DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 21
Issue 2 *Spring 2011*

Article 5

# The Bill of Unintended Consequences: The Combating Online Infringement and Counterfeit Act

Ashley S. Pawlisz

# THE BILL OF UNINTENDED CONSEQUENCES: THE COMBATING ONLINE INFRINGEMENT AND COUNTERFEIT ACT

## I. INTRODUCTION

The problem is a real one: on a regular basis, a vast number of goods protected by intellectual property rights are bought and sold illegally around the world.[1] The U.S. Chamber of Commerce estimated that more than $5 trillion of the United States' gross domestic product is accounted for by intellectual property.[2] Additionally, these industries employ tens of millions of people whose jobs are affected by intellectual property piracy.[3] Estimates show that each year, online theft of motion pictures, music, software and video games alone "costs the U.S. economy $58.0 billion in total output, costs American workers 373,375 jobs and $16.3 billion in earnings, and costs federal, state and local governments $2.6 billion in tax revenue."[4] These numbers do not include counterfeit goods that are bought and sold online and do not take into account the ripple effect such losses have on upstream and downstream suppliers.[5] Encouraging creativity by granting creative people enforceable intellectual property rights is

1. Remarks by Thomas J. Donohue, President and CEO, U.S. Chamber of Commerce, *Protecting Intellectual Property in the 21st Century - A Vital Mission*, Fourth Annual Anti-Counterfeiting and Piracy Summit, Oct. 2, 2007, http://www.uschamber.com/press/speeches/2007/protecting-intellectual-property-21st-century-vital-mission-remarks-thomas-j-don.

2. 156 CONG. REC. S7207 (daily ed. Sept. 20, 2010) (statement by Sen. Leahy).

3. *Id.*

4. Stephen E. Siwek, Institute for Policy Innovation, *The True Cost of Copyright Industry Piracy to the U.S. Economy*, Policy Report 189 (Oct. 2007), at 1, *available at* http://www.ipi.org/IPI/IPIPublications.nsf/PublicationLookupFullTextPDF/02DA0B4B44F2AE9286257369005ACB57/$File/Copyright Piracy.pdf.

5. *Id.*

an essential part of a society and economy.[6] However, there must be a limit to the costs incurred to protect intellectual property. This Article discusses Senate Bill 3804: The Combating Online Infringement and Counterfeit Act (COICA).[7] COICA works toward the admirable goal of encouraging thriving businesses and promoting jobs in the midst of a struggling economy by aggressively fighting online piracy.[8] However, COICA's broad grant of power to the Department of Justice to block websites in the name of preventing piracy is concerning. While the goal of the bill is to prevent copyright infringement, non-infringing content could also be greatly affected by the mechanisms this bill employs, and the potential for abuse is cause for concern.

The purpose of this Article is to separate the goal from the potential unintended consequences of COICA in order to evaluate its efficacy in practice. Section II of this Article sets out background information necessary to an understanding of the debate surrounding the proposed Bill. Part A of Section II details the technical foundation of COICA in order to help elucidate its practical goals and how they will play out in application. Part B details the United States' historical approach to Internet regulation. Part C explores current liability for online infringement under the Digital Millennium Copyright Act.

Section III focuses on explaining COICA itself. Part A of Section III addresses the opening remarks by Senator Patrick Leahy to identify the intended goal of the Act. Part B breaks down the various statutory provisions of the Act. Part C addresses arguments by proponents of the Bill, and Part D addresses arguments by opponents of the Bill.

Section IV analyzes the consequences of COICA if implemented. This section specifically addresses: COICA's threat to free speech and expression, including Constitutional concerns

---

6. *See id*; *see also* James V. DeLong, *Protecting Property on the Internet*, THE AMERICAN, Dec. 9, 2010 http://www.american.com/archive/2010/december/get-the-governments-hands-on-this-junk, *infra* note 141.

7. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. (2010).

8. 156 CONG. REC. S7208 (daily ed. Sept. 20, 2010) (statement by Sen. Leahy).

raised by COICA and the United States' role in international censorship activities (all addressed in Part A); potential conflicts between COICA and prior legislation, making its practical applicability somewhat ambiguous (addressed in Part B); and technical problems, which suggest that the goals of COICA may not be attainable through the provisions as they are currently written (found in Part C).

## II. BACKGROUND

### *A. How The Domain Name System (DNS) Works*

In order to understand how the Department of Justice would effectuate the provisions of COICA and the various arguments on both sides of the debate, one must first understand how the Domain Name System works. The Domain Name System (DNS) is a set of rules and procedures that are used to identify resources online, according to Internet Protocols.[9] The DNS as structured today has three functions: (1) providing for the top-level domains; (2) providing for a registrar for users to register new domain names; and (3) resolving a URL address requested by users into its registered location.[10] The DNS allows Internet applications to have uniquely named web addresses that will not change based on physical location.[11] This result is possible because the DNS resolves a URL web address into its current Internet location, which can change without changing the URL web address.[12] This separation of name and location occurs because DNS servers translate the URL text of a web address into readable addresses

9. Kevin Werbach, *Castle in the Air: A Domain Name System for Spectrum*, 104 NW. U. L. REV. 613, 622 (2010).

10. *Id.* at 622-23.

11. *Id.* at 623-24.

12. Sara D. Sunderland, *Domain Name Speculation: Are We Playing Whac-A-Mole*, 25 BERKELEY TECH. L.J. 465, 467-68 (2010) (stating that "resolving" simply means the process by which the domain names are matched to an IP address within DNS servers); *see also* Daniel Karrenberg, The Internet Domain Name System Explained for Non-Experts, March, 2004, http://www.isoc.org/briefings/016/briefing16.pdf.

based on Internet Protocol ("IP addresses").[13] IP addresses indicate what the user seeks and where it is located so that they can be routed to the correct Internet site.[14] A domain name also identifies the person or entity holding the authority for a particular domain or sub-domain.[15] Within a web address, dots separate different top-level domains and second-level domains.[16] For example, in the address "pawlisz.com," "pawlisz" is a second-level domain and <.com> is the top-level. In practice, this means that when a user tries to access an Internet application with a unique address (for example, by typing in the address www.pawlisz.com), the user's computer must ask a DNS server where the user should be sent.[17] The DNS server tells the user's computer the appropriate numeric address in order to make a connection sufficient to send packets of information between the user and content providing computers.[18] In short, DNS servers translate the unique name into the appropriate address under Internet Protocols. Given the incredible amount of traffic on the Internet, it is not practical or feasible for all of this information to be centralized; otherwise all Internet traffic would have to be routed through a single point.[19]

The Internet Assigned Number's Authority (IANA) manages IP address allocation around the globe, in conjunction with the Internet Corporation for Assigned Names and Numbers (ICANN).[20] Blocks of IP addresses are allocated by IANA to regional Internet registries, which each deal with different areas of

13. *Id.*

14. Sunderland, *supra* note 12, at 466-67; *see also* Karrenberg, *supra* note 12.

15. Sunderland, *supra* note 12, at 467.

16. Werbach, *supra* note 9, at 622; *see also* Karrenberg, *supra* note12.

17. *Id.*

18. Sunderland, *supra* note 12, at 467-68; *see also* Karrenberg, *supra* note 12.

19. *See* Kevin Werbach, *The Centripital Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart*, 42 U.C. DAVIS L. REV. 343, 348 (2008).

20. Peter K. Yu, *The Origins of CCTLD Policymaking*, 12 CARDOZO J. INT'L & COMP. L. 387, 397-98 (2004) (the Internet Corporation for Assigned Names and Numbers (ICANN) now oversees a number of Internet-related tasks including IANA).

the world.[21] Additionally, IANA gives data to "root domain name servers" that publish a website's "root zone file," as received from the IANA, to the Internet.[22] DNS root servers know the addresses for the authoritative servers of Top Level Domains (TLDs) such as <.com,> <.org,> <.gov,> <.es,> etc.[23] This is the first step in the DNS database.[24] These DNS root servers are operated by thirteen different organizations.[25] Actual root name servers are located in 240 locations within more than 60 countries worldwide.[26]

A user's computer normally first queries a DNS "caching server," which is a server that retains DNS translations from previous transactions on that server.[27] The user's Internet Service Provider (ISP) or other relevant network operators may operate these caching servers.[28] Additionally, a hierarchy of caching servers can be used within a network to speed up query responses for a large number of users.[29] The benefit of caching servers is that they help to diffuse the burden on root DNS servers and speed up Internet access by using cached information.[30]

If a user's local caching server does not have the information to resolve the user's query, it will have to find the "authoritative"

---

21. *Id.* at 389-90.

22. Karrenberg, *supra* note 12.

23. 1 Paul D. McGrady, *McGrady on Domain Names* § 1.08(3) (2010).; *see also* Karrenberg *supra* note 12; Root Zone Database, http://www.iana.org/domains/root/db/ (for a current list of top-level domain delegations).

24. Karrenberg, *supra* note 12.

25. *See* Root Server Technical Operations Assn., http://www.root-servers.org (last visited Dec. 20, 2010) (for a current list of root name servers and locations). These organizations include Verisign, Inc., Information Services Institute, Cogent Communications, the University of Maryland, NASA Ames Research Center, Internet Systems Consortium, Inc., U.S. Department of Defense Network Information Center, U.S. Army Research Lab, Autonomica, RIPE NCC, ICANN, and WIDE Project.

26. *Id. See also* 1 Paul D. McGrady, *McGrady on Domain Names* § 1.14(2)(a) (2010).

27. Karrenberg, *supra* note 12; *see also* Microsoft TechNet, *How DNS query works: Domain Name System (DNS)*, http://technet.microsoft.com/en-us/library/cc775637(WS.10).aspx (last visited Dec. 20, 2010).

28. *Id.*

29. *Id.*

30. *Id.*

server for the domain name requested by the user.[31] The caching server could search its cache for the authoritative server covering everything with ".pawlisz.com" in the address, regardless of what comes before the first dot.[32] The domain name system generally has a lot of redundancy in that there are many servers, in different locations to provide answers at each step.[33] However, if the caching server does not have any information stored to resolve the address or find the authoritative server, the DNS root servers always have the root information needed to start the search.[34] The addresses of DNS root servers are pre-configured in all caching servers, with a mechanism for updating addresses if there are any changes.[35]

In short, DNS servers have the very basic but essential job of translating unique web address to the usable numerical format required of Internet protocols in order to direct a user to the correct place. The Domain Name System functions as a decentralized network of servers, which span the globe and utilize a significant amount of redundancy to make the Internet work more efficiently and effectively.[36]

### *B. Regulation of Access to Internet Content*

#### *1. Private Regulation*

The consumer market contains a wide range of software products that can be used to limit, filter or block access to content on Internet sites.[37] Individuals, corporations, and even governments use products such as web filters, censorware, or

31. *Id.*

32. *Id.*

33. Karrenberg, *supra* note 12; *see also* Microsoft TechNet, *How DNS query works: Domain Name System (DNS)*, http://technet.microsoft.com/en-us/library/cc775637(WS.10).aspx (last visited Dec. 20, 2010).

34. *Id.*

35. *Id.*

36. *Id.*

37. *See* OpenNet Initiative, *About Filtering*, http://opennet.net/about-filtering (last visited Dec. 20, 2010).

firewalls to censor what information certain groups can access.[38] Most consumer products of this nature are used to limit malicious code or other harmful content supplied by hackers.[39] A large majority of corporations employ these types of software in order to protect company assets, limit liability, and increase productivity by limiting which sites can be visited on employer computers.[40] For example, many companies block access to pornographic websites or social networking sites for these reasons. Firewalls are frequently used to protect individual computers or entire networks for security reasons, however, most of these limitations rarely raise concerns by users because they are relatively harmless and are supported by legitimate purposes.[41]

Additionally, corporations that provide access to the Internet have a significant role in what content is accessible on the Internet. These ISPs are allowed to implement bandwidth usage charges on content providers, meaning that sites that pay additional fees will load faster.[42] Many opponents of this practice argue for "net neutrality," which requires all content providers to have a level playing ground.[43] In *Comcast Corp. v. FCC*, the Court of Appeals

38. *See* OpenNet Initiative, *About Filtering*, *supra* note 37; *see e.g.,* Barracuda Web Filter, http://www.barracudanetworks.com/ns/products/web-filter-overview.php (last visited Dec. 20, 2010) (software to filter content accessible on a computer); Websense.com, Web Security, Email Security, Data Security, http://www.websense.com/content/home.aspx (last visited Dec. 20, 2010) (provider of web, email and data security solutions).

39. *See, e.g.,* Barracuda Web Filter, *supra* note 38; Websense.com, Web Security, Email Security, Data Security, http://www.websense.com/content/WebSecurityOverview.aspx (last visited Dec. 20, 2010) ("Websense® Web Security Gateway solutions provide employee productivity, malware protection, and data loss prevention (DLP)").

40. *See, e.g.,* Websense.com, *supra* note 38 ("Web Security solutions provide dynamic Web malware protection and employee productivity with industry-leading Web filtering").

41. *See e.g.,* Websense.com, *supra* note 38 ("Websense® Web Security Gateway solutions provide employee productivity, malware protection, and data loss prevention (DLP)").

42. Benjamin Rupert, *The 110th Congress and Network Neutrality: S. 215 - The Internet Freedom Preservation Act*, 18 DEPAUL J. ART, TECH. & INTELL. PROP. L. 325, 330 (2008).

43. *Id.* at 325.

for the District of Columbia Circuit curbed the Federal Communication Commission's authority to regulate how ISPs manage their networks.[44] The implications are that certain content providers could be given preferential access to the Internet, which could potentially lead to a form of private Internet censorship.[45] Regardless, the debate over net neutrality is still ongoing, given the conflict between allowing private companies to self-regulate their business practices and allowing the government to oversee and regulate access to the Internet in the name of non-discrimination.[46]

*2. The United States' Approach*

While a great number of countries around the globe implement some form of Internet filtering to some degree, the United States has historically maintained efforts to limit censorship and content blocking by governments.[47] In a recent speech, Secretary of State Hilary Clinton remarked that "[t]hose who disrupt the free flow of information in our society or any others pose a threat to our economy, our government, and our civil society."[48] Going further, she cautioned against allowing "a new information curtain,"[49] and noted that:

> On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single Internet where all of humanity has equal access to knowledge and ideas. And we recognize that the

44. Comcast Corp. v. Federal Communications Commission, 600 F.3d 642, 661 (D.C. Cir. 2010).

45. Rupert, *supra* note 42, at 332.

46. *Id.* at 338.

47. Christopher Stevenson, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*, 30 B.C. INT'L & COMP. L. REV. 531, 536-37 (2007).

48. Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010) *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm.

49. *Id.*

> world's information infrastructure will become what we and others make of it. Now, this challenge may be new, but our responsibility to help ensure the free exchange of ideas goes back to the birth of our republic. The words of the First Amendment to our Constitution are carved in 50 tons of Tennessee marble on the front of this building. And every generation of Americans has worked to protect the values etched in that stone.[50]

Congress's first significant attempt to regulate material on the Internet, and one of the earliest attempts at doing so in general,[51] came in the form of the Communications Decency Act of 1996 (CDA).[52] The Act criminalized the actions of anyone who knowingly used the Internet to display or send information, to a person under 18 years of age, containing obscene or indecent materials.[53] However, in *Reno v. American Civil Liberties Union*, the anti-indecency provisions were struck down by all nine Justices of the Supreme Court as a violation of the First Amendment freedom of speech.[54] The majority opinion written by Justice Stevens reasoned that the CDA lacked "the precisions that the First Amendment requires when a statute regulates the content of speech."[55] The opinion continued:

> In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate

50. *Id.*
51. Stevenson, *supra* note 47, at 534.
52. *Id.*
53. 47 U.S.C. § 223 (2006).
54. Reno v. ACLU, 521 U.S. 844, 874 (1997).
55. *Id.*

purpose that the statute was enacted to serve.[56]

The Child Online Protection Act (COPA) of 1998 also attempted to restrict the access of minors to harmful material on the Internet.[57] Once again, the Legislation was found to violate the First Amendment freedom of speech and parts of it were struck down by the Federal Courts in *Ashcroft v. ACLU*.[58] The Supreme Court declined to hear any appeals in the case, effectively abolishing COPA.[59] The Children's Internet Protection Act (CIPA) of 2000 conditioned the receipt of federal funds by schools and public libraries on the proper implementation and use of Internet filters to limit the exposure of minors to explicit material.[60] The Supreme Court in *United States v. American Library Association* upheld CIPA as constitutional because it only conditioned federal funds on compliance with filtering requirements, as opposed to prohibiting certain content outright.[61]

COICA exemplifies how the United State's strict limits on Internet filtering are occasionally at odds with its strong desire to enforce copyrights. Today, the United State's role in advocating for enhanced global copyright protections is somewhat ironic given the fact that in its early stages, the United States refused to grant copyright protections to foreign works.[62] Concern for the United States domestic market largely drove the development of foreign copyright protection in the United States.[63] Intellectual

---

56. *Id.*

57. 47 U.S.C. §231 (1998).

58. Ashcroft v. ACLU, 542 U.S. 656, 670 (2004).

59. PC World, *COPA Child-Porn Law Killed*, http://www.pcworld.com/article/158131/copa_childporn_law_killed.html (last visited Dec. 20, 2010).

60. Internet Free Expression Alliance, CIPA, http://ifea.net/cipa.pdf (last visited Dec. 20, 2010).

61. United States v. Am. Library Ass'n, 539 U.S. 194, 211-12 (2003).

62. Edward Choi, *With Great Power Comes Great Responsibility: Korea's Role in the War Against Online Piracy*, 10 SAN DIEGO INT'L L. J. 555, 578 (2009) (citing Julie E. Cohen et al., *Copyright in a Global Information Economy*, 33, 34 (2nd ed. 2006)).

63. *Id.*at 579 (citing James D. Thayer, *Market Based Anti-American Sentiment: A Study of Non-Resident Copyright Protection*, J. KOREAN L., Vol. 3, No. 2, 193, 198 (2003), *available at* http://www.snujkl.org/archives (follow "Journal of Korean Law Vol.3 No.2" hyperlink; then follow "Vol3No2.pdf"

property infringement cost the United States billions of dollars, particularly as the base of its economy shifted from importing to exporting goods.[64] The more goods the United States created and exported, the more essential protection of intellectual property rights became to the domestic economy. This concern over domestic markets and sense of economic self-interest is very much the driving force for the United State's aggressive approach to copyright protection today.[65] The billions of dollars lost annually by the United States due to copyright infringement has lead the United States to actively promote the enforcement of copyright protections on an international level.[66] The arguments for and against COICA reflect the conflict between the United States' desire to protect copyrights while limiting Internet filtering.

### *C. Current Online Infringement Liability under the Digital Millennium Copyright Act (DMCA)*

The Digital Millennium Copyright Act of 1998 (DMCA) was Congress' effort to adapt the United States' copyright law to the modern digital age.[67] Additionally, the United States needed to meet obligations under the World Intellectual Property Organization (WIPO) treaties, including prohibitions on the use of circumvention measures to evade technological protections.[68] The DMCA was introduced by Congressmen Rick Boucher and Tom Campbell in 1997, and adopted by Congress in 1998.[69] The

---

hyperlink)).

64. *Id.*

65. *Id.*

66. *Id.* at 579-80 (citing Zorina Khan, *IP Rights and Economic Development: A Historical Perspective*, WIPO MAG. at 11 (June 2007), *available at* http://www.wipo.int/wipo_magazine/en/2007/03/article_0006.html (stating "copyright piracy benefited the U.S. initially when the country was a net debtor. But once the balance of trade moved in its favor, America had an incentive to adopt stronger laws to protect its authors internationally"); and Lee Wilson, *Fair Use, Free Use and Use by Permission* 18-19 (2005)).

67. Executive Summary Digital Millennium Copyright Act Section 104 Report, *available at* http://www.copyright.gov/reports/studies/dmca/dmca_executive.html.

68. *Id.*

69. *Id.*

conflict in enacting the DMCA focused on balancing interests.[70] As the Senate Committee on the Judiciary Report explained, "due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."[71] At the same time, clarity of service provider liability was needed, otherwise service providers "may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet."[72] The goal of the DMCA was to limit the liability of "service providers,"[73] to ensure "that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand."[74]

*1. DMCA Safe Harbor*

The Online Copyright Infringement Liability Limitation Act (OCILLA) was passed as part of the 1998 Digital Millennium Copyright Act (DMCA).[75] This provision is often referred to as a "safe harbor" provision because it doesn't imply or impose liability.[76] Rather, the DMCA outlines when liability will not be imposed, meaning that liability needs to be premised on some other law.[77] As a threshold issue, in order to claim the DMCA's safe harbor provision, the entity in question must be a "service provider."[78] There has been little litigation construing this term, so, it is not clear whether any company hosting user-generated

70. *See id.*

71. S. Rep. No. 105-190, at 112 (1998).

72. *Id.*

73. 17 U.S.C. § 512(k)(1)(A) (2006) ("the term 'service provider' means any entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user").

74. S. Rep. No. 105-190, at 112 (1998).

75. 17 U.S.C. § 512 (2006).

76. Charles W. Hazelwood, Jr., *Fair Use and the Takedown/Put Back Provisions of the Digital Millennium Copyright Act*, 50 IDEA 307, 311 (2010).

77. 17 U.S.C. § 512 (2006).

78. *Id.* at § 512(k)(1).

content would be shielded under the DMCA.[79] Thus, unless the entity is an ISP, it cannot assume that it can seek protection under the DMCA §512 safe harbor provision. If the entity is a "service provider" for purposes of the DMCA, it will be shielded from liability if it follows certain procedural steps in responding to infringement allegations.[80] Specifically, the service provider must designate an agent to receive take-down notices[81] and, upon receiving a take-down notice, [82] must act "expeditiously to remove or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[83] The service provider must also take reasonable steps to notify the subscriber that the material has been taken down.[84] Generally, the DMCA imposes no affirmative obligation to investigate or monitor infringement activity.[85]

*2. Relevant Case Law Construing the DMCA*

In *Viacom v. YouTube*, the District Court for the Southern District of New York held that the statutory phrases of 17 U.S.C. §512(c)(1)(A)(i) and (ii) require actual or constructive knowledge of specific instances of infringement, rather than a generalized knowledge that infringing activity occurs on a site.[86] This approach generally discourages service providers from investigating what contents are on their sites. If they only have general knowledge of infringing activity, they are not required to take preventative steps in order to qualify for safe harbor under the DMCA.[87]

---

79. *See In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003).

80. Hazelwood, *supra* note 76, at 312-13.

81. 17 U.S.C. § 512(c)(2) (2006).

82. Hazelwood, *supra* note 76, at 312.

83. 17 U.S.C. § 512(d)(3) (2006).

84. *Id.* at § 512(g)(2)(A).

85. *Id.* at § 512(c)(1)(A). This section requires that a service provider have actual or constructive knowledge that the material is infringing in order to be liable for monetary or injunctive relief.

86. Viacom Int'l Inc. v. YouTube Inc., 718 F. Supp. 2d 514, 522 (S.D.N.Y. 2010).

87. *Id.*

Additionally, the courts have been hesitant to imply contributory infringement liability on service providers, except where bad faith intentions are blatantly obvious, as in the case of *MGM v. Grokster*.[88] With respect to secondary liability for infringement, the Supreme Court in *Sony Corp. v. Universal City Studios* stated:

> [There must be] a balance between a copyright holder's legitimate demand for effective - not merely symbolic - protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce. Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses. . ..[89]

In short, the DMCA requires that service providers have good intentions, designate an agent to receive notice of infringement from copyright holders,[90] make such agent available to the public,[91] and follow steps to remove the contested content.[92] Thus, the safe harbor provision immunizes service providers, but not the actual individual infringers from liability.

88. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 941 (2005).

89. Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

90. 17 U.S.C. § 512(c)(2) (2006).

91. *Id.*

92. *Id.* § 512(c)(1).

## III. PROPOSED LEGISLATION: S. 3804 - THE COMBATING ONLINE INFRINGEMENT AND COUNTERFEIT ACT

### *A. Opening Statements*

Senator Patrick Leahy introduced Senate Bill 3804 by first emphasizing the importance of intellectual property for the future of the American economy.[93] In his opening remarks, he reminded the Senate how each year, the financial losses felt by American businesses from online piracy and counterfeiting result in hundreds of thousands of lost jobs.[94] The importance of protecting intellectual property in the digital marketplace motivated the introduction of COICA, to "provide the Justice Department with an important tool to crack down on Web sites dedicated to online infringement."[95] In expressing additional support for S. 3804, Senator Orrin Hatch remarked:

> In our global economy the Internet has become the glue of international commerce-connecting consumers with a wide-array of products and services worldwide. But it has also become a tool for online thieves to sell counterfeit and pirated goods. . . . Not only do these websites facilitate massive theft of American IP, but they undermine legitimate commerce. We cannot afford to not act, especially when, by some estimates, IP accounts for a third of the market value of all U.S. stocks-approximately five trillion dollars or more. That accounts for more than 40 percent of the U.S. gross domestic product, and is greater than the entire GDP of any other nation in the world.[96]

93. 156 CONG. REC. S7207 (daily ed. Sept. 20, 2010) (statement by Rep. Leahy).

94. *Id.*

95. *Id.*

96. *Id.* at 7209 (statement by Rep. Hatch).

Senator Leahy acknowledged that enacting COICA will not eliminate the issue of online infringement, "but it will make it more difficult for foreign entities to profit off American hard work and ingenuity."[97] Senator Leahy emphasized that "[t]his bill targets the most egregious actors, and is an important first step to putting a stop to online piracy and sale of counterfeit goods."[98]

### *B. Summary of Proposed Legislation*

COICA would amend Chapter 113 of Title 18 of the United States Code to aggressively combat Internet based infringing and counterfeiting activity.[99] The bill consists of four sections: Section 1 provides the title "Combating Online Infringement and Counterfeits Act"[100]; Section 2 addresses internet sites dedicated to infringing activity[101]; Section 3 lists separate actions that are required of the Attorney General[102]; and Section 4 calls for a report on the impact of the bill within one year of enactment.[103] The bulk of the bill's operative provisions are outlined under Section 2, which focuses on providing the Department of Justice with the authority and process to take down offending websites.[104] Section 2(a) of the Bill defines when an Internet site is "dedicated to infringing activities" for purposes of the bill.[105] An Internet site satisfies this standard if it is:

> [P]rimarily designed, has no demonstrable, commercially significant purpose or use other than, or is marketed by its operator, or by a person acting

97. *Id.* at 7208 (statement by Rep. Leahy).

98. *Id.*

99. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. (2010).

100. *Id.* § 1.

101. *Id.* § 2.

102. *Id.* § 3.

103. *Id.* § 4.

104. 156 CONG. REC. S7207, 7210 (daily ed. Sept. 20, 2010) (statement by Rep. Hatch).

105. Combating Online Infringement and Counterfeit Act, S. 3804 § 2(a), 111th Cong. (2010).

> in concert with the operator, to offer . . . goods or services in violation of title 17 United States Code, or enable or facilitate a violation of title 17 United States Code, including by offering or providing access to works, without authorization . . . and when taken together, such activities are central to the activity of the Internet site or sites accessed through a specific domain name.[106]

Section 2(b) through (g) outlines the role and powers of the Attorney General in shutting down such sites.[107] The focus of the Bill is its grant of power to the Department of Justice to file an *in rem* civil action against a domain name that is "dedicated to infringing activity."[108] Under subsection (b), a court may issue injunctive relief if the Attorney General applies for it.[109] The Attorney General will be required to publish notice of all court orders issued in accordance with this bill.[110]

Section 2(e) states that for domestic domain names, the Attorney General must serve court orders issued under this section on the domain name registrar or registry.[111] Domestic domain names will be deemed to have the situs where the registrar is located or where there are "sufficient documents to establish control and authority of the registration and use of the domain name" within the United States.[112]

For non-domestic domain names, the Attorney General may serve court orders issued under this section on: (i) a relevant service provider, as defined in §512(k)(1) of Title 17 of the United states Code; (ii) a relevant financial transaction provider as defined in §5362(4) of title 31, United States Code, or; (iii) an advertising

106. *Id.*

107. *Id.* § 2(b) - (g).

108. *Id.* § 2(c) (an *in rem* action is filed against a thing rather than a person, which may include property, a right or a status).

109. *Id.* § 2(b).

110. *Id.* § 2(f).

111. Combating Online Infringement and Counterfeit Act, S. 3804 § 2(e)(1), 111th Cong. (2010).

112. *Id.* § 2(d)(1).

service that uses the accused Internet site.[113] An action may be brought in the District of Columbia against a foreign domain name only if the accused website directs business to U.S. residents and harms U.S. intellectual property right holders.[114] The bill lists four different factors that could be used to determine what it means to direct business to U.S. residents[115], which include: (i) when the Internet site provides goods or services to United States subscribers,[116] (ii) when the Internet site attempts to prevent or declares that it has no intention to provide infringing material to the United States,[117] (iii) when services on the Internet site are offered to the United States,[118] and (iv) when an Internet site lists prices in United States currency.[119]

To enforce orders under this Bill, the Attorney General may bring an action against any party that "willfully or persistently fails to comply with such order."[120] However, a showing that a party cannot technically comply with such an order is a complete defense to such action.[121] Section 2(h) provides procedures for modification or vacation of orders by the Attorney General, a defendant, or an owner or operator of a domain name subject to an order under this section.[122] This section states that the Attorney General may apply for a modification of an order to expand it to additional domain names by giving proper proof to the court.[123] A defendant or owner or operator of a domain name, or any party required to take action based on and order under this Bill, can petition the court for a modification, suspension or vacation of

113. *Id.* § 2(e)(2).
114. *Id.* § 2(d)(2).
115. *Id.* § 2(d)(2)(B).
116. *Id.* § 2(d)(2)(B)(i).
117. Combating Online Infringement and Counterfeit Act, S. 3804 § 2(d)(2)(B)(ii), 111th Cong. (2010).
118. *Id.* § 2(d)(2)(B)(iii).
119. *Id.* § 2(d)(2)(B)(iv).
120. *Id.* § 2(g).
121. *Id.*
122. *Id.* § 2(h).
123. Combating Online Infringement and Counterfeit Act, S. 3804 § 2(h)(1)(A), 111th Cong. (2010).

such order.[124] To do so, they must show that the Internet site is no longer dedicated to infringing activities, or the interests of justice require a modification.[125]

In summary, COICA attempts to curb infringing and counterfeiting activity online by enabling the Attorney General to shut down targeted websites whose domain names are registered in the United States.[126] An *in rem* action may be commenced against a domestic "domain name or names used by an Internet site in the judicial district in which the domain name registrar or domain name registry for at least 1 such domain name is located or doing business . . .."[127] For foreign-based domain names, the Attorney General may issue an order telling "service providers"[128] to take "technically feasible and reasonable steps designed to prevent a domain name from resolving to that domain name's Internet protocol address."[129] Alternatively, the Attorney General may issue an order for a "financial transaction provider"[130] to "prevent or prohibit its service from completing payment transactions between its customers located within the United States,"[131] or provide notice to the Internet site in question that its trademarks cannot be used on the site.[132] Additionally, the Attorney General may order advertising services to take reasonable measures "to prevent its network from providing advertisements to an Internet site associated with such domain name."[133] The Attorney General must inform the Intellectual Property Enforcement Coordination and other law enforcement agencies of all court orders issued to

124. *Id.* § 2(h)(1)(B).

125. *Id.*

126. *Id.* § 2(c)(1).

127. *Id.*

128. *Id.* § 2(e)(2)(B)(i) ("service provider" as that term is defined in section 512(k)(1) of title 17, United States Code, which includes any entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user).

129. Combating Online Infringement and Counterfeit Act, S. 3804 § 2(e)(2)(B)(i), 111th Cong. (2010).

130. *Id.* § 2(e)(2)(B)(ii) ("financial transaction provider" as that term is defined in section 5362(4) of title 31, United States Code).

131. *Id.* § 2(e)(2)(B)(ii)(I).

132. *Id.* § 2(e)(2)(B)(ii)(II).

133. *Id.* § 2(e)(2)(B)(iii).

specific domain names, which may publicly post such information.[134]

### *C. Proponents of COICA*

COICA was sponsored by Senator Patrick Leahy, and has gained additional support from another seventeen co-sponsors.[135] Proponents of COICA see it as a much-needed aggressive step in fighting online piracy. Mark Corallo, formerly chief spokesperson for Attorney General John Ashcroft wrote, "[t]he Internet is not at risk of being censored. But without robust protections that match technological advances making online theft easy, the creators of American products will continue to suffer."[136] He explained that "[c]ounterfeiting and online theft of intellectual property is having devastating effects on industries where millions of Americans make a living. Their futures are at risk due to Internet-based theft."[137] Illegal file sharing over the Internet has cost companies billions of dollars and many companies feel that they have limited or no practical options available to remedy the situation.[138] As an initial matter, it can be difficult and time consuming for companies to determine who is responsible for specific acts of online piracy.[139] Record companies have tried going after individuals, but suing one college student at a time to recover billions of dollars of lost intellectual property is impractical and unlikely to actually remedy the losses felt by these companies, given the high cost of litigation.[140] With respect to the free speech concerns raised by

134. *Id.* § 2(f).

135. *See Support for S. 3804, The Combating Online Infringement and Counterfeits Act: Protecting American Jobs, American Innovation, and American Consumers*, http://leahy.senate.gov/imo/media/doc/PRESS-Support-OnePager.pdf (last visited Feb. 27, 2011).

136. Mark Corallo, Daily Caller, *Conservatives should support COICA*, Nov. 18, 2010, http://dailycaller.com/2010/11/18/conservatives-should-support-coica/2/.

137. *Id.*

138. Antionette D. Bishop, *Illegal P2P File Sharing on College Campuses - What's the Solution?* 10 VAND. J. ENT. & TECH. L. 515, 517 (2008).

139. *Id.* at 519.

140. *Id.* at 517.

COICA, proponents have argued, "free speech does not include the right to shout, "Fake goods here!" in a crowded marketplace."[141] The problem of rampant online piracy is well documented, with much concern over organizations that engage in these activities and go offshore to avoid liability in the United States.[142] Concerns over the limited mechanisms for combating such activity have been the motivating force for COICA.[143] An infringing site under COICA is one that is "primarily designed, or has no demonstrable commercially significant purpose or use other than, or is marketed by its operator, or by a person acting in concert with the operator . . . to offer goods or services in violation of title 17, United States Code, or that enable or facilitate a violation of title 17, United States Code . . .."[144] When such activities, taken together, "are the central activities of the Internet site or sites accessed through a specific domain name,"[145] the Internet site is deemed "dedicated to infringing activity."[146] Proponents of the Bill argue that this is a very high standard since it essentially requires an Internet site be almost completely focused around disseminating infringing or counterfeiting material. These proponents argue that requiring that accused sites be "dedicated to infringing activities" helps to limit the number of Internet sites that could potentially be inappropriately blocked under it. Groups who have publicly supported the Bill largely include businesses that are impacted by the online infringement of goods.

### *D. Opponents of COICA*

In November, the Senate Judiciary Committee unanimously

141. James V. DeLong, The American, *Protecting Property on the Internet* (Dec. 9, 2010) (on file with author) *available at* http://www.american.com/archive/2010/december/get-the-governments-hands-on-this-junk.

142. *Id.*

143. 156 CONG. REC. S7207, 7208 (daily ed. Sept. 20, 2010) (statement by Rep. Leahy).

144. Combating Online Infringement and Counterfeit Act, S. 3804 § 2(a)(1)(B)(i), 111th Cong. (2010).

145. *Id.* § 2(a)(1)(B)(ii).

146. *Id.* § 2(a)(1).

voted to approve COICA.[147] Oregon Senator Ron Wyden has actively opposed the Bill since then, vowing to prevent it from coming to a vote on the full Senate. Senator Wyden has argued that online copyright infringement is a legitimate problem, but COICA is the wrong answer.[148] Going further, he argued that COICA is "almost like using a bunker-busting cluster bomb when what you really need is a precision-guided missile. The collateral damage of this statute could be American innovation, American jobs, and a secure Internet."[149] Forty-nine law professors stated in an open letter to Senator Leahy, that if COICA was enacted it "would fundamentally alter U.S. policy towards Internet speech, and would set a dangerous precedent with potentially serious consequences for free expression and global Internet freedom."[150] A group of Internet engineers wrote, in an open letter to the Senate Judiciary Committee, that,

> "[i]f enacted, this legislation will risk fragmenting the Internet's global domain name system (DNS), create an environment of tremendous fear and uncertainty for technological innovation, and seriously harm the credibility of the United States in its role as a steward of key Internet infrastructure. In exchange for this, the bill will introduce censorship that will simultaneously be circumvented by deliberate infringers while hampering innocent parties' ability to communicate."[151]

147. Sam Gustin, Wired, *Web Censorship Bill Sails Through Senate Committee* (Nov. 18, 2010), http://www.wired.com/epicenter/2010/11/coica-web-censorship-bill/.

148. Nate Anderson, Wired, *Senator: Web Censorship Bill a 'Bunker-Busting Cluster Bomb'* (Nov. 20, 2010), *available at* http://www.wired.com/epicenter/2010/11/senator-web-censorship-bill-a-bunker-busting-cluster-bomb/.

149. *Id.*

150. Open Letter from Law Professors' to Senator Leahy in Opposition to S.3804 (Combating Online Infringement and Counterfeits Act) (Nov. 16, 2010), *available at* http://www.publicknowledge.org/files/docs/LawProfCOICA.pdf.

151. Open Letter from Internet Engineers to Senate Judiciary Committee in

Due to concerns that COICA is over-broad, a number of opponents of the Bill have also argued that the number of jobs lost or businesses negatively impacted by attempts to block domain names under COICA will outweigh the number of jobs or revenue lost by piracy.[152] Other groups who have publicly opposed the Bill largely include human rights organizations and free speech advocates.

## IV. ANALYSIS

### *A. COICA's Threat to Free Speech and Expression*

The legislative process can yield laws with unintended consequences, which produce results well outside the anticipated scope. In implementing COICA, violations of First and Fifth Amendment Constitutional rights would be a concerning, unanticipated consequence. Serious violations of Constitutional rights may greatly outweigh the intended goal of curbing infringement and counterfeiting activity online. The free expression of ideas is considered by many countries to be a fundamental right of human beings.[153] Free speech is vital to a democracy, which thrives on the ability to form opinions through freely given and received information.[154] As Michael Macleod-Ball, ACLU Washington Legislative Office Chief of Staff and

---

Opposition to COICA *available at* http://www.publicknowledge.org/files/docs/COICA_internet_engineers_letter.pdf.

152. Steve DelBianco and Braden Cox, *I Think I Can, I Think ICANN: Regulating the Internet . . . or Not: ICANN Internet Governance: Is It Working?* 21 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 27, 31 (2008).

153. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948), *available at* http://www.un.org/en/documents/udhr/index.shtml ("Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."); *see also* MARK W. JANIS, RICHARD S. KAY & ANTHONY W. BRADLEY, EUROPEAN HUMAN RIGHTS LAW 235 (Oxford University Press 2008).

154. Keith Werhan, *The Classical Athenian Ancestry of American Freedom of Speech*, 2009 SUP. CT. REV. 293, 296 (2008).

First Amendment Counsel stated, "[t]he Internet is, and must remain, the most open marketplace of ideas in the privacy rights of all Americans. Trading our civil liberties for the promise of security will leave us with neither."[155] The First Amendment to the United States Constitution states, "Congress shall make no law . . . abridging the freedom of speech."[156] Free speech protections under the First and Fifth Amendments have been upheld in a wide range of circumstances, only to be overcome in specific and narrowly tailored situations.[157] Under the broad provisions of COICA, whole websites would be blocked or shut down even if only portions of them are "dedicated to infringing activity."[158] COICA is an aggressive attempt to reduce the significant amount of infringing activity that occurs online,[159] however, its overly broad approach seems to be unnecessary and unjustified. As Justice Hughes wrote many years ago in an opinion for the Supreme Court in another First Amendment context:

> If we cut through mere details of procedure, the operation and effect of the statute in substance is that the public authorities may bring the owner of a newspaper or periodical before a judge upon a charge of conducting a business of publishing scandalous and defamatory matter . . . and . . . his

155. *House Committee Advocates Internet Censorship: ACLU Voices Serious First Amendment Concerns*, ALCU.org (Sept. 29, 2010), *available at* http://www.aclu.org/free-speech/house-committee-advocates-internet-censorship.

156. U.S. CONST. amend. I.

157. *See e.g.,* Reno v. ACLU, 521 U.S. 844, 874 (1997)(the Supreme Court struck down anti-indecency provisions of the Communications Decency Act of 1996 as a violation of First Amendment freedom of speech); Ashcroft v. ACLU, 542 U.S. 656, 670 (2004)(the Supreme Court found portions of the Child Online Protection Act of 1998 to violate free speech); United States v. Am. Library Ass'n, 539 U.S. 194, 211-12 (2003)(the Supreme Court upheld as constitutional the Children's Internet Protection Act of 2000 because it only conditioned federal funds on compliance with filtering requirements, as opposed to prohibiting certain content outright).

158. Combating Online Infringement and Counterfeit Act, S. 3804,111th Cong., § 2(a) (2010).

159. DeLong, *supra* note 141.

> newspaper or periodical is suppressed and further publication is made punishable as a contempt. This is the essence of censorship.[160]

Under COICA, public authorities may bring the owner of an Internet site before a judge upon a charge of conducting a business of online infringement or counterfeiting and his Internet site is suppressed and further publication is made punishable as contempt. Under this description, Justice Hughes could easily find COICA to strike at the essence of censorship by suppressing Internet content, just as the statute in *Near v. Minnesota* did.

As in *Near v. Minnesota*, the United States Supreme Court has repeatedly stated that "prior restraints" on expression, or the restriction of speech prior to communication, rather than implementing sanctions afterwards is excessively restrictive of free speech rights.[161] In *Nebraska Press Ass'n v. Stuart*, Justice Burger stated that "prior restraints" on free speech were "the most serious and the least tolerable infringement on First Amendment rights."[162] The Supreme Court has said, "only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint."[163] Accordingly, if protected material is blocked from publication or circulation without these procedural protections in place, it is an invalid prior restraint.[164]

In *Center For Democracy & Technology v. Pappert*, the District Court for the Eastern District of Pennsylvania held that it was an unconstitutional prior restraint on free speech rights for a

160. Near v. Minnesota, 283 U.S. 697, 713 (1931).

161. *See id.* at 721-23 (holding that prior restraints are unconstitutional outside of exceptional circumstances such as national security needs); *see also* Carroll v. Princess Anne, 393 U.S. 175, 180-81 (1968); Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963).

162. Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).

163. Freedman v. Maryland, 380 U.S. 51, 58 (1965); *see also* United States v. Thirty-Seven Photographs, 402 U.S. 363 (1971); Southeastern Promotions v. Conrad, 420 U.S. 546 (1975).

164. Center for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 656 (E.D. Pa. 2004).

Pennsylvania statute to require access to be blocked for certain domain names which were accused of providing access to child pornography.[165] There, the Act at issue allowed the Pennsylvania Attorney General or a district attorney in Pennsylvania to obtain a court order requiring an ISP to "remove to disable" child pornography "residing on or accessible through" an ISP's service.[166] The goal of the Act in *Pappert*, was to protect children from sexual exploitation and abuse by interfering with the online distribution of child pornography.[167] The court held the Act to be an unconstitutional prior restraint on free speech, reasoning that the IP address and DNS filtering it employed resulted in unacceptable over-blocking.[168] The court found specifically that the DNS filtering used blocked hundreds of thousands of web sites that had no child pornography and were only related to the targeted material because they were sub-domains of the same parent domain.[169]

Additionally, the Supreme Court has said that the First Amendment requires that restrictions on speech "be precise and narrowly tailored to achieve the pin-pointed objective of the needs of the case."[170] In practice, COICA's provisions could operate as a form of prior restraint on expression or free speech, which is greatly disfavored by the Supreme Court.[171] COICA seeks to shut down whole Internet sites that are accused of propagating or attempting to propagate the transfer of infringing or counterfeiting content, regardless of whether the site was successful in doing so.[172] In shutting down the whole site, COICA will impact a significant amount of content that is legal or even protected

165. *Id.* at 663.

166. *Id.* at 619.

167. *Id.*

168. *Id.* at 651.

169. Center for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004).

170. Troy v Cochran, 544 U.S. 734, 738 (2005).

171. Near v. Minnesota, 283 U.S. 697, 721-23 (1931) (holding that prior restraints are unconstitutional outside of exceptional circumstances such as national security needs).

172. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(a), (2010).

speech. Rather than creating additional liabilities for illegal activity such as infringing or counterfeiting intellectual property, COICA seeks to snuff out offenders and anything else in its path with a broad swipe.

In *Freeman v. Maryland*, the Supreme Court made it clear that prior restraints on speech must at a minimum abide by strong procedural safeguards.[173] COICA, however, allows the Attorney General to obtain an order to block a domain name without first conducting an adversarial hearing on the merits of the accusations.[174] In short, it potentially allows for a prior restraint on speech with inadequate procedural safeguards in place. The reach of COICA is also extended to domain names owned by individuals outside of the United States' borders. As a group of law professors wrote in a letter to Senator Leahy:

> Rather than give these foreign website operators a meaningful opportunity to be heard and to contest the allegations of illegality in an adversarial hearing, the Act requires only that the Attorney General notify the domain name *registrant* - who may, but in many cases will not, be the operator of the website in question - of an intent to proceed against the site. Injunctions may be entered entirely *ex parte*, without the participation of any other party, and the Act does not provide for any review of a judge's *ex parte* determination that the website in question contains unlawful material. This falls short of what the Constitution requires before speech can be eliminated from public circulation.[175]

While the Bill does provide for a process to appeal or reverse the

173. Freedman v. Maryland, 380 U.S. 51, 58-60 (2005).

174. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(c), (2010).

175. Open Letter from Law Professors' to Senator Leahy in Opposition to S.3804 (Combating Online Infringement and Counterfeits Act) (Nov. 16, 2010) (on file with author) *available at* http://www.publicknowledge.org/files/docs/LawProfCOICA.pdf.

order,[176] this deference to the Attorney General's accusations of infringing or counterfeiting activity threatens Constitutional due process requirements of a full and fair trial with all interested parties present.[177] The loss of rights associated with this approach hardly justifies the Bill's intended goal.

While COICA presents a clear risk of unintentionally blocking large amounts of protected speech, it is uncertain whether web content discussing, encouraging, or in furtherance of infringing or counterfeiting activity is considered protected speech. In *New York v. Ferber*, the United States Supreme Court held that child pornography was "a category of material outside the protection of the First Amendment"[178] and was subject to content-based regulations.[179] However, no such exception has been explicitly made for speech discussing, encouraging or in furtherance of infringement or counterfeiting. When the Supreme Court struck down the anti-indecency provisions of the CDA in *Reno v. ACLU* as unconstitutional, the Court reasoned that adults should not be prohibited from receiving and sending adult pornography simply because of its potentially harmful effect on minors who might be exposed to it, particularly if there are less restrictive means available.[180] This reasoning implies that just because content has associated risks does not mean that those using such content legally should be prohibited from accessing it. However, it is questionable how far lawmakers can go to regulate or censor such speech in order to prevent the illegal activity from happening, as is attempted by the procedures of COICA.[181] The United States Government's aversion to limiting or regulating speech makes it likely that COICA would not fare well under the eyes of the United States Supreme Court.[182]

---

176. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong., § 2(h), (2010).

177. U.S. CONST. amend. V. ("No person shall . . . be deprived of life, liberty, or property, without due process of law").

178. New York v. Ferber, 458 U.S. 747, 763 (1982).

179. *Id.* at 763-764.

180. Reno v. ACLU, 521 U.S. 844, 882 (1997).

181. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(b)-(c) (2010).

182. *See* Clinton, *supra* note 48.

Historically, the United States and the international human rights community have strongly advocated against censorship, particularly with respect to the Internet.[183] Countries have censored Internet content for a wide range of reasons, including content that conflicts with local law,[184] content that offends the morals of the public,[185] content that is against public interest,[186] content that threatens the stability or dignity of the government,[187] or content that threatens the security of the country[188] or general public.[189] Starting in early 2007, the Turkish government began blocking YouTube because it refused to block the access of users to content the Turkish government found offensive and illegal under local law.[190] The Turkish government wanted Google, which owns YouTube, to block access to the video worldwide.[191] Google refused to institute such a widespread ban, but Turkey continues to block YouTube within its borders today.[192]

183. Stevenson, *supra* note 47, at 547-48 (2007); *see also* Memorandum from CDT to Senator Patrick J. Leahy, The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture (Sept. 28, 2010), http://www.cdt.org/files/pdfs/Leahy_bill_memo.pdf [hereinafter CDT Memo].

184. Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES, Nov. 28, 2008), *available at* http://www.nytimes.com/2008/11/30/ magazine/30google-t.html.

185. Clinton, *supra* note 48 (explaining how access to popular social networking Internet sites in Vietnam has suddenly disappeared).

186. Jane Spencer & Kevin J. Delaney, *YouTube Unplugged: As Foreign Governments Block Sensitive Content, Video Site Must Pick Between Bending to Censorship, Doing Business*, WALL ST. J., at B1 (Mar. 21, 2008), *available at* http://online.wsj.com/article/SB120605651500353307.html (reporting that a court in Turkey ordered blockage of all access to YouTube after a video appeared on the Web site that was deemed insulting to Mustafa Kemal Ataturk, the founder of modern Turkey).

187. *Id.* (China banned access to YouTube after video clips showing Tibetan monks being dragged through the streets by Chinese soldiers appeared on the site).

188. Rosen, *supra* note 184 (commenting on U.S. debates over censoring terrorists propaganda).

189. CDT Memo, *supra* note 183 (describing how hate speech is proscribable in France).

190. Spencer & Delaney, *supra* note 186. *See also* Rosen, *supra* note 184.

191. Rosen, *supra* note 184.

192. *Id.*

Additionally, some governments have taken advantage of copyright laws by using them as a pretext for suppressing political speech.[193] In a notable example, Russian authorities confiscated the computers of an environmental group who were protesting Vladimir Putin's decision to reopen a particular factory.[194] The Russian security services claimed that the confiscation was the result of a concern over pirated Microsoft software.[195] While Microsoft itself backed the actions of the Russian authorities who claim to have been attempting to comply with Russian law, there has since been an outcry from human rights organizations and a significant amount of controversy regarding the true intent of the Russian authorities.[196]

In recent years, there has been an increase in threats to the free flow of information over the Internet.[197] As Secretary of State Clinton noted in her *Remarks on Internet Freedom*, "[a]s I speak to you today, government censors somewhere are working furiously to erase my words from the records of history. But history itself has already condemned these tactics."[198] Most censorship activity on the international front has come with strong condemnation from the human rights community.[199] The United States government has made a clear commitment to advancing a single global Internet with equal access to knowledge and ideas, for all individuals.[200] In enacting COICA, the United States government would be taking a step back from this initiative by authorizing the Attorney General to direct ISPs or other entities to block website content through

193. Clifford J. Levy, *Russia Uses Microsoft to Suppress Dissent*, N.Y. TIMES, Sept. 11, 2010, *available at* http://www.nytimes.com/2010/09/12/world/europe/12raids.html.

194. *Id.*

195. *Id.*

196. *Id.*

197. Clinton, *supra* note 48.

198. *Id.*

199. Letter from human rights organizations to Senator Patrick J. Leahy (Oct. 26, 2010), *available at* http://www.eff.org/files/filenode/coica_files/COICA_human_rights_letter.pdf.

200. Clinton, *supra* note 48; *see also* Letter from Law Professors' to Senator Patrick J. Leahy in Opposition to S.3804 (Combating Online Infringement and Counterfeits Act) (Nov. 16, 2010), http://www.publicknowledge.org/files/docs/LawProfCOICA.pdf.

DNS tampering.[201] The United States would be sending a message that it supports forms of censorship when the content in question is considered unlawful in a particular country, as described in the Turkish and Russian cases discussed above.[202]

Overall, implementation of COICA would undermine the free expression of ideas and open the United States' gates to a wider use of censorship, in violation of the United States Constitution,[203] anti-censorships human rights initiatives,[204] and the United States' global Internet initiative.[205] Certainly, combating online infringement and counterfeiting activity is not the only goal that might be served by employing these techniques. This is a slippery slope. Before starting down it, serious consideration must be given to whether this type of censorship is even justified. Thus, before enacting COICA, Congress should consider, comprehensively, the various reasons for employing DNS blocking techniques and determine where the limits to DNS blocking should be.

### *B. COICA's Conflicts with Prior Legislation*

Established United States law and policy has limited the responsibility of "service providers"[206] in policing user behavior on Internet sites.[207] Some of the uncertainty associated with COICA stems from the gray areas in which it overlaps with prior legislation. Under the DMCA safe harbor provision, Congress ensured that under certain conditions, service providers would not be held liable for the actions of users who transmit infringing material.[208] This provision encourages service providers to follow certain take down procedures for infringing content of which they have constructive or actual knowledge.[209] However, there is no

201. CDT Memo, *supra* note 183.
202. *See* Levy, *supra* note 193; *see also* Rosen, *supra* note 184.
203. U.S. CONST. amend. I.
204. CDT Memo, *supra* note 183.
205. Clinton, *supra* note 48.
206. 17 U.S.C. § 512(k)(1) (2006).
207. *Id.* § 512(c).
208. *Id.* § 512(a).
209. *Id.* § 512(c).

obligation for these service providers to act as gate-keepers or to seek out such content for removal. This approach emphasizes the role of service providers as promoters of free communication among Internet users, rather than acting as a supervisory or regulatory force for Internet content. This approach encourages a decentralized Internet structure that functions on input and management from a wide range of sources in order to maximize the free flow of information.[210] However, this decentralized structure also relies on coordination of domain names in order to ensure functionality.[211] From a policy perspective, not placing a gate-keeping or policing responsibility on service providers helps to promote the decentralized structure of the Internet, which is fundamental to how the Internet works.[212]

A conflict between COICA and the DMCA arises due to the ambiguity of the term "service providers" as it is used in both COICA[213] and the DMCA.[214] A "service provider'" can refer generally to any provider of services, specifically to only Internet service providers (ISPs), or cover a group somewhere in between. The term is ambiguous, and depending on what it means, the DMCA could provide a safe harbor for the same entities that COICA looks to in blocking access to a domain name accused of infringing or counterfeiting activity.[215] Additionally, it is uncertain whether a service provider's actions of intentionally preventing a domain name from resolving to that domain name's Internet protocol address under COICA would satisfy the procedural requirements of the DMCA.[216] Under the DMCA a service provider may not be held liable for infringing content on an Internet site if they promptly "remove, or disable access to, the

210. ICANN CEO Talks About the New Affirmation of Commitments (Sept. 30, 2009), http://www.icann.org/en/announcements/announcement-30sep09-en.htm#video.

211. *Id.*

212. *Id.*

213. Combating Online Infringement and Counterfeit Act, S. 3804 111th Cong. § 2(e)(2)(B)(i) (2010).

214. 17 U.S.C. § 512(k)(1) (2006).

215. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(b), (e)(2)(B)(i) (2010).

216. 17 U.S.C. § 512(c)(1)(C) (2006).

material that is claimed to be infringing or to be the subject of the infringing activity."[217] However, the DMCA also imposes additional procedural steps in order to qualify for immunity, including blocking Internet sites that they know to be infringing, providing notice to accused sites, and designating an agent to receive notifications of claimed infringement.[218]

Additionally, the bill originally proposed that the Attorney General could maintain a list of domain names that are accused of infringing activity, operating as an effective blacklist.[219] Instead, the revised version of the Senate bill allows a private party to initiate the domain blocking process under COICA based on a reasonable belief that a website is infringing.[220] Thus, while COICA does not call for a "blacklist" of websites, it does provide that the Attorney General shall inform the Intellectual Property Enforcement Coordinator of any court order issued in compliance with COICA.[221] The Intellectual Property Enforcement Coordinator shall in turn post the accused domain names on a public Internet site, along with relevant information.[222] The Attorney General must maintain a public listing of domain names that are determined by the Department of Justice to be "dedicated to infringing activity."[223] While this change in the bill

217. *Id.*

218. *Id.*§ 512(c).

219. *See* Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(j) (as introduced in the Senate Sept. 20, 2010). The version introduced in the Senate included section 2(j), which stated, "The Attorney General shall maintain a public listing of domain names that; upon information and reasonable belief; the Department of Justice determines are dedicated to infringing activities but for which the Attorney General has not filed an action under this section." *Id.* The version reported in the senate did not include section 2(j).

220. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(e)(5)(B) (2010) ("No domain name registry, domain name registrar, financial transaction provider, or service that provides advertisements to Internet sites shall be liable to any person on account of any action described in this subsection voluntarily taken if the entity reasonably believes the Internet site is dedicated to infringing activities").

221. *Id.* §2(f).

222. *Id.*

223. *Id.*

appropriately limits some of the concentration of power under the Attorney General, it does little to lessen or remedy the concerns associated with such a blacklist. These changes make it easier for websites to be blocked based on a false or inappropriate accusation of infringing activity, since third parties only have to operate under a reasonable belief to block a website. This is especially concerning since COICA also immunizes third parties from liability for shutting down domain names.[224] Since no recourse or remedy is available under COICA for any person or entity harmed in the process, there is little to prevent these third parties from overzealously blocking websites.

The safe harbor provisions of the DMCA do not apply if a service provider has actual or constructive knowledge of infringing material on a site and does nothing about it.[225] These "red flag" situations remove a service provider's DMCA liability protections.[226] However, it is uncertain what actions taken under COICA serve as "actual or constructive knowledge" sufficient to trigger a "red flag" situation under the DMCA.[227] If such an action does trigger a "red flag" situtation, COICA could potentially strip a service provider of its DMCA protections unless it acts quickly to remove or disable the content in question.[228] COICA does not require that an entity take action to prevent a domain name from resolving to that domain name's IP address based on such "notice."[229] However, COICA could create an obligation on

224. *See id.* § 2(e)(5).

225. 17 U.S.C. § 512(c)-(d) (2010).

226. Viacom Int'l Inc. v. YouTube Inc., 718 F. Supp. 2d 514, 520-21 (S.D.N.Y. 2010) (citing Senate Committee on the Judiciary Report, S. Rep. No. 105-190 at 44-45 (1998) and House Committee on Commerce Report, H.R. Rep. No. 105-551 pt. 2 at 53-54 (1998)).

227. Posting of Sherwin Siy to publicnkowledge.org, *New Copyright Bill Bears Problems: Concerns with S.3804, the Combating Online Infringement and Counterfeits Act (COICA)* (Sept. 25, 2010, 13:02 EST) (on file with author), *available at* http://www.publicknowledge.org/blog/new-copyright-bill-bears-problems-concerns-s3. *See also Viacom*,718 F. Supp. 2d at 520-21 (citing Senate Committee on the Judiciary Report, S. Rep. No. 105-190 at 44-45 (1998) and House Committee on Commerce Report, H.R. Rep. No. 105-551 pt. 2 at 53-54 (1998)).

228. 17 U.S.C. § 512(c)(1)(C) (2006). *See* Siy, *supra* note 227.

229. Combating Online Infringement and Counterfeit Act, S. 3804 § 2(f)

service providers to actively monitor what actions taken are under COICA in order to comply with the DMCA, even if they had no other knowledge of infringing activity on an Internet site. Thus, it is essential that any obligations arising out of actions taken under COICA be properly delineated.

This additional burden would encourage service providers to act more proactively. It emphasizes a change in the role of service providers by creating greater incentives and obligations for them to police the Internet for infringing activity in order to remain within the DMCA's safe harbor provision.[230] This more pronounced role of service providers as overseers of Internet activity is potentially at odds with the safe harbor protections of the DMCA.[231] These conflicting obligations under COICA and the DMCA would need to be clarified before COICA could effectively be put into action.

### *C. Technical Problems Making COICA Difficult to Effectuate*

The goals of COICA may not be attainable through the provisions as they are currently written due to a series of technical problems with the Bill. As currently written, COICA's provisions apply to domestic domain names or foreign domain names. For domestic domain names, the Attorney General may serve orders to block the domain name of an Internet site believed to be "dedicated to infringing activity"[232] on domain name registrar or registry.[233] "Upon receipt of such order, the domain name registrar or registry shall suspend operation of, and may lock, the domain name."[234] For non-domestic domain names, the Attorney General may serve such orders on: (i) a service provider[235] or any other operator of a non-authoritative domain name system server, (ii) a

(2010).

230. *See id.*; *see also* 17 U.S.C. § 512(c)-(d) (2006).

231. *See* Combating Online Infringement and Counterfeit Act, S. 3804 111th Cong. § 2(f) (2010); *see also* 17 U.S.C. § 512(c)(1) (2006).

232. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(c)(1) (2010).

233. *Id.* § 2(e)(1).

234. *Id.*

235. *Id.* at § 2(e)(2)(B)(i) ("service provider" as it is defined in section 512(k)(1) of title 17, United States Code).

financial transaction provider,[236] or (iii) an Internet advertising service.[237] As discussed above, the term "service providers" is somewhat ambiguous.[238] COICA states that "a service provider, as that term is defined in section 512(k)(1) of title 17, United States Code, or other operator of a domain name system server" could be ordered by the Attorney General to block access to a site.[239] Section 512(k)(1) of title 17 covers almost any DNS server operator while explanations of the bill limit "service provider" to Internet Service Providers only.[240] The term "service providers" could refer to all ISPs, the root zone servers operated by the Internet Corporation for Assigned Names and Numbers (ICANN), the authoritative root zone servers operated by Verisign, or it may generally cover any entity "offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user."[241] If the burden is on the root zone servers, this is problematic because they are not all based in the US and most are run by private entities, making compliance difficult to achieve. Generally, "the DNS's structure shapes the degree to which the Internet is truly international or inherently tilted toward the United States and other Western countries"[242] in part because ICANN was established by the United States government as a quasi-private, international body that oversees DNS management.[243] In September of 2009, ICANN announced that it had reached a new deal with the US Department of Commerce, which would allow it to operate as a more independent entity, allowing other governments and other private entities to have a greater say in how domain names will be managed.[244] This change exemplifies an attempt to decrease the

236. *Id.* at § 2(e)(2)(B)(ii) ("financial transaction provider" as it is defined in section 5362(4) of title 31, United States Code).

237. *Id.* at § 2(e)(2)(B)(iii).

238. Siy, *supra* note 227.

239. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(e)(2)(B)(i) (2010).

240. 17 U.S.C. § 512(k)(1) (2006). *See also* Siy, *supra* note 227.

241. 17 U.S.C. § 512(k)(1) (2006).

242. Kevin Werbach, *supra* note 9, at 624.

243. *Id.*

244. ICANN CEO Talks About the New Affirmation of Commitments (Sept.

role of the United States as an overseer of the Internet, in favor of a more balanced and global influence on how it is run. By requiring root zone servers to block domain names under COICA, the United States would be working in the opposite direction, attempting to exert greater influence over the Internet.

If COICA generally burdens any providers of service on the Internet, there is a significant amount of ambiguity in determining what obligations COICA would place on them. For example, if COICA extends as far as requiring any provider of service on the Internet to remove links to accused sites, the consequences of such a mandate could be devastating to the functionality and goal of the Internet as an open forum for information. Additionally, the broad scope of COICA is concerning because it requires entire Internet sites to be blocked, rather than just the portions associated with infringing or counterfeiting activity.[245] By using the DNS to filter Internet content, a blocked domain name ends all activity on that site, or any sub-sites associated with the site.[246] This means, for example, that if the hosting service allows users to post third party material as sub-sites of the accused website, all of the sub-sites would also by blocked by DNS filtering.[247] Also, if a parent domain name were blocked, for example "il.com," any sub-domains of the parent would also be blocked, for example "pawlisz.il.com."[248]

COICA also defines the circumstances under which an Internet site is "dedicated to infringing activity,"[249] by requiring that the Internet site be primarily designed, marketed, or have no demonstrable commercially significant purpose, other than to offer infringing goods or services, or enable or facilitate infringement.[250]

---

30, 2009), http://www.icann.org/en/announcements/announcement-30sep09-en.htm#video. *See also,* 1 MCGRADY, *supra* note 23, § 1.14(b).

245. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(e)(1) (2010).

246. Center for Democracy & Technology v. Pappert, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004).

247. *Id.*

248. *Id.*

249. Combating Online Infringement and Counterfeit Act, S. 3804, 111th Cong. § 2(a) (2010).

250. *Id.* § 2(a)(1).

Some proponents of the Bill argue that this language sets a sufficiently high standard, such that it weeds out the majority of false accusations that opponents of the Bill are concerned with. While being "primarily designed" or having "no demonstrable commercially significant purpose" are certainly high standards of conduct, including the phrase "enable or facilitate" infringement is somewhat broad, particularly because there is no requirement that the owner or operator of an Internet site have knowledge of infringing activity before the site is blocked.[251] Thus, sites that facilitate transactions between users, many of which include infringing or counterfeited goods, could be blocked regardless of their knowledge that such goods are illegal, because they are primarily designed to enable or facilitate conduct which turns out to be illegally infringing. This is a far cry from the safe harbor of the DMCA and could hypothetically include sites such as Ebay, YouTube, Amazon, etc., particularly given the ambiguous definition of "service provider."[252]

However, "for all the risks it poses, the domain name blocking contemplated in S. 3804 can be easily circumvented, and thus will have little ultimate effect on online piracy."[253] This ineffectiveness also directly touches on COICA's unconstitutionality, based on the Supreme Court's statement in *Central Hudson Gas & Elec. Corp v. Public Serv. Comm'n*, that a law restricting speech "may not be sustained if it provides only ineffective or remote support for the government's purpose."[254] Through the large number of caching servers used to resolve IP addresses, users would be able to access unblocked cached versions of Internet sites that were prohibited or blocked.[255] This means that the blocked sites would be accessible to users until the caching servers refreshed themselves by talking to root or authoritative servers.[256] Alternatively, users could

---

251. *Id.*

252. 17 U.S.C. § 512(k)(1) (2006).

253. CDT Memo, *supra* note 183.

254. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564 (1980). *See* CDT Memo, *supra* note 183.

255. Microsoft TechNet, How DNS query works: Domain Name System (DNS), http://technet.microsoft.com/en-us/library/cc775637(WS.10).aspx (last visited Dec. 20, 2010).

256. *Id.*

circumvent a domain name block by accessing Internet sites using the IP address directly, rather than querying the DNS to translate the web address.[257] This would require that Internet users basically bypass the DNS system and catalog sites by IP address rather than URL web address, or, "operators of blacklisted websites could distribute a small browser plug-in or other piece of software to allow users to retrieve the IP addresses of the operators' servers."[258] However, "[t]he unified addressing system is, on some level, what makes the Internet the Internet. Without the ability to know that en.wikipedia.org is the English-language Wikipedia, there would be a collection of loosely connected private networks, rather than a single Internet."[259]

An even more serious risk is that an increasing number of foreign DNS servers would pop up outside the United States in order to avoid blocking orders under COICA.[260] "Users who want to engage in infringement will thus easily be able to route their traffic around DNS providers that enforce the blacklist."[261] As a result, COICA could cause a large amount of legitimate traffic to be blocked or re-routed, while the illegitimate traffic or targeted content will likely be disseminated in new or different fashions to get around the DNS re-routing. Damage to the functionality of the DNS also raises serious problems for businesses and consumers, while re-routing large amounts of Internet traffic to foreign servers poses some potentially serious security issues.[262] In a 2006 poll, 78% of small business owners said that a less reliable Internet would damage their business.[263] In April of 2010, China Telecom advertised network traffic routes that enticed fifteen percent of the world's Internet traffic to travel through Chinese servers for eighteen minutes.[264] This Internet hijacking affected a wide range

257. CDT Memo, *supra* note 183.

258. *Id.*

259. Werbach, *supra* note 9242, at 623.

260. CDT Memo, *supra* note 183.

261. *Id.*

262. *Id.*

263. Steve DelBianco and Braden Cox, *I Think I Can, I Think ICANN: Regulating the Internet . . . or Not: ICANN Internet Governance: Is It Working?* 21 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 27, 31 (2008).

264. Jason Ryan, *US Government and Military Websites Redirected to*

of sites, including NASA, the United States Senate, the four branches of the military and the office of the Secretary of Defense.[265]

If more and more public DNS servers were set up to avoid COICA by enticing traffic from inside the United States, "it would be easy for that operator to, for example, re-reroute requests for banking websites not to the requested sites but to phishing sites set up specifically to steal unsuspecting users' personal information in order to gain access to financial accounts or perpetrate other fraud."[266] In such a case, the United States would have a difficult time prosecuting or regulating such offshore servers, making COICA of little or no consequence in combating online infringement or counterfeiting.

## V. CONCLUSION

The struggle to effectively enforce intellectual property rights is an ongoing battle to achieve balance. New legislation passed in protection of intellectual property rights must take care to minimize any negative impact on other rights and encouraging legitimate business as much as possible. Congress must engage in a careful review of any overly broad legislation that may have significant unintended consequences. A legitimate and justified concern for the damage online infringement and counterfeiting causes to American businesses motivated the introduction of COICA to the Senate. However, equally legitimate and justified concerns over its impact on Constitutional rights to free speech, due process, and the consequences of COICA's technical problems are even more important. The issues addressed by parties on either side of the debate over COICA will not disappear, however, COICA is not the remedy needed.

*Ashley S. Pawlisz*

---

*Chinese Servers*, Nov. 17, 2010, http://abcnews.go.com/Technology/american-government-websites-hijacked-chinese-hackers-massive-april/story?id=12165826.

265. *Id.*

266. CDT Memo, *supra* note 183.