2010, with attachments; statement of James M. Yates; prepared statement of Victoria A. Espinel; prepared statement of Barry M. Meyer; prepared statement of Paul E. Almeida; prepared statement of David Hirschmann; and prepared statement of Caroline Bienstock.

On February 16, 2011, in the 112th Congress, the Senate Committee on the Judiciary held a hearing on “Targeting Websites Dedicated to Stealing American Intellectual Property.” This hearing was attended by Chairman Leahy, Senator Grassley, Senator Blumenthal, Senator Coburn, Senator Coons, Senator Franken, Senator Klobuchar, Senator Kyl, and Senator Whitehouse. Testifying at this hearing were Tom Adams, President and CEO of Rosetta Stone, Inc.; Scott Turow, President of the Authors Guild; Christine N. Jones, Executive Vice President, General Counsel, and Corporate Secretary of the Go Daddy Group, Inc.; Thomas M. Dailey, Vice President and Deputy General Counsel for Verizon; and Denise Yee, Senior Trademark Counsel for Visa, Inc.³² The following materials were submitted for the record: Letter from William Samuel, Director of Government Affairs for the AFL–CIO, dated February 15, 2011; letter from AT&T to Victoria Espinel, U.S. Intellectual Property Enforcement Coordinator, dated March 24, 2010; letter from Brian Keane, CEO of Blue Sky, to Senator Blumenthal, dated February 15, 2011; statement of the Computer and Communications Industry Association; statement of the Consumer Electronics Association; statement of the Center for Democracy and Technology; letter from Floyd Abrams to Chairman Leahy, Senator Grassley, and Senator Hatch, dated February 11,

³² Google Inc. was asked by the Committee to testify as a hearing witness, but declined.

2011; letter from Sascha Meinrath, Aparna Sridhar, M. Chris Riley, Open Technology Initiative, New America Foundation, and Free Press Action Fund to Chairman Leahy, dated February 15, 2011; statement of Daniel Castro, Senior Analyst, Information Technology and Innovation Foundation; statement of the Motion Picture Association of America, Inc.; statement of the NetCoalition, with attachments; Op-Ed by Scott Turow, Paul Aiken, and James Shapiro from the February 14, 2011 edition of the New York Times; statement of Public Knowledge; letter from Nora Roberts to Chairman Leahy and Members of the Senate Judiciary Committee, dated February 13, 2011; letter from multiple companies and associations to Members of the United States Congress, dated February 15, 2011; statement of the United States Chamber of Commerce; prepared statement of Tom Adams; prepared statement of Scott Turow; prepared statement of Christine N. Jones; prepared statement of Thomas M. Dailey; and prepared statement of Denise Yee.

On June 22, 2011, in the 112th Congress, the Senate Committee on the Judiciary held a hearing on “Oversight of Intellectual Property Law Enforcement Efforts.” This hearing was attended by Chairman Leahy, Senator Grassley, Senator Blumenthal, Senator Coburn, Senator Coons, Senator Franken, Senator Klobuchar, Senator Kohl, and Senator Whitehouse. Testifying at this hearing were Victoria Espinel, United States Intellectual Property Enforcement Coordinator; Jason Weinstein, Deputy Assistant Attorney General for the Criminal Division, United States Department of Justice; Gordon M. Snow, Assistant Director for the Cyber Division, Federal Bureau of Investigation; Allen Gina, Assistant Commissioner, Office of International Trade, United States Customs and Border Protection; and Erik Barnett, Assistant Deputy Director, United States Immigration and Customs Enforcement. The following materials were submitted for the record: Letter from the American Federation of Musicians, the American Federation of Television and Radio Artists, the Directors Guild of America, the International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists, and Allied Crafts of the United States, Its Territories, and Canada, the International Brotherhood of Teamsters, and the Screen Actors Guild, dated June 20, 2011, to Chairman Leahy and Senator Grassley; letter from Paul Williams, President and Chairman of the Board of the American Society of Composers, Authors, and Publishers, dated June 20, 2011, to Chairman Leahy and Senator Grassley; letter from Tom Giovanetti, President of the Institute for Policy Innovation, dated June 20, 2011, to Chairman Leahy and Senator Grassley; letter from Mitch Bainwol, Chairman and CEO of the Recording Industry Association of America, Inc., dated June 21, 2011, to Chairman Leahy; letter from the Motion Picture Association of America, Inc., and member studios, dated June 22, 2011, to Chairman Leahy and Senator Grassley; statement of Colleen M. Kelley, National President of the National Treasury Employees Union; statement of the United States Chamber of Commerce; prepared statement of Victoria Espinel; prepared statement of Jason Weinstein; prepared statement of Gordon M. Snow; prepared statement of Allen Gina; and prepared statement of Erik Barnett.

C. LEGISLATIVE HISTORY

The bill was on the agenda for the May 19, 2011 business meeting, but it was held over. On May 26, 2011, the Committee on the Judiciary considered S. 968. Chairman Leahy offered a substitute amendment, which was adopted by unanimous consent. Chairman Leahy and Senator Grassley offered an additional amendment to clarify that when Customs and Border Protection suspects a product that is being imported or exported of being counterfeit, it is not prohibited by the Trade Secrets Act to share samples of packaging or labels of suspected counterfeits with the purported rights owner. This amendment was adopted by voice vote. No other amendments were considered during this debate.

The Committee then voted to report S. 968, with amendments, favorably to the Senate. The Committee reported this bill by voice vote.

The following companies or groups submitted letters in support of S. 968: United States Chamber of Commerce; AFL–CIO; Business Software Alliance; National Cable and Telecommunications Association; National Association of Broadcasters; National Association of Manufacturers; Comcast/NBC Universal; Copyright Alliance; American Federation of Musicians; American Federation of Television and Radio Artists; Directors Guild of America; International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, Its Territories, and Canada; Screen Actors Guild; International Brotherhood of Teamsters; National Music Publishers' Association; Institute for Policy Innovation; Software and Information Industry Association; Writers Guild of America, West; Viacom; Independent Film & Television Alliance; Motion Picture Association of America; National Association of Theatre Owners; Paramount Pictures Corporation; Association for Safe Online Pharmacies; Small Business & Entrepreneurship Council; Songwriters Guild of America; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLC; Walt Disney Studios Motion Pictures; Warner Bros. Entertainment Inc.; Deluxe Entertainment Services Group; 1–800 Contacts, Inc.; 1–800–PetMeds; ABRO Industries, Inc.; Acushnet Company; Adidas America; Advanced Medical Technology Association (AdvaMed); Alliance of Automobile Manufacturers; Alliance of Visual Artists (AVA); American Association of Independent Music (A2IM); American Board of Internal Medicine; American Made Alliance; American Society of Composers, Authors and Publishers (ASCAP); American Society of Media Photographers; Anti-Counterfeiting and Piracy Initiative (ACAPI); Arts+Labs; Association of American Publishers (AAP); Association of Equipment Manufacturers; Association of Independent Music Publishers (AIMP); Association of Text Publishers; Autodesk, Inc.; Automotive Aftermarket Industry Association; Beachbody, LLC; Beam Global Spirits & Wine; Blue Sky Studios, Inc.; Bose Corporation; Brigid Collins Family Support Center; Broadcast Music, Inc. (BMI); Burberry; Cascade Designs Incorporated; CBS Corporation; Cengage Learning; CFA Institute; Chanel USA; Church Music Publishers Association; Coalition Against Counterfeiting and Piracy (CACP); The Collegiate Licensing Company/IMG College; Commercial Photographers International; Copyright Clear-

ance Center (CCC); Coty Inc.; Country Music Association; Dayco Products, LLC; Deckers Outdoor Corporation; Dolce & Gabbana; Dollar General Corporation; Electronic Components Industry Association (ECIA); Eli Lilly and Company; Entertainment Software Association (ESA); ERAI, Inc.; The Estee Lauder Companies; Evidence Photographers International Council; Ex Officio; Exxel Outdoors; Far Bank Enterprises; Fashion Business Incorporated; Federation of State Boards of Physical Therapy; Ford Motor Company; Fortune Brands, Inc.; Gemvision Corporation; Gospel Music Association; Governors America Corp.; Graduate Management Admission Council; Greeting Card Association (GCA); Guru Denim; HarperCollins Publishers; Harry Fox Agency; Hastings Entertainment, Inc.; ICM Distributing Company, Inc.; IDS Publishing; IEC Electronics Corp.; Imaging Supplies Coalition (ISC); Independent Distributors of Electronics Association (IDEA); Innate-gear; Intellectual Property Owners Association; International AntiCounterfeiting Coalition (IACC); International Trademark Association (INTA); John Wiley & Sons, Inc.; Johnson & Johnson; Kekepana International Services; Leatherman Tool Group, Inc.; Lexmark International, Inc.; L'Oréal USA; LVMH Moët Hennessy Louis Vuitton; Macmillan; Major League Baseball; Marmot; The McGraw-Hill Companies; Merck & Co., Inc.; Messy Face Designs, Inc.; MicroRam Electronics, Inc.; Microsoft; Monster Cable Products, Inc.; Music Managers Forum-U.S.; Nashville Songwriters Association International; National Association of Recording Merchandisers (NARM); National Basketball Association (NBA); The National Collegiate Athletic Association (NCAA); National Electrical Manufacturers Association (NEMA); National Football League (NFL); Nervous Tattoo Inc., dba Ed Hardy; Netflix; New Era Cap Co Inc.; News Corporation; Nike, Inc.; Nintendo of America Inc.; Oakley, Inc.; OpSec Security, Inc.; Outdoor Industry Association; Outdoor Power Equipment Institute (OPEI); Outdoor Research, Inc.; Pacific Component Xchange, Inc.; Perry Ellis International; Personal Care Products Council; Petzl America; Pfizer Inc.; Picture Archive Council of America (PACA); PING; Premier League; Production Music Association (PMA); Professional Photographers of America; Quality Float Works, Inc.; The Recording Academy (National Academy of Recording Arts and Sciences); Recording Industry Association of America (RIAA); Reebok International Ltd.; Reed Elsevier Inc.; Revlon; Romance Writers of America (RWA); Rosetta Stone Inc.; Schneider Electric; SESAC, Inc.; SG Industries, Inc.; SMT Corp.; Society of Sport & Event Photographers; Sony Music Entertainment; SoundExchange; Specialty Equipment Market Association (SEMA); Sports Rights Owners Coalition; Spyder Active Sports, Inc; Stock Artist Alliance; Stuart Weitzman Holdings, LLC; Student Photographic Society; SunRise Solar Inc.; Taylor Made Golf Company, Inc.; Tednologies, Inc.; Tiffany & Co.; The Timberland Company; Time Warner Inc.; Toshiba America Business Solutions, Inc.; Ultimate Fighting Championship; Underwriters Laboratories Inc.; Universal Music Group; Uniweld Products Inc.; Vibram USA, Inc; W.R. Case & Sons Cutlery Co.; Wal-Mart; The Walt Disney Company; Warner Music Group; Winestem Company; Xerox Corporation; Zippo Manufacturing Company.

III. SECTION-BY-SECTION SUMMARY OF THE BILL

Section 1. Short title

This section provides that the legislation may be cited as the “Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act”.

Section 2. Definitions

This section provides definitions referenced in the Act, including the definition of an “Internet site dedicated to infringing activities.” Under this definition, provided in paragraph (7), an “Internet site dedicated to infringing activities” means an Internet site that falls into one of two categories. The first category is an Internet site that has no other significant use other than engaging in, enabling, or facilitating the infringement of substantially complete copyrighted material (paragraph (7)(A)(i)); the circumvention of copyright protection systems (paragraph (7)(A)(ii)); or the sale of goods, services or materials bearing a counterfeit mark (paragraph (7)(A)(iii)). The second category is an Internet site that is designed, operated, or marketed by its operator, primarily as a means for engaging in, enabling or facilitating the infringement of substantially complete copyrighted material; the circumvention of copyright protection systems; or the sale of goods, services or materials bearing a counterfeit mark.

Section 3. Enhancing enforcement against rogue websites operated and registered overseas

Subsection (a). This subsection authorizes the Attorney General to commence either an in personam action against a registrant or owner of a nondomestic domain name dedicated to infringing activities (subsection (a)(1)), or an in rem action against a nondomestic domain name dedicated to infringement (subsection (a)(2)). An in rem action is only authorized where, after due diligence, the defendant owner or registrant cannot be found. The Attorney General is required to identify any third parties that may be required to take action under subsection (d) (subsection (a)(3)).

Subsection (b)(1). This subsection provides the court with the authority to issue a temporary restraining order, a preliminary injunction or an injunction, in accordance with rule 65 of the Federal Rules of Civil Procedure, against an infringing nondomestic domain name, registrant, or owner or operator of such a site. The injunction directs the site to cease and desist from further infringing activity, provided that the domain name is being used within the United States to access an infringing site, conducts business directed at residents of the United States, and harms intellectual property rights holders in the United States.

Subsection (b)(2). This subsection provides factors the court may consider, among other indicia, to determine if a site is conducting business directed at residents of the United States. These factors include whether a site is providing infringing goods or services to users in the United States (subsection (b)(2)(A)); whether there is evidence that the site is not intended to provide such goods to users in the United States, or access or delivery of such goods to users in the United States (subsection (b)(2)(B)); whether the site has reasonable measures in place to prevent such goods and serv-

ices from being accessed from or delivered to the United States (subsection (b)(2)(C)); whether the site offers services obtained in the United States (subsection (b)(2)(D)); and whether the site offers goods and services for sale in U.S. Dollars (subsection (b)(2)(E)).

Subsection (c). This subsection directs the Attorney General to send notice of an alleged violation and intent to proceed under the Act to the registrant of the domain name of the Internet site. This notice can be sent to the best available postal or email address, or in any other form the court finds necessary, including in the manner provided to serve individuals in foreign countries under Rule 4(f) of the Federal Rules of Civil Procedure. The Attorney General is also required to notify any third parties that may be required to take action under subsection (d).

Subsection (d)(1). This subsection requires Federal law enforcement to serve a copy of a court order issued pursuant to this section on any third party which has been identified either in the complaint or any amendments thereto.

Subsection (d)(2). This subsection details the reasonable measures that identified third parties must take after being served with an order. There are four classes of third parties described in this subsection: Operators of nonauthoritative domain name system servers (subsection (d)(2)(A)), financial transaction providers (subsection (d)(2)(B)), Internet advertising services (subsection (d)(2)(C)), and information location tools (subsection (d)(2)(D)). Operators of nonauthoritative domain name system servers shall take the least burdensome technically feasible and reasonable measures to prevent the domain name described in the order from resolving. Safeguards prevent the operator from having to modify its network, software, systems, or facilities in order to comply with this subsection. Financial transaction providers must take reasonable measures to prevent, prohibit or suspend their service from completing payment transactions associated with the site involving U.S. customers. Internet advertising services must take technically feasible and reasonable measures to prevent their service from providing advertisements to the infringing site, and cease making available any advertisements for that site, or any paid or sponsored links that provide access to the site. Information location tools must take technically feasible and reasonable measures to remove or disable access to the infringing site and not serve a hypertext link to such a site.

Subsection (d)(3). This subsection gives third parties discretion to determine if and how they will communicate actions taken under this subsection to their users.

Subsection (d)(4). This subsection is a rule of construction that ensures that the obligations of a third party relating to an action commenced under this section are limited to those described in the section.

Subsection (d)(5). This subsection provides immunity to third parties for actions taken to reasonably comply with an order issued under this subsection (subsection (d)(5)(A)). In addition, actions taken by customers or users of a third party to circumvent any good faith effort to restrict access to an infringing site pursuant to this subsection shall not incur liability for that third party (subsection (d)(5)(B)).

Subsection (e). This subsection authorizes the Attorney General to bring an action for injunctive relief against any party that receives an order under this section and willfully fails to comply with the order. This is the sole legal remedy to enforce the obligations under this section for any third party described in it. A defendant in this action may establish an affirmative defense by showing that it does not have the technical means to comply with the subsection without incurring unreasonable economic burden, or that the order is inconsistent with the Act.

Subsection (f). This subsection provides the manner in which an order under subsection (b) can be modified, suspended, or vacated. After the issuance of such an order, a motion to modify, suspend, or vacate the order may be filed at any time by: Any person, owner or operator of property bound by the order (subsection (f)(1)(A)); any registrant of the domain name or the owner or operator of the site subject to the order (subsection (f)(1)(B)); any domain name registrar or registry that has registered or assigned the domain name of the site (subsection (f)(1)(C)); or any third party required to take action under subsection (d) (subsection (f)(1)(D)). Relief can be granted if the court finds that the site associated with the domain name is no longer or never was dedicated to infringing activities, or the interests of justice require that the order be modified, suspended or vacated (subsection (f)(2)). The court can also consider whether the domain name has expired or been registered to a different party (subsection (f)(3)). Additionally, third parties can intervene at any time in an action commenced under subsection (a), or in any action to suspend, modify, or vacate an order (subsection (f)(4)).

Subsection (g). This subsection authorizes the Attorney General, if alleging that the underlying Internet site at issue was previously determined to be an “Internet site dedicated to infringing activities” in a prior action, to commence a related action against the domain name owner, registrant or site itself, in the same judicial district as the previous action.

Section 4. Eliminating the financial incentive to steal intellectual property online

Subsection (a). This subsection authorizes a qualifying plaintiff, which is defined as the Attorney General or a U.S. intellectual property rights holder, to commence either an in personam action against a registrant, owner, or operator of a domain name used by a site dedicated to infringing activities (subsection (a)(1)), or an in rem action against a domain name used by a site dedicated to infringing activities, if after due diligence such persons cannot be found (subsection (a)(2)). The qualifying plaintiff is required to name any third parties that may be required to take action under subsection (d) (subsection (a)(3)).

Subsection (b)(1). This subsection provides the court with the authority to issue a temporary restraining order, a preliminary injunction or an injunction, in accordance with rule 65 of the Federal Rules of Civil Procedure, against an infringing domain name, registrant, or owner or operator of such a site. The injunction directs the site to cease and desist from further infringing activity, provided that the domain name is registered or assigned by a domain name registry located or doing business in the U.S., the domain

name is used within the U.S. to access such an infringing site, and the site conducts business related to the residents of the U.S. and harms U.S. intellectual property rights holders.

Subsection (b)(2). This subsection provides factors the court may consider, among other indicia, to determine if a site is conducting business directed at residents of the U.S. These factors include whether a site is providing infringing goods or services to users in the U.S. (subsection (b)(2)(A)); whether there is evidence that the site is not intended to provide such goods to users in the U.S., or access or delivery of such goods to users in the U.S. (subsection (b)(2)(B)); whether the site has reasonable measures in place to prevent such goods and services from being accessed from or delivered to the U.S. (subsection (b)(2)(C)); whether the site offers services obtained in the U.S. (subsection (b)(2)(D)); and whether the site offers goods and services for sale in U.S. Dollars (subsection (b)(2)(E)).

Subsection (c). This subsection directs the qualifying plaintiff to send notice of an alleged violation and intent to proceed under the Act to the registrant of the domain name of the Internet site. This notice can be sent to the best available postal or email address, or in any other form the court finds necessary, including in the manner provided to serve individuals in foreign countries under Rule 4(f) of the Federal Rules of Civil Procedure. The qualifying plaintiff is also required to notify any third parties that may be required to take action under subsection (d).

Subsection (d)(1). This subsection requires a qualifying plaintiff to serve a copy of a court order issued pursuant to this section on any third party which has been identified either in the complaint or any amendments thereto.

Subsection (d)(2). This subsection details the reasonable measures that identified third parties must take after being served with an order. There are two classes of third parties described in this subsection: Financial transaction providers (subsection (d)(2)(A)) and Internet advertising services (subsection (d)(2)(B)). Financial transaction providers must take reasonable measures to prevent, prohibit or suspend their service from completing payment transactions associated with the site involving U.S. customers. Internet advertising services must take technically feasible and reasonable measures to prevent their service from providing advertisements to the infringing site, and cease making available any advertisements for that site, or any paid or sponsored links that provide access to the site.

Subsection (d)(3). This subsection gives third parties discretion to determine if and how they will communicate actions taken under this subsection to their users.

Subsection (d)(4). This subsection is a rule of construction that ensures that the obligations of a third party relating to an action commenced under this section are limited to those described in the section.

Subsection (d)(5). This subsection provides immunity to third parties for actions taken to reasonably comply with an order issued under this subsection (subsection (d)(5)(A)). In addition, actions taken by customers or users of a third party to circumvent any good faith effort to restrict access to an infringing site pursuant to

this subsection shall not incur liability for that third party (subsection (d)(5)(B)).

Subsection (e). This subsection authorizes the Attorney General to bring an action for injunctive relief against any party that receives an order under this section and willfully fails to comply with the order. This is the sole legal remedy to enforce the obligations under this section for any third party described in it. A defendant in this action may establish an affirmative defense by showing that it does not have the technical means to comply with the subsection without incurring unreasonable economic burden, or that the order is inconsistent with the Act.

Subsection (f). This subsection provides the manner in which an order under subsection (b) can be modified, suspended, or vacated. After the issuance of such an order, a motion to modify, suspend, or vacate the order may be filed at any time by: Any person, owner or operator of property bound by the order (subsection (f)(1)(A)); any registrant of the domain name or the owner or operator of the site subject to the order (subsection (f)(1)(B)); any domain name registrar or registry that has registered or assigned the domain name of the site (subsection (f)(1)(C)); or any third party required to take action under subsection (d) (subsection (f)(1)(D)). Relief can be granted if the court finds that the site associated with the domain name is no longer or never was dedicated to infringing activities, or the interests of justice require that the order be modified, suspended or vacated (subsection (f)(2)). The court can also consider whether the domain name has expired or been registered to a different party (subsection (f)(3)). Additionally, third parties can intervene at any time in any action commenced under subsection (a), or in any action to suspend, modify, or vacate an order (subsection (f)(4)).

Subsection (g). This subsection authorizes the qualifying plaintiff, if alleging that the underlying Internet site at issue was previously determined to be an “Internet site dedicated to infringing activities” in a prior action, to commence a related action against the domain name owner, registrant or site itself, in the same judicial district as the previous action.

Section 5. Voluntary actions against websites stealing American intellectual property

This section provides a safe harbor from liability to financial transaction providers and Internet advertising services that voluntarily take actions described under sections 3(d) or 4(d) with regard to an Internet site if those entities act in good faith and based on credible evidence that the site is dedicated to infringing activities (subsection (a)). This section also protects domain name registries, registrars, financial transaction providers, information location tools, or Internet advertisers from liability if they voluntarily stop providing or refuse to provide service to sites that endanger the public health by selling counterfeit, misbranded, or adulterated pharmaceuticals, or regularly sell pharmaceuticals without a valid prescription, so long as the third party’s action is taken in good faith and based on credible evidence (subsection (b)).

Section 6. Savings clauses

These savings clauses ensure that nothing in the Act will be construed to limit or expand civil or criminal remedies available to any person for infringing activities on the Internet pursuant to other Federal or State laws (subsection (a)); enlarge or diminish liability for any cause of action under either the Lanham Act or the Copyright Act, nor create an obligation to take action pursuant to section 5 of the Act (subsection (b)); or serve as a basis to determine the application of section 512 of the Copyright Act, providing limitations on liability relating to material online (subsection (c)).

Section 7. Guidelines and studies

Subsection (a). This subsection requires the Attorney General, in consultation with other relevant law enforcement agencies, to publish procedures to receive information from the public about Internet sites dedicated to infringing activities, and to develop a deconfliction process with relevant law enforcement agencies to coordinate the enforcement activities brought under the Act.

Subsection (b). This subsection requires a series of reports designed to review the effectiveness of the Act and related oversight. The Secretary of Commerce, the Register of Copyrights, the Attorney General, and the Government Accountability Office are required to produce reports under this subsection.

Section 8. Preventing the importation of counterfeit products and infringing devices

This section clarifies that when Customs and Border Protection suspects a product that is being imported or exported of being counterfeit, the Secretary of Homeland Security is not prohibited by the Trade Secrets Act from sharing samples of packaging or labels of suspected counterfeits with the purported rights owner. Similarly, it ensures that the Secretary of Homeland Security can share information and samples relating to anti-circumvention devices that have been seized with affected parties.

IV. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not available for inclusion in this report. The estimate will be printed in either a supplemental report or the Congressional Record when it is available.

V. REGULATORY IMPACT EVALUATION

In compliance with rule XXVI of the Standing Rules of the Senate, the Committee finds that no significant regulatory impact will result from the enactment of S. 968.

VI. CONCLUSION

The Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act will provide the Justice Department and rights holders with an important new mechanism for combating online copyright infringement and the sale of counterfeit goods.

VII. CHANGES TO EXISTING LAW MADE BY THE BILL, AS REPORTED

Pursuant to paragraph 12 of Rule XXVI of the Standing Rules of the Senate, the Committee finds no changes in existing law made by S. 968, as ordered reported.

