GO TO JAIL—DO NOT PASS GO, DO NOT PAY CIVIL DAMAGES: THE UNITED STATES' HESITATION TOWARDS THE INTERNATIONAL CONVENTION ON CYBERCRIME'S COPYRIGHT PROVISIONS

ADRIENNE N. KITCHEN

Abstract

The problem of combating copyright infringement increases tenfold when considered in light of today's global and digital environment. As more authors seek copyright protection, others seek to get around it by evading jurisdictional reach. The Council of Europe has developed the world's first International Convention on Cybercrime, which incorporates harsh substantive copyright provisions but neglects to include effective enforcement protocols. This Comment proposes that the United States not rush to adopt the Council of Europe's Convention, but rather seek a more definitive and effective solution in a singularly-focused agreement on intellectual property rights in a global economic context.

Cite as 1 J. MARSHALL REV. INTELL. PROP. L. 364

GO TO JAIL—DO NOT PASS GO, DO NOT PAY CIVIL DAMAGES: THE UNITED STATES' HESITATION TOWARDS THE INTERNATIONAL CONVENTION ON CYBERCRIME'S COPYRIGHT PROVISIONS

ADRIENNE N. KITCHEN*

> There are millions of people with personal computers to make copies. That is exactly one of the reasons I think you want to be very careful. You do not want to be accidentally taking a large percentage of the American people, either small business or citizens, into the gray area of criminal law.[1]

INTRODUCTION

In the summer of 2001, a young Russian man named Dmitri Skylarov traveled to Las Vegas to take part in the Defcon 9 computer hacker conference.[2] As a cryptographer for Elcomsoft, a Russian corporation involved primarily in developing computer forensic utility software,[3] Skylarov gave a presentation before hundreds of computer programmers entitled, "ebook Security: Theory and Practice."[4] The presentation consisted of a demonstration of Elcomsoft's "Advanced ebook Processor" software that allowed a user to view, edit, and copy books and other documents written in Adobe Systems' portable document format (PDF), formerly considered to be "unalterable."[5]

Skylarov did not return home to Russia for another six months.[6] On the evening following his demonstration, he was arrested by the F.B.I. at his hotel.[7] An unwilling guinea pig, Skylarov became one of the first persons to be prosecuted under the 1998 Digital Millennium Copyright Act ("DMCA")[8] for trafficking in software to circumvent

---

* J.D. Candidate, June 2003, The John Marshall Law School. B.A. in English & Rhetoric, Univ. of Ill. at Urbana-Champaign, 2000. The author wishes to thank Prof. Doris Estelle Long for her insights and Karl Maersch for his editorial assistance.

[1] United States v. LaMacchia, 871 F. Supp. 535, 544 (D. Mass. 1994) (quoting the Vice-President and General Counsel of the Computer and Communications Industry Association in Hearing on S. 893, Aug. 12, 1992).

[2] Jennifer B. Lee, *U.S. Arrests Russian Cryptographer as Copyright Violator*, N.Y. TIMES, July 18, 2001, at C8, *available at* LEXIS News Library, N.Y. Times File.

[3] *Id.* Interestingly enough, Elcomsoft's clients include many United States government agencies, including the F.B.I. and the C.I.A. *Id.*

[4] *Russian Computer Programmer Arrested for US Copyright Infringement*, AGENCE FRANCE PRESSE, July 18, 2001, *available at* LEXIS Library, News Group File, Most Recent Two Years [hereinafter *Russian Programmer*].

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2827 (1998). The DMCA was enacted by the Clinton administration on October 28, 1998 and implemented the obligations of the World Intellectual Property Organization into United States law. *Id.* The DMCA prohibits the use of anti-circumvention devices, which allow a person to bypass technological protection measures so that he may access or copy a work. Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J.

copyrighted materials on electronic books.[9] Suddenly, this twenty-seven-year-old father of two was faced with a potential five-year jail sentence and a $500,000 fine for demonstrating software that was "perfectly legal" in his own country.[10] By the time of his indictment by a California grand jury, the charges against him had grown to include conspiracy to traffic in circumvention technology, which would bump his potential jail sentence up to twenty-five years with a monetary fine up to $2.25 million.[11] Advocates of the prosecution initially hoped that Skylarov's incarceration would "send a message to Russian and European hackers that software tampering and pirating would be aggressively pursued across borders."[12]

Internet liberty advocates quickly jumped to Skylarov's defense, contending that the dispute between Adobe and Elcomsoft was clearly of a commercial, not criminal, nature.[13] Asserting that free speech was at risk, they voiced protests that software programmers and computer security researchers joined nationwide.[14] Within a week, Adobe retracted their support of Skylarov's prosecution, conceding that it "was not conducive to the best interests of any of the parties involved or the industry."[15] Despite this, the U.S. Department of Justice pressed on, determined to make an example of the Russian who would dare show how to decrypt an e-book code.

519, 519 (Spring 1999). The DMCA also prohibits circumvention in general. *Id.* The DMCA was intended to protect the rights of copyright holders, but it also protects Internet service providers ("ISPs") from liability for end-user infringement. *Id.* The DMCA contains five main sections: Title I, dealing with WIPO treaty implementation; Title II, establishing ISP liability limitations; Title III, establishing exemption from liability for copyright infringement done in the course of restoring or repairing software programs on computers; Title IV, covering miscellaneous provisions; and Title V, dealing with protection of certain original designs. Jo Dale Carothers, Note, *Protection of Intellectual Property on the World Wide Web: Is the Digital Millennium Copyright Act Sufficient?*, 41 ARIZ. L. REV. 937, 939 (Fall 1999). Congress included a clause that a fair use defense to infringement may still be applied despite the restrictions on anti-circumvention measures, but failed to establish what exactly a fair use is on the Internet. *Id.* at 944-45. Interestingly enough, the DMCA anti-circumvention laws did not go into effect until two years after its enactment, which is suggestive of the problems Congress faced in adapting the law to increasingly complex technology issues. *Id.* at 952-53.

[9] *Russian Programmer*, *supra* note 4.

[10] Lee, *supra* note 2, at C8; *see also* Sabrina Tavernise, *Russians Deem Arrest Insult to Their Industry*, N.Y. TIMES, Aug. 30, 2001, at C3, *available at* LEXIS News Library, N.Y. Times File (quoting a Russian programmer who denounced the U.S. actions as "rubbish" and "crazy," and who analogized that, "[i]t's the same as buying a loaf of bread, and when you find the middle isn't baked, you come back to show the baker and get put in jail").

[11] Adam Creed, *Skylarov Indicted, Could Face 25 Years in Jail*, NEWSBYTES, Aug. 28, 2001, *available at* LEXIS News Library, Newsgroup File, Most Recent Two Years.

[12] *See Russian Programmer*, *supra* note 4; *see also* Tavernise, *supra* note 10, at C3 (remarking that even prior to Skylarov's prosecution, Russia struggled with its reputation as a country that bred software piracy). With the collapse of the Communist state, Russia's economy collapsed as well, breeding and marketing software piracy that still exists on nearly every street corner there today. *Id.*

[13] *Fate of Russian Arrested for Hacking Undecided*, AGENCE FRANCE PRESSE, July 23, 2001, *available at* LEXIS News Library, News Group File, Most Recent Two Years.

[14] *Id.*

[15] *U.S. Company Backs Down on Prosecuting Russian Hacker*, AGENCE FRANCE PRESSE, July 24, 2001, *available at* LEXIS News Library, Newsgroup File, Most Recent Two Years.

Insisting he had done nothing wrong, Skylarov pled not guilty to the charges against him.[16]

In November 2001, while Skylarov remained in California, the Council of Europe ("CoE") called upon their member and observer-status countries to adopt the Council's Convention on Cybercrime. The Convention was the first treaty to seek harmonization of cybercrime laws, like those contained within the DMCA. With the initiative of the Convention, countries around the world began to discuss the line separating copyright infringement from criminal activity, whether new and harsher laws are needed, and how to make such laws effective worldwide. These issues beg the questions: What should be done with people like Skylarov? Did Congress intend to punish his conduct criminally? In a growing global economic community, who will be responsible for pursuing the copyright offender and determining whether the punishment fits the crime?

This Comment discusses the goals, scope, and effectiveness of the world's first international cybercrime treaty and its criminal copyright provisions. Part I.A discusses the evolution of cybercrime and its impact on the global economy. Part I.B examines the history and structure of the CoE and its relationship with the United States. Part I.C then explains the purpose and goals of CoE's Draft International Convention on Cybercrime.

Part II.A describes the criminal standards and penalties imposed by the terms of the Convention. Part II.B contrasts the Convention with current United States copyright and cybercrime statutes, particularly the No Electronic Theft Act and Title 18 of the United States Code, to determine what copyright infringement the United States criminalizes and why. Part II.C dissects the major purported objections and challenges to the Convention from an American legal and Constitutional standard.

Part III proposes that the United States Congress refuse to take the final step of ratification of the Convention treaty as it exists now. Part III also suggests that while the issue of cybercrime prevention and penalty is ripe, the United States needs to quickly address the issue of criminal copyright infringement in a broader form. Finally, Part IV advocates that the need for an effective international force against cybercrime is real and concludes that fundamental American values and rights need not be sacrificed at the expense of a hasty preemptive strike at cybercrime.

I. THE COUNCIL OF EUROPE, CYBERCRIME, AND THE DRAFT INTERNATIONAL CONVENTION

A. The Evolution of Cybercrime and its Global Consequences

Cybercrime is a relatively new term for crimes that involve computer networks.[17] In this age of digitalization, companies all over the world rely heavily on computer

---

[16] Colin McMahon, *Russian Hacker Cuts Freedom Deal*, CHI. TRIB., Dec. 21, 2001, at 35, *available at* LEXIS News Library, Chicago Tribune File. While awaiting trial, Skylarov made a deal with the United States in which he admitted to the facts of his situation but not illegal activity, and effectively secured his freedom and a trip back to Moscow. *Id.*

[17] *See* BLACK'S LAW DICTIONARY 319 (7th ed. 1999). The term cybercrime is a general term that encompasses such illegal acts as "cybersquatting," "cyberstalking," and "cybertheft." *Id.* Cybersquatting is the act of reserving a domain name on the Internet, especially a name that would

networks for transferring and storing information, as well as communicating with other businesses and consumers.[18] Computer users, known as "hackers," use their knowledge of computer systems to break into complex databases and networks to commit various crimes.[19]

The Internet finds itself conducive to fraud, copyright infringement, child pornography, and other crimes because its content can be easily dispersed all over the world in a relatively anonymous manner.[20] Cybercrime also has the potential to cause serious public safety problems, most notably when critical infrastructure operation systems are targeted.[21]

As such networks reach across international lines, the crimes committed have great jurisdictional range.[22] Cybercrimes, including criminal copyright infringement, have been increasing in both frequency and severity in recent years as hackers and other criminals keep up with the latest technological encryption and protection advances.[23]

For example, a survey conducted by the Computer Emergency Response Team ("CERT") Coordination Center at Carnegie-Mellon University indicated a 183% jump in the number of hacking incidents over a one-year span.[24] Also, the Spring 2000 Computer Security Institute ("CSI")/FBI Computer Crime and Security Survey projected monetary losses exceeding $265 million in 2000, up from $100 million in 1997; those may in fact be underestimated figures, because only forty-two percent of respondents were able to quantify their losses.[25] A more recent study by an independent research institute, Computer Economics, indicated that the spreading of the "I Love You" virus from the Philippines, as well as copycat viruses, resulted in $6.7 billion in damages to businesses worldwide.[26] Virus attacks also resulted in

---

be associated with a company's trademark, and then seeking to profit by selling or licensing the name to the company that has an interest in being identified with it. *Id.* Cyberstalking is the act of threatening, harassing, or annoying someone through multiple e-mail messages, through the Internet. *Id.* Cybertheft is the act of using an online computer service, such as one on the Internet, to steal someone else's use and enjoyment of property. *Id.*

[18] *See* U.S. Dept. of Justice Frequently Asked Questions About the Council of Europe Convention on Cybercrime, *available at* http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm [hereinafter Dept. of Justice—Convention FAQs] (last visited Nov. 4, 2001).

[19] *See* Agent Steal, *available at* http://www.agentsteal.com (last visited Nov. 4, 2001). Articles, written by Agent Steal, otherwise known as Justin Petersen, include titles such as "Everything a Hacker Needs to Know About Being Busted by the Feds," and "Tapping Data Phone Lines." *Id.*

[20] *See generally* Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 CAL. CRIM. LAW REV. 1 (2001) (noting that most "cybercrimes" are just regular crimes that are capable of being carried out via the use of a computer, including theft and embezzlement, fraud, forgery, pornography, obscenity, stalking, vandalism, burglary, common trespass, as well as inchoate offenses).

[21] *See* Dept. of Justice—Convention FAQs, *supra* note 18 (offering an example of a case in which a juvenile disabled a telephone company computer that supported communications services to an airport, forcing the FAA to close its control tower for several hours).

[22] *See id.* (offering an example of the international scope of cybercrime). In 1998, Vladimir Levin was convicted of hacking into a major international bank from Russia and transferring $12 million from accounts located around the world. *Id.*

[23] *See id.*

[24] *Id.*

[25] *Id.*

[26] *Id.* Also known as the "Love Bug," the "I Love You" virus took VBScript form and called itself VBS_LOVELETTER. *Id.* The virus used Microsoft Outlook to send e-mail to all on its

more than $12.1 billion in damages to businesses during 1999 alone, with such figures projected to rise in the following years.[27]

B. The History and Structure of the Council of Europe

The Council of Europe ("CoE"), organized in 1948,[28] is an intergovernmental organization[29] comprised of forty-three European member countries.[30] Any European country is welcome to become a member of CoE provided it accepts the principle of the rule of law and guarantees human rights and fundamental freedoms to everyone under its jurisdiction.[31] CoE states four goals of its assembly: (1) to protect human rights, pluralist democracy, and the rule of law; (2) to promote awareness and encourage the development of Europe's cultural identity and diversity; (3) to seek solutions to problems facing European society;[32] and (4) to help consolidate

---

address list with a subject line reading, "ILOVEYOU". *Id.* The body of the message read, "kindly check the attached LOVELETTER coming from me," and included the lethal attachment file entitled, "LOVE-LETTER-FOR-YOU.TXT.VBS." *Id.* When the attachment was opened, the virus would overwrite the computer's files with specific extensions for its codes, which effectively wiped out the host codes and replaced them with the infected codes, ready to be forwarded on to other unsuspecting e-mailers. *Id.* The virus also replicated itself through the mIRC chat program, where one infected user would inadvertently spread the virus to everyone in that user's chat channel. *Id.*; *see* Virus Encyclopedia, *available at* http://www.antivirus.com/vinfo/virusencyclo/ (last visited Jan. 10, 2002).

[27] *See* Dept. of Justice—Convention FAQs, *supra* note 18.

[28] *See* A Short History of the Council of Europe, *available at* http://www.coe.int/portalt.asp (last visited Nov. 4, 2001) (explaining how CoE sprung out of a movement dedicated to European unity and rebuilding the continent after the liberation of the European States following World War II). Winston Churchill proposed "a remedy which, as if by miracle, would transform the whole scene and in a few years make Europe as free and happy as Switzerland is today. We must build a kind of United States of Europe." *Id.*

[29] *See* Council of Europe: an Overview, *available at* http://www.coe.int/portalt.asp [hereinafter Overview of Council of Europe] (last visited Nov. 4, 2001) (clarifying that CoE is not to be confused with the European Union, which is a distinct organization comprised of 15 member countries). All fifteen European Union states are also members of the Council of Europe. *Id.* The official languages of CoE are English and French; however, the Parliamentary Assembly also uses German, Italian, and Russian as working languages, and other languages may be interpreted during debates. *Id.*

[30] *See* Council of Europe: the Parliamentary Assembly, *available at* http://www.coe.int/portalt.asp (last visited Nov. 4, 2001) (listing member countries of the Council of Europe and their number of representatives: Albania (4), Armenia (4), Andorra (2), Austria (6), Azerbaijan (6), Belgium (7), Bulgaria (6), Croatia (5), Cyprus (3), Czech Republic (7), Denmark (5), Estonia (3), Finland (5), France (18), Georgia (5), Germany (18), Greece (7), Hungary (7), Iceland (3), Ireland (4), Italy (18), Latvia (3), Liechtenstein (2), Lithuania (4), Luxembourg (3), Malta (3), Moldova (5), Netherlands (7), Norway (5), Poland (12), Portugal (7), Romania (10), Russia (18), San Marino (2), Slovakia (5), Slovenia (3), Spain (12), Sweden (6), Switzerland (6), "the former Yugoslav Republic of Macedonia" (3), Turkey (12), Ukraine (12), United Kingdom (18)).

[31] *See* Overview of Council of Europe, *supra* note 29 (noting that the Council also grants consultative status to over 350 non-governmental organizations ("NGO") so that they may work together to represent the ordinary public). NGO's are consulted via discussions and colloquies with members of the Parliamentary Assembly to ensure a free-flowing dialogue between the two sectors. *Id.*

[32] *See id.* (noting that such problems include discrimination against minorities, xenophobia, intolerance, environmental protection, human cloning, AIDS, drugs, organized crime, and others).

democratic stability in Europe by backing political, legislative and constitutional reform.[33]

The framework upon which CoE stands is comprised of the Parliamentary Assembly, which serves to hear deliberations on issues,[34] and a Committee of Ministers, which makes decisions on the issues at hand.[35] The Assembly meets four times a year for a week at a time in plenary session in the Chamber of the Palais de l'Europe in Strasbourg.[36] An essential role of the Assembly is to create treaties with the effect of harmonizing European legal systems.[37] The United States, as a non-member State, holds observer status in the Committee of Ministers' decision-making activities, and may choose to adopt or reject the conventions enacted by CoE at its discretion.[38]

---

[33] *See id.* (stating that CoE's work reaches into such areas as human rights, media, legal co-operation, social and economic questions, health, education, culture, heritage, sport, youth, local democracy and trans-frontier co-operation, the environment and regional planning). CoE receives financing for its projects and activities from the governments of its member states, who each contribute an amount proportionate to their population and wealth. *Id.* CoE's 2002 budget is roughly 169 million Euros. *Id.*

[34] *See* Council of Europe: the Parliamentary Assembly, *available at* http://www.coe.int/portalt.asp (last visited Nov. 4, 2001) (articulating that the Assembly is comprised of 602 members (301 representatives and 301 substitutes) drawn from each of the 43 represented nations). Every country contributes between 2 and 18 representatives depending on population size. *Id.* Five political groups are officially represented: the Socialist Group, the Group of the European People's Party, the European Democratic Group, the Liberal, Democratic and Reformers' Group, and the Group of the Unified European Left. *Id.*

[35] *See* Council of Europe: the Committee of Ministers, *available at* http://www.coe.int/t/e/committee_of_ministers/public (last visited Nov. 4, 2001) (describing that the Foreign Ministers of the member states meet at least twice a year to review political issues and matters of European co-operation and to give the necessary political impetus to CoE's activities). The Committee of Ministers functions not only as the decision-making body of CoE, but also as the facilitator of its enacted international agreements. *Id.*

[36] *See* Council of Europe: the Parliamentary Assembly, *supra* note 34 (describing that each session involves political debates on issues of importance to European nations and serves to create international treaties, known as conventions in Europe, to be ratified by the Committee of Ministers and to be effective upon all member countries). In an effort to create dialogue between representatives and experts on vital social and political issues, the Assembly also holds regular conferences, symposiums, and public parliamentary hearings. *Id.*

[37] *See* Council of Europe: Legal Co-operation, *available at* http://www.coe.int/portalt.asp/ (last visited Nov. 4, 2001) (identifying measures the Council is taking to shape European legislation).

[38] *See* Council of Europe's Member States, *available at* http://www.coe.int/portalt.asp (last visited Nov. 4, 2001) (describing the rules of membership). The United States gained observer status to the Committee of Ministers on October 1, 1996, meaning that it may participate in discussions and may adopt CoE enactments, but is not technically bound to comply with all CoE decisions, member states must. *Id.* Other countries with observer status to the Committee are: Canada, Holy See, Japan, and Mexico. *Id.* Canada, Israel, and Mexico hold observer status to the Parliamentary Assembly. *Id.* Additionally, two countries, Bosnia-Herzegovina and the Federal Republic of Yugoslavia, are deemed Special Guests to the Parliamentary Assembly. *Id.*

C. History, Purpose, and Goals of the Council of Europe's International Convention on Cybercrime

Recognizing the increasing growth of computer and Internet technology on a global scale, the CoE began discussions about combating cybercrimes in the late 1980's.[39] In 1989, CoE created its first official recommendation that new substantive laws be developed that would criminalize certain conduct committed through computer networks.[40] Twelve years later, in April 2001, the Committee of Ministers and the Parliamentary Assembly approved the final draft of the International Convention on Cybercrime. Because the Convention draft differs in several respects to United States statutes, the treaty has been signed by the United States, but Congress has not yet ratified it.[41]

"The Convention covers three main topics: harmonisation of the national laws which define offences, definition of investigation and prosecution procedures to cope with global networks, and establishment of a rapid and effective system of international co-operation."[42] Offenses criminalized by the Convention include offenses against the confidentiality and integrity of computer systems, computer-related offenses such as forgery and fraud, content-related offenses, and copyright infringement offenses.[43] Although United States law encompasses the majority of these offenses, the Convention creates an international minimum standard for criminal behavior, a procedural format for enforcement, and most notably, a requirement of international cooperation and assistance in investigation and prosecution of such cybercrimes.[44]

---

[39] *See* First International Treaty to Combat Crime in Cyberspace, *available at* http://conventions.coe.int/Treaty/EN/cadreprojets.htm (last visited Mar. 1, 2002) (noting that traditional international cooperation efforts would not be sufficient to keep up with the explosive growth of technology and its capacity for use in criminal pursuits).

[40] *See* Council of Europe Press Service, *available at* http://www.press.coe.int (last visited Nov. 4, 2001) (identifying a second study and recommendation on corresponding procedural law which was completed in 1995). In February 1997, the Council of Europe's Committee of Ministers devised a new committee, the Committee of Experts on Crime in Cyberspace, to prepare a binding legal document that would incorporate issues such as substantive criminal offenses, the use of coercive powers, and jurisdiction in cybercrime cases. *Id.* Between April 1997 and December 2000, the Committee held ten meetings, and the drafting group held fifteen meetings to debate and draft the Convention. *Id.* In April 2000, the draft text was declassified and published on Internet, so that specialists and network users could comment. *Id.* In March 2001, the Parliament invited international experts to a special hearing to debate the major premises as well as the fine points of the Convention. *Id.* Following this, the Committee of Ministers asked the Assembly for an opinion on the draft, which it adopted, with several amendments, at its April 2001 session. *Id.*

[41] *Council of Europe Signs Draft Cybercrime Treaty*, THE INDUSTRY STANDARD.COM, June 22, 2001, *available at* LEXIS, News Library, The Industry Standard file. The United States signed the treaty on June 22, 2001. *Id.*

[42] *See generally* Main Lines of the Convention, *available at* http://www.press.coe.int (last visited Nov. 4, 2001).

[43] *Id.*

[44] *See* Dept. of Justice—Convention FAQs, *supra* note 18; *see also* Main Lines of the Convention, *supra* note 42 (stating that the international enforcement of the criminal provisions would require law enforcement authorities in different countries to collect and exchange information as well as computer-based evidence, though purportedly not to facilitate "transfrontier" searches; the system was intended to be fast-paced and operating at all times to ensure immediacy of investigation).

II. COMPARISON AND CONTRAST OF THE COPYRIGHT REGULATIONS AND PENALTIES OF CURRENT U.S. STATUTES AND THE CRIMINAL COPYRIGHT PROVISIONS OF THE CONVENTION

A. United States Statutes Involving Criminal Copyright Violations

Copyright protection serves to promote the progress of science and the useful arts by granting exclusive rights to the copyright holder.[45] Copyright law in the United States is currently governed mainly by four statutes: the Copyright Act of 1976;[46] the No Electronic Theft Act;[47] the Audio Home Recording Act of 1992;[48] and the Digital Millennium Copyright Act.[49] Generally, United States copyright law does not exist to criminalize copyright offenses; the majority of remedies are civil.[50] Nonetheless, the No Electronic Theft Act ("NET Act") consists of amendments to the Copyright Act of 1976 that were created "to provide greater copyright protection by amending criminal copyright provisions, and for other purposes."[51] The NET Act[52] applies criminal infringement remedies in § 506(a) to one who willfully infringes a copyright[53] either:

> (1) for purposes of commercial advantage or private financial gain,[54] or
>
> (2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords, or more copyrighted works, which have a total retail value of more than $1,000.[55]

---

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

[46] Copyright Act of 1976, 17 U.S.C. §§ 101-810 (1994 & Supp. 2000).

[47] No Electronic Theft Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997).

[48] Audio Home Recording Act, 17 U.S.C. §§ 1001-1010 (1992).

[49] *See generally* DMCA, *supra* note 8.

[50] *See* 17 U.S.C. §§ 501-505 (2000) (listing such civil remedies as injunctions, impounding and disposition of infringing articles, damages (actual and statutory) and profits, and costs and attorney's fees). The provisions make extensive use of the word "may" in explaining the powers that the judiciary has to adjudicate such infringement actions. *Id.*

[51] NET Act, 111 Stat. 2678 (1997); *see also* UCLA Online Institute for Cyberspace Law and Policy: The 'No Electronic Theft' Act, *available at* http://www.gseis.ucla.edu/iclp/hr2265.html (last visited Nov. 4, 2001) (remarking that the Act was meant to close a loophole in the previous criminal copyright laws, where intentional copiers and distributors of copyrighted material over the internet did not face criminal penalties so long as they did not profit from their actions).

[52] *See generally* 17 U.S.C. §§ 1201-02, 1204 (2000) (discussing criminal infringement remedies). The NET Act is discussed specifically because it provides the most comprehensive criminal copyright provisions, while the Digital Millennium Copyright Act's criminal provisions, for example, apply only to limited copyright violations such as circumvention of copyright protection systems and tampering with copyright management information.

[53] *See* Copyright Act of 1976, 17 U.S.C. § 101 (1994 & Supp. 2000) (failing to define the term "willful"). *But see* 17 U.S.C. § 506(a)(2) (2000) ("For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.").

[54] *See* 17 U.S.C. § 101 (2000) ("The term 'financial gain' includes receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works.").

[55] NET Act, 111 Stat. 2678 (1997).

The penalties applied for criminal infringement are governed by 18 U.S.C. § 2319.[56] When a violation of the NET Act occurs, the offender is subject to a jail sentence and monetary fine, the respective length and amounts of which are contingent upon the degree of infringement.[57] The degree is measured by several factors: the number of infringing actions; the value of the copyrighted works; and the number of previous offenses by the infringer; the greater these factors, the more severe the punishment.[58]

Thus, turning a copyright violation that occurs by electronic means into a cybercrime was a somewhat difficult process under United States law, though the NET Act made prosecution a more viable option than it previously had been.[59]

---

[56] 17 U.S.C. § 506(a)(2) (2000).

[57] 18 U.S.C. § 2319 (2000). Section 2319 provides that one who violates 506(a) shall be punished in the following manner and in addition to any other applicable provisions of Title 17:

> (b) Any person who commits an offense under section 506 (a)(1) of Title 17—
>
> (1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;
>
> (2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
>
> (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.
>
> (c) Any person who commits an offense under section 506(a)(2) of Title 17, United States Code-
>
> (1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;
>
> shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
>
> shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords or 1 or more copyrighted works, which have a total retail value of more than $1,000.

Id.

[58] *Id.*

[59] *See generally* Business Software Alliance: First Guilty Verdict Under NET Act Draws Praise, *available at* http://www.bsa.org/usa/press/newsreleases/1999-08-20.181.phtml (last visited Nov. 4, 2001). While the NET Act was passed in 1997, the first conviction under the Act did not take place until May 11, 2001. *Id.* Christian Morley of Salem, Massachusetts was found guilty of conspiracy to infringe software copyrights as a member of the hacker organization "Pirates with Attitudes." *Id.* The group regularly distributed unauthorized copies of software, including unreleased versions. *Id.*

Copyright violations are still criminalized where illegal reproductions and distributions, including "sharing," knowingly occur on a relatively grand scale, but may also be criminalized for even smaller degrees of infringement.[60] The NET Act amendments reflect a desire to protect copyright owners while maintaining intent, value, and time restrictions, so as not to promote zealous and fruitless prosecutions of small-time offenders.[61]

Recognizing the need for copyright protection worldwide, the United States has also committed itself to international agreements such as the Berne Convention for the Protection of Literary and Artistic Property ("Berne Convention")[62] and the Universal Copyright Convention,[63] which provide that United States copyright law will be protected even where infringements occur in other countries.[64]

The United States is also a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods ("TRIPS"), which is administered by the World Trade Organization ("WTO").[65] TRIPS provides for enforcement procedures that are "fair and equitable" and those that will permit "effective action against any act of infringement of intellectual property rights."[66] Article 61 of TRIPS promotes criminal penalties including imprisonment and monetary fines "sufficient to provide a deterrent, consistently with

---

[60] *See* File-Sharing Primer, *available at* http://hotwired.lycos.com/webmonkey (last visited Nov. 4, 2001). File and software "sharing" is a popular trend amongst college students and adults alike. *Id.* Popular file-sharing applications include Napster, Macster (for Macintosh operating systems), Gnutella, and Scour Exchange. *Id.* These "peer-to-peer" applications allow file-sharers to swap music, videos, and other files amongst themselves. *Id.* Recently, Napster became the subject of a very public debate on the legal validity of file sharing. *Id.*; *see also* A & M Records, Inc. v. Napster Inc., 239 F.3d 1004 (9th Cir. 2001) (finding that by its transmission and database of peer-to-peer music files, Napster probably engaged in contributory and vicarious copyright infringement).

[61] *See* 17 U.S.C. § 507(a)-(b) (2000) (establishing a five-year statute of limitations, commencing after the cause of action first arose, for maintaining a criminal proceeding, and a three-year statute of limitations, beginning after the claim accrued, for bringing a civil suit).

[62] Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, last revised in Paris, July 24, 1971, 828 U.N.T.S. 221. The United States did not become a member of the Berne Convention until March 1, 1989. *Id.*

[63] Universal Copyright Convention, Aug. 11, 1910, last revised in Paris, July 24, 1971, 6 U.S.T. 2731.

[64] International Copyright, *available at* http://www.loc.gov/copyright/fls/fl100.pdf (last visited Dec. 7, 2001). True "international copyright" does not exist to protect expression throughout the world. *Id.* Prior to these treaties, if an author's work was copyright-protected in the United States and then was used without authorization in another country, the author would only have redress according to the copyright laws—if any existed—in the other country. *Id.*

[65] General Agreement on Tariffs and Trade-Multilateral Trade Negotiations: Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods, Apr. 15, 1994, 33 I.L.M. 81 [hereinafter TRIPS]. TRIPS sought to "establish a mutually supportive relationship between the WTO and the World Intellectual Property Organization (WIPO) as well as other relevant international organizations." *Id.* Both the TRIPS Agreement and the WIPO Copyright Treaty incorporate the Berne Convention as a foundation for their principles. *Id.*

[66] *Id.* art. 41(1). The most notable advance in protection contained in TRIPS is its establishment of procedural enforcement norms that signatory countries must incorporate into their domestic laws; the advance is substantial in comparison to the Berne Convention, which did not contain procedural enforcement norms. Doris Estelle Long, Enforcement and the TRIPS Agreement (excerpted) in *A Coursebook in International Intellectual Property Law* (Doris Estelle Long & Anthony D'Amato eds., 2000).

the level of penalties applied for crimes of a corresponding gravity."[67] What TRIPS does *not* do is require a harmonization of enforcement standards and procedures between nations, which the Convention purports to necessitate.[68]

B. Criminal Standards and Penalties Imposed by the Convention

The Convention on Cybercrime consists of four chapters encompassing forty-eight articles.[69] Copyright offenses comprise their own title within chapter two: measures to be taken at the national level.[70] Though brief, Article 10, "Offenses Related to Infringement of Copyright and Related Rights," takes a serious stance on the establishment and enforcement of criminal copyright provisions.[71] Specifically, Article 10[72] *requires* that signatory countries criminalize any instance of copyright infringement or related infringement "where such act[s] are committed wil[]fully, on

---

[67] *See* TRIPS, *supra* note 65, art. 61.

[68] *See* The TRIPS Agreement and Trade Facilitation: Background Note by the Secretariat, *available at* http://docsonline.wto.org (last visited Nov. 20, 2001). "Wide disparities between levels of intellectual property protection cause problems in international trade as goods and services which may be produced and sold in one jurisdiction may be infringing in another. The approximation of legal standards and enforcement procedures tends to alleviate these problems, but the TRIPS Agreement will not eliminate them." *Id.*

[69] *See* Convention on Cybercrime, *available at* http://conventions.coe.int/treaty/en/projets.htm [hereinafter Convention](last visited Nov. 4, 2001).

[70] *Id.*

[71] *Id.*

[72] *Id.* Article 10 provides:

> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, [sic] on a commercial scale and by means of a computer system.
>
> 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
>
> 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

a commercial scale and by means of a computer system."[73] The copyright provisions state that each country must establish laws that would create criminal copyright offenses, pursuant to the countries' obligations under the Berne Convention, TRIPS Agreement, and WIPO Copyright Treaty, in cases of willful infringement on a commercial scale by the use of a computer system.[74] Further, the Convention's copyright provisions provide for criminal laws enforcing the infringement of related rights with the same requirements of willful infringement on a commercial scale by the use of a computer system.[75] Lastly, the Convention copyright provisions allow for a country to reserve its right *not* to impose criminal liability on a copyright infringer, but only where other "effective" measures are in place that would not clash with the Convention's rules within Article 10.[76] Thus, the Convention establishes international rules intended to harmonize copyright laws between nations, with the plain intent to take a stricter stance on criminal copyright liability.

In contrast to the United States' NET Act, copyright infringement actions that merely meet the three aforementioned requirements are automatically delineated as criminal, with no minimum damage amount, time frame, or number of copies made.[77] Any infringement that is done with knowledge that it is illegal, on a commercial scale,[78] by the use of a computer system makes the infringer criminally liable and subject to criminal punishment under the law of that country.[79] However, unlike in the TRIPS Agreement, there is no provision for "effective enforcement" of the types of punishment enumerated in the Convention.[80] Hence, the Convention creates blanket substantive laws but does not address their application and enforcement.

C. The United States' (and Other) Objections to the Convention's Criminal Provisions for Copyright

The Convention drafters recognized that their proposed treaty would be met with intense scrutiny.[81] Problems acknowledged by the drafters include: the

---

[73] *Id.*; *see also* Berne Convention for the Protection of Literary and Artistic Works, July 24, 1971; TRIPS Agreement; and WIPO Copyright Treaty, December 20, 1996.

[74] *See* Convention, *supra* note 69.

[75] *Id.*

[76] *Id.*; *see also Explanatory Report*, *infra* note 117, *available at* http://www.conventions.coe.int/Treaty/en/Reports/Html/185.html (last visited Mar. 1, 2002) (explaining that the clause was not intended to extend the protection that authors, film producers, performers, phonogram producers, broadcasting companies, and other right holders have to those that are not eligible under their own domestic copyright laws or under international copyright agreements).

[77] *Id.*; *see also* 17 U.S.C. § 506 (2000); 18 U.S.C. § 2319 (2000).

[78] *See* E-Commerce News: Convention on Cybercrime, *available at* http://www.wilmer.com/docs/news_items/ACFD9E.pdf (last visited Nov. 4, 2001) (noting that "commercial scale" is never defined in the Convention, leaving the phraseology open to questions of whether personal-use file-sharing is to be automatically criminalized as well as infringement for profit).

[79] *See* Convention, *supra* note 69, art. 10.1 (last visited Nov. 4, 2001) ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright.").

[80] *See* TRIPS, *supra* note 65.

[81] *See* Council of Europe, *Big Brother or Free-for-All—How Can the Law Strike a Balance?*, *available at* http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/cybercrime/e_bigbrother.asp#topofpage (last visited Nov. 4, 2001) (observing an ensuing "clash" in the

potential denial of civil liberties;[82] overreaching government power;[83] lack of privacy rights;[84] reduction of the free-flow of information by tighter restraints;[85] and imposition of third-party content liability for Internet Service Providers ("ISPs").[86]

Some of the most intense criticisms of the Convention come from organizations such as the Global Internet Liberty Campaign ("GILC"),[87] which argue that the Convention threatens free speech and privacy rights by improperly and dangerously extending the reach of the policing authority of national governments.[88] Additionally, GILC asserts that the broad extension of copyright crimes in Article 10 is objectionable, because it is not yet established that criminal penalties are the appropriate remedies for instances of copyright infringement in the majority of States.[89] Furthermore, Article 10 allows for mutual assistance in prosecuting copyright crimes without dual-criminality. However, when one country deems an instance of copyright infringement to be a crime and another country does not, how can they work together to prosecute that offense?[90]

Convention between individual rights to free speech and privacy, state rights to combat cybercrime, society's need for secure information networks, and a general corporate need to protect its business interests in an electronically-driven market).

[82] *See* ACLU/EPIC, *Comments on CoE Cybercrime Convention*, at http://www.pili.org/lists/piln/archives/msg00777.html (last visited Nov. 4, 2001) (noting that Article 19.4 of the Convention appears to require countries to adopt laws that force users to provide their encryption keys and the plain text of the encrypted files, which raises the issue of the right against self-incrimination).

[83] *See* Associated Press, *Cybercrime Treaty Raises Concern*, at http://www.jsonline.com/bym/tech/ap/oct00/ap-europe-cybercri102800.asp (last visited Nov. 4, 2001) (remarking that the Convention gives law enforcement officials a basis to investigate any crime where evidence may be stored on a computer, and that it also gives the government an overreaching power to collect private information).

[84] *Id.*

[85] *See* Convention, *supra* note 69.

[86] *Id.*

[87] *See* Global Internet Liberty Campaign, *Statement of Principles at* http://www.gilc.org/about/principles (last visited Nov. 4, 2001). Primarily a privacy watchdog group, the GILC advocates, among other things, ending prior censorship of Internet communication, sustaining free speech on the Internet and in other digital communications with limited government restrictions, and the unrestricted encryption and protection of digital information. *Id.*

[88] *See* GILC Member Letter, *at* http://www.gilc.org/privacy/coe-letter-1000.html (last visited Nov. 4, 2001) (posting a letter objecting to the Convention that was signed by the following groups: American Civil Liberties Union (US), Association for Computing Machinery (International), Associazione per la Libertà nella Comunicazione Elettronica Interattiva (IT), Bits of Freedom (NL), Canadian Journalists for Free Expression (CA), Center for Democracy and Technology (US), Computer Professionals for Social Responsibilities (US), Crypto-Rights Foundation (US), Cyber-Rights & Cyber-Liberties (UK), Derechos Human Rights (US), Digital Freedom Network (US), Digital Rights (DK), Electronic Frontier Foundation (US), Electronic Frontiers Australia (AU), Electronic Privacy Information Center (US), Equipo Nizkor (ES), Feminists Against Censorship (UK), FITUG e.V.(DE), Foundation for Information Policy Research (UK), Human Rights Network (RU), Internet Freedom (UK), Internet Society – Bulgaria (BG), Internet Society, IRIS – Imaginons un réseau Internet solidaire (FR), Kriptopolis (ES), Liberty (UK), The Link Centre, Wits University, Johannesburg (ZA), NetAction (US), Networkers Against Surveillance Taskforce (JP), Opennet, PGP en Français (FR), Privacy International (UK), quintessenz (AT), Verein für Internet Benutzer (AT), and XS4ALL (NL)).

[89] *Id.* "New criminal penalties should not be established by international convention in an area where national law is so unsettled." *Id.*

[90] *Id.*

Besides the problems that lie within the Convention document, there are many objections to the procedural manner in which the Draft Convention was drawn.[91] Only law enforcement groups were involved in the drafting of the language, without any non-governmental organization or industry input.[92] Without consumer or industry input, the document lists the rules but lacks the economic realities of enforcement. Additionally, the Final Draft was only made available on the Internet for general public comment in April, 2000, roughly four years after drafting began.[93]

The Convention, most notably, does not provide for "effective" enforcement of the laws and penalties it creates. When compared to the TRIPS agreement, promulgated five years before it, the Convention seems to take a step back by not specifying the level of penalties and other remedies available. What remains is a virtually ineffective set of laws designed to apply to everyone but actually enforceable upon few. The Convention takes a harsher tone than TRIPS, and threatens more, but fails to ultimately and effectively punish copyright infringers. At the same time, the Convention overreaches, giving great power to law enforcement to reach into databases, retrieve private information, and prohibit content. Thus, there is less protection of copyright offered than United States citizens already receive via TRIPS, despite the illusion of harsher standards.

III. CONGRESS SHOULD REFUSE TO RATIFY THE CONVENTION TREATY IN ITS CURRENT FORM

On November 23, 2001, the Convention on Cybercrime was opened for signature in Budapest, Hungary.[94] The United States signed only after provisions banning racist and xenophobic content were dropped.[95] Concerns with the Convention, well

---

[91] *See* ACLU/EPIC Comments on CoE Cybercrime Convention, *supra* note 82 (commenting that while the Convention's proposed laws require transparency and harmonization, the manner in which they were promulgated was rather opaque, with extremely limited opportunity for public comment or criticism).

[92] *Id.*

[93] *See* The Council on Europe, *The Draft International Convention*, *available at* http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cybercrime/e_projconvention.asp#TopOfPage (last visited March 22, 2002) (providing a timeline for drafts that stretches four years).

[94] *Id.* The following thirty countries have signed the Convention: Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Malta, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the "Former Yugoslav Republic of Macedonia", Ukraine, the United Kingdom, Canada, Japan, South Africa, and the United States. *Id.*

[95] Paul Meller, *Hate Crime Footnote Added to Council of Europe Cybercrime Treaty*, InfoWorld Daily News, November 9, 2001. Such provisions would clash with the First Amendment freedom of speech guarantees in the U.S. Constitution. *Id.* However, a "footnote" or "protocol" has been added to the Convention, allowing countries who agree to it to sign on and those who don't to refuse, while still abiding by the main text of the Convention. *Id.* Those who refuse to sign onto the protocol, however, are still expected to enforce the racist-content bans when such content originates in their country and is aimed at a country that makes them illegal. *Id. See also* Council of Europe, *Elaboration of an Additional Protocol to the Convention on Cybercrime, Dealing with the Criminalization of Acts of Racist or Xenophobic Nature Committed through Computer Networks at* http://www.legal.coe.int/economiccrime/cybercrime/AP_Protocol(2002)5E.pdf (last visited Mar. 1, 2002). CoE suggests that many countries are in strong favor of criminalizing racist and xenophobic

voiced in the months prior to the signing, remain high as the Convention merely needs ratification before becoming substantive United States law.[96]

Why is the Convention so threatening to the United States' interests? Primarily, the Convention establishes criminal penalties for copyright infringement—actions not traditionally considered to be deserving of criminal punishment. Dmitri Skylarov was arrested under the Digital Millennium Copyright Act, but Adobe quickly dropped its support of the prosecution. Why? Adobe received bad publicity for punishing the "poor foreigner" who was only doing something in America that was perfectly legal in his own country.[97] The United States is not ready to criminalize people like Skylarov. What he did was legal in his own country, and while copyright infringement is a serious offense and can cost copyright holders millions of dollars, few United States citizens accept it as criminal on the same level as fraud or embezzlement. College students everywhere downloaded songs off of Napster.[98] Should the United States make an example out of these kids? While staunch defenders of copyright protection shout "yes," the economics of enforcement may weigh against such prosecutions.

The CoE seems to want to "get things done" without answering the most important question: How will it all work? The copyright laws offered by the Convention seek to bind all signatory countries to vague enforcement protocols. Copyright laws are already in effect in the United States—through our own statutes, TRIPS, WIPO, and other international agreements.[99]

---

content. *Id.* The protocol, then, is intended to be an extension of the Convention's scope of substantive, procedural, and enforcement rules in order to additionally prohibit "such behaviour." *Id.* "Racist or xenophobic material" is defined by CoE as "any written material, any image or any other representation of thoughts or theories, which advocates, promotes, incites (or is likely to incite) acts of violence, hatred, or discrimination against any individual or group of individuals, based on race, colour, (religion, descent, nationality), or national or ethnic origin." *Id.* Expression of the intent to be bound by the protocol is evidenced by either signature without reservation as to acceptance or by signature subject to acceptance and followed by acceptance. *Id.* However, any country has the option to reject their acceptance of the protocol by notifying the CoE Secretary General. *Id.*; *see also* Edouard Launet, *Council of Europe Secretary General: The aim is to harmonise criminal law* LIBERATION March 9, 2002 *at* http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cybercrime/e_InterviewSGLiberation.asp#TopOfPage (last visited Mar. 12, 2002) (interviewing the Secretary General of the CoE). The CoE Secretary General noted that an additional protocol that would criminalize the dissemination of terrorist messages may be drawn, and that CoE was in the process of assembling a committee of terrorism experts to gain their opinion on such a protocol. *Id.*

[96] *See* European Forum on Harmful and Illegal Cyber Content, *available at* http://press.coe.int/cp/2001/884a(2001).htm (last visited Mar. 1, 2002). In a move contradictory to United States free speech policies and indicative of CoE's enforcement priorities, CoE announced on November 28, 2001 that they had organized a European forum on harmful and illegal cyber content. *Id.* CoE intended to bring in experts in content-regulation fields to establish procedures for determining what would be allowed legally on the Internet. *Id.* The focus of the forum dealt with combining the efforts of the public and private sectors to regulate "offensive" content such as child pornography, racist statements, and xenophobic sites. *Id.*

[97] *See* McMahon, *supra* note 16. Skylarov presented detailed anti-encryption instructions to hundreds of people, and his company dealt with the United States government on a regular basis. *Id.* Hence, it is difficult to seriously view him as innocent and completely oblivious to U.S. law. *Id.* In fact, several Russian programmers admitted that Skylarov bragged about breaking the law, and that he and Elcomsoft "were trying to push the limit." *Id.*

[98] *See* A & M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001).

[99] *See* TRIPS, *supra* note 65.

The United States should first take a hard look at its goals to determine the best way to accomplish them. Initially, Congress should determine whether the laws in place are sufficient and consist of an effective way to protect intellectual property holders. The real purpose of copyright laws is to encourage creativity and thus stimulate the economy with new products, not to overly punish those who violate the law by criminalizing violations at any cost. The drafters of the Convention, being mainly law-enforcement officials, lost sight of this goal despite their good intentions. It is difficult to see how imposing a prison sentence on a college student sharing music files with another student in Great Britain could be justified or viewed as reasonable. If Skylarov's arrest taught the United States anything, it may be that Americans do not necessarily want copyright infringement to be a criminal offense on the same level as embezzlement or assault.

The United States should look to other platforms for addressing copyright law harmonization outside of its existing laws and the new Convention. One such platform may be an economic trade agreement. The United States-Jordan Free Trade Agreement[100] is one of the first bilateral trade agreements to address intellectual property rights protection.[101] The initial question may be: Is a trade agreement a proper forum for the establishment of copyright laws? The answer is a resounding yes. The difference between the Jordan Free Trade Agreement and the Cybercrime Convention, insofar as copyright provisions are concerned, is the context in which they are presented.[102] The Convention, created mainly by the United States Department of Justice and other law enforcement officials, presents its two paragraphs of copyright infringement policies in the context of a harmonization treaty that covers the infinitely broad topic of "cybercrime." But copyright infringement, standing alone, is difficult to equate with stealing or arson as a "criminal" act for a majority of people unless it is placed in a more appropriate context where those people will be able to understand what makes criminal copyright infringement laws publicly justifiable. The Jordan Free Trade Agreement, in contrast to this, presents the issue in context of economic relations, as copyright protection ultimately affects consumers and valuable intellectual property rights. This premise should be presented in a context, such as that of an economic agreement that provides clear justification of the criminal consequences. Presenting criminal punishments for copyright infringement to the public in the context of preventing economic harm would likely lead to their acceptance more easily than doing so without a context or in a broad, all-encompassing one.

IV. CONCLUSION

Had the drafters of the Convention considered not only what the law and punishment would be, but also how to make the entire process effective at deterring copyright infringement, their rules would appear as more than scare tactics. Without

---

[100] U.S.-Jordan Free Trade Agreement, Oct. 24, 2000, *at* http://www.ustr.gov/regions/eu-med/middleeast/ textagr.pdf (last visited Nov. 4, 2001).

[101] *See id.* The Free Trade Agreement was scheduled to enter into force on December 17, 2001. *Id.* The most well-known trade agreement incorporating intellectual property rights protection is the aforementioned WTO Agreement. *See* TRIPS, *supra* note 65.

[102] *See* U.S.-Jordan Free Trade Agreement, *supra* note 100.

economic and practical considerations, the Convention stands as an ineffective tool with no force. One example of a potentially proper venue would be a trade agreement. With incorporation of substantive copyright provisions in its text, a trade agreement is a practical forum through which laws may be created and effectively enforced in the marketplace, the niche where copyright fits. Jordan adopted and ratified the WIPO Copyright Treaties, which protects copyrighted works in a digital network environment. In the "Enforcement of Intellectual Property Rights" section, the Jordan Free Trade Agreement sets out distinct and explicit protocols for enforcement, including fines sufficiently high to deter "with a policy of removing the monetary incentive to the infringer," seizure of suspected copyright goods, payment of compensatory damages to the right-holder and repayment of profits made by infringer to the right-holder.[103]

Another way to tackle the issue in a broader form may be to devote an entire international treaty to the subject of digital copyright infringement, so that the issue is not, as it is in the Convention, a smaller part of a larger ideal. This would put the proper perspective on the substantive and procedural laws and would lead to more focused enforcement efforts. First, the treaty would identify the interests and rights of individual and corporate copyright holders, specifically those of Internet users and website authors. Then, the treaty would establish substantive and procedural norms to which all signing countries could conform. Finally, such a treaty would reflect an international policy consensus on enforcement procedures, with carefully delineated guidelines as to what conduct is deserving of criminal punishment. Also included should be rules concerning how such punishments would be executed when one country's established laws differ from another, or in situations where one country has copyright laws and another does not.

Proponents of the Convention assert that it, and specifically the copyright provisions, are a brazen step forward in computer-user and network security, because harmonization is essential in a global and digital environment.[104] Without this harmonization treaty, they argue, American substantive and procedural law may clash with the laws of other countries, punishing those who would go free in their homeland and freeing those who would be punished.[105]

---

[103] *Id.*

[104] *See* Cyber-crime: The Law Moves In, *available at* http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cybercrime/e_intro.asp#TopOfPage (last visited Jan. 10, 2002). CoE sought to "bring legal and ethical standards into an area where—for good or ill, and in liberty's name—only the laws of the market have applied so far." *Id.* Additionally, the U.S. Department of Justice comments that a multilateral treaty such as the Convention, that erases jurisdictional obstacles that hamper international investigations and prosecutions of cybercrimes, is particularly desirable because of the United States' reliance on the Internet as a communication, business, and educational tool. *See* Dept. of Justice—FAQ's, *supra* note 18.

[105] One limited example of how clashing laws affect judgments in internet-crime cases may be found in the recent discussion of *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal 2001). In *Yahoo!*, a French Court found the Yahoo! Internet Company criminally liable for allowing nearly 1,000 Nazi and Third Reich objects to be sold on the Yahoo.com auction site, which is also linked to on the Yahoo.fr (France) site. *Id.* at 1184. Yahoo!, which is based in the United States, sought a declaratory judgment to make the French court's ruling unenforceable under U.S. law, arguing that banning such anti-Semitic materials would infringe impermissibly upon its First Amendment free speech rights. *Id.* at 1186. Concerned with the potential of "chilling protected speech that occurs simultaneously within our borders," Judge Jeremy Fogel opined:

Some Americans opposed to the Convention retort that the laws that the United States has enacted are sufficient, and that "new" laws (i.e., the Convention) are unnecessary.[106] This point of view is naïve, however, since it discounts the possibility that as the digital environment expands, American-owned businesses will increasingly be put at risk by infringers. This argument also does not take into account the variety of substantive and procedural laws that exist throughout the world, and it does not touch the question of whose system of laws should preside in the cyberworld. While such conflicts have already appeared in the Internet speech and encryption software arenas, one may anticipate that the same conflict will arise in all areas subject to cybercrime—including digital copyright infringement.

This Comment does not suggest that the Convention's goals of harmonization are wrong, or that its aims are off the mark. There must be harmonization and cooperation between nations in preventing and investigating digital copyright infringements that span borders in seconds. But, the United States cannot afford to sacrifice the cornerstones of its democracy in order to make music-loving college kids criminals.

In drafting a treaty that fails by both overreaching and shrinking from its goals, CoE attacks a very real problem by proposing an ineffective and uncertain solution. CoE should have treated the criminal copyright provisions of Article 10 with a determined aim at a deterrent effect.[107] The United States Congress should reject the Convention because of its faulty Article 10, as well as the entire document. Instead, legislation should be drafted that will specifically address harmonization of copyright infringement laws in a significantly broader form, such as within a trade agreement or by encompassing its own treaty. We cannot criminalize all copyright

---

> Absent a body of law that establishes international standards with respect to speech on the internet and an appropriate treaty or legislation addressing enforcement of such standards to speech originating within the United States, the principle of comity is outweighed by the Court's obligation to uphold the First Amendment.

Id. at 1193.

[106] At a Congressional hearing, Harris Miller, President of the Information Technology Association of America, testified:

> We don't believe the U.S. laws by and large need to be changed. There are a lot of other countries around the world where there are huge holes in the ability of those countries to prosecute cyber-criminals. So most of the work to be done is not necessarily in the U.S. code or in state laws. Most of the work that is to be done is around the world.

Security Risks in Electronic Commerce: Hearing Before the Senate Commerce, Science, Technology and Space Subcommittee, 108th Cong. (2001) [hereinafter Senate Hearing].

Bruce Schneier, Chief Technical Officer of Counterpane Internet Society, testified:

> We need old laws applied cleanly to the new environment, because the crimes are the same, the people are the same, the environment is the same. The techniques are different, but you don't want the same crime to be suddenly much worse or much better if a computer is used. Fraud is fraud, theft is theft. And just because the tool is different, doesn't mean the ramifications should change.

Id.

[107] *See* Janet Reno, *Statement by the Attorney General, Symposium of the Americas: Protecting Intellectual Property in the Digital Age* (Sept. 12, 2000), *available at* http://www.cybercrime.gov/ipsymposium.htm (last visited Jan. 10, 2001) (advocating the Justice Department's strong commitment to prosecuting cases and making sure that "serious IP criminals go to jail for significant prison terms" and that "[t]here is no safe place to hide.").

infringement, but we need to provide routine, international deterrence.[108] There is no doubt that there exists a need to prevent copyright infringement, but it must be done the right way.

---

[108] *See* Senate Hearing, *supra* note 106 (quoting Vinton Cerf, Senior Vice-President for Internet Architecture and Technology, WorldCom).

> For this to work on a global scale, there will have to be some degree of collaboration and work to make the laws of the national boundaries somehow be at least compatible, so that law enforcement can work across international boundaries. This is not new. It's just perhaps made more visible, more highlighted by the global nature of the Internet.

Id.