The Convention on Cyber-Crime: Should the United States Ratify?

I. INTRODUCTION

The Convention on Cyber-crime [hereinafter, the Convention] is the first international treaty to battle a relatively new area of crime that is feverishly spreading around the globe: cyber-crime.1 As the number of countries being affected by cyber-crime increases, the Council of Europe decided to address the issue by creating a Draft Convention on Cyber-crime.2 With the Draft Convention now complete, the Convention on Cyber-crime was presented on November 8, 2001 to foreign affairs ministers in Strasbourg.3 This was followed by an International Conference held in Budapest on November 23, 2001, where the Convention was “opened for signatures” for the first time.4 The signing ceremony was held in the Hungarian Parliament at 11:00 a.m. on November 23, 2001.5 At precisely 11:30 a.m. the Ministers (or their representatives) signed the Convention.6 The Convention includes forty-three European member states in addition to Japan, Canada, South Africa, and the United States.7 Although an international treaty combating cyber-crime is much needed, the question arises: is this the right treaty for the United States? Individuals in the United States who hold their civil liberties in high regard must be wary of the United States’ ratification of the Convention, as there are serious issues of whether the Convention goes far enough to protect individual rights.8 There are two competing interests facing the United States with respect to

4. See id.
5. See Budapest, supra note 3 and accompanying text. See also International Conference on Cybercrime and Signing Ceremony of the Council of Europe Convention on Cybercrime, at http://www.coe.int (last visited Nov. 5, 2002).
6. See Budapest, supra note 3 and accompanying text.
7. See Lawlor, supra note 1.
8. See id. See also Big Brother or Free-For-All—How Can the Law Strike a Balance?, at http://www.coe.int (last visited Nov. 5, 2002) [hereinafter Big Brother].
the ratification of the Convention: (1) society’s interest in protection from and prevention of crimes committed through the Internet and on computers, as well as society’s demand for secure networks; (2) the interest of those who wish to maintain their civil liberties, such as privacy and free speech, while on the Internet, and protections against self-incrimination as well as fourth amendment search and seizure provisions. While one would anticipate the consideration of both interests in the Convention, critics argue it does not appear to go far enough to protect civil liberties to the extent that citizens of the United States have come to expect.

This Note will analyze both the positive and negative implications that the ratification of the Convention may have on the United States. Before such an analysis can begin, the Note must outline several other issues. Part II of the Note will discuss a wide range of background information regarding cyber-crime. Section A of Part II will include a brief explanation as to the purpose of this Note. Section B of Part II will define cyber-crime and will also include examples of cyber-crime. Section C will explain the history of the Convention, including a description of the Council of Europe, why the Convention was created, the purpose of the Convention, and the role of the United States in drafting the Convention.

Part III of this Note will discuss the effect the Convention may have upon particular constitutional rights. This section will include a discussion as to whether the Convention infringes upon privacy rights, whether the Convention infringes upon protections against self-incrimination, whether the Convention will benefit the United States, and the need for the United States to combat cyber-crime.

Part IV will begin the analysis as to whether the benefit conferred upon the United States will outweigh the potential threat to particular constitutional rights. This section will also address the possible benefits the Convention may provide the United States and how the citizens of the United States will be affected by such benefits. More specifically, this portion will discuss society’s needs for secure communication networks

9. See Big Brother, supra note 8.
10. See Lawlor, supra note 1. See also Big Brother, supra note 8.
11. See infra Part III.
12. See infra Part II.
13. See infra Part II.A.
14. See infra Part II.B.
15. See infra Part II.C.
16. See infra Part III.
17. See infra Part III.
18. See infra Part IV.
19. See infra Part IV.
and the related interests of big business. This section will also discuss the disadvantages the Convention could impose upon the United States and how United States citizens will be affected by such disadvantages. The Note will then analyze, based upon prior discussion, whether or not the United States should ratify the Convention.

Finally, Part V of the Note will conclude with a recommendation to Congress and the President of the United States as to whether the Convention should be ratified.

II. LEGAL REACTION TO CYBER-CRIME

A. Why the Convention on Cyber-Crime?

The purpose of this Note is to evaluate the Convention and its possible positive and negative implications upon the United States and her citizens. After the positive and negative implications have been analyzed, a recommendation will be made as to whether the United States should ratify the Convention. The Note’s purpose would be served if referenced by Congress or the President of the United States in order to determine some implications of the Convention before a decision is made as to whether or not to ratify the Convention. Therefore, the final purpose of this Note is to be an additional aid to Congress or the President of the United States when deciding whether the United States should ratify the Convention.

B. What is Cyber-Crime: A Brief History

Although the term ‘cyber-crime’ implies crime occurring on the Internet or via the Internet, the Convention covers crime that not only occurs on or via the Internet, but also crimes that occur through the use of a computer and crimes that involve computers in general. The terms ‘computer crime,’ ‘computer related crime,’ ‘high-tech crime,’ and ‘cyber-crime’ are regularly interchanged with one another and therefore can have a similar meaning. For the purposes of this Note, the term cyber-crime will be used throughout, as it is the term the Council of Europe has chosen to refer to
such crimes.\textsuperscript{26} There is a distinction between computer specific crimes and traditional crimes performed with the aid of a computer.\textsuperscript{27} This Note refers to traditional crimes performed with the aid of a computer, as well as computer specific crimes.\textsuperscript{28}

Keeping in mind the interchangeability of various phrases when referring to cyber-crime, Black’s Law Dictionary defines “computer crime” as “[a] crime requiring knowledge of computer technology, such as sabotaging or stealing computer data or using a computer to commit some other crime.”\textsuperscript{29}

The ease of accessibility to information and communication networks benefits cyber-criminals.\textsuperscript{30} Such networks are far-reaching, inexpensive to access, and seemingly private.\textsuperscript{31} Misuse and abuse of computers began with the first wave of computer technology in the late 1940s.\textsuperscript{32} Computer crime intensified as computer technology allowed an increase in the use of computers in private and sensitive areas of society.\textsuperscript{33} Computer abuse first began in military systems, and then spread to the scientific arena, and finally to business and private applications.\textsuperscript{34} It seems inevitable that with ever-changing technology, computer crimes will only worsen. The sudden and massive increase in the use of computers has been the main contributor to the large and steadily increasing growth of cyber-crime, “exploiting modern technologies to the full[est].”\textsuperscript{35} Technology only increases the ability of criminals to commit crimes via the Internet.\textsuperscript{36}

As technology improves, computer crimes will grow in number and complexity.\textsuperscript{37} An enormous amount of people are using the Internet—in the

\textsuperscript{26} See The Convention, supra note 2.

\textsuperscript{27} See Communication from the Commission, supra note 25. A traditional crime performed with the aid of a computer refers to crimes that are committed by using the Internet and crimes that “call for improved co-operation and procedural measures.” Id. Computer specific crimes require legislators to constantly improve and bring up-to-date definitions of crimes in national criminal codes. See id.

\textsuperscript{28} See The Convention, supra note 2.


\textsuperscript{30} Communication from the Commission, supra note 25.

\textsuperscript{31} See id.

\textsuperscript{32} SLOAN, supra note 29.

\textsuperscript{33} See id.

\textsuperscript{34} Id.

\textsuperscript{35} Democracy at Risk, at http://www.coe.int (last visited Nov. 5, 2002).

\textsuperscript{36} See id.

\textsuperscript{37} See id. For example, it takes the police “eighteen months to investigate” a money-laundering operation, whereas it takes a criminal less than one minute to complete the crime. Id.
year 2000 the number of Internet users increased to over 350 million users world-wide.\textsuperscript{38} This number, though incredibly large, is not surprising, given that the price of computers and Internet access is going down while there has been an increase in accessibility.\textsuperscript{39} In addition, this number is increasing daily as technology improves, more computers are sold, and more Internet accounts are opened.\textsuperscript{40}

Increases in cyber-crime are unsurprising, considering how seemingly available the Internet and computers are for criminals, as the Internet provides inexpensive and worldwide communication in seconds, has few barriers and relatively no limitations.\textsuperscript{41} Characterized by ease of use, low cost, and a wide variety of capabilities, the Internet feels like home to many types of criminals, from those that are termed “hardened criminals” to those who are still on the brink of breaking the law.\textsuperscript{42}

Cyber-crime has been referred to by some as the “perfect crime” because cyber-crime can be committed anonymously and is not easily traceable.\textsuperscript{43} Cyber-crime is also a favorite to many criminals because the Internet is seldom policed.\textsuperscript{44} The crimes that occur on the web include: the spread of computer viruses; the creation, maintenance and distribution of child pornography and child pornography sites; piracy and fraud; and, although not technically a crime, the maintenance of websites promoting and encouraging racism.\textsuperscript{45}

The spread of computer viruses are frequently heard about through e-mail and sometimes on the news.\textsuperscript{46} Oftentimes, warnings are sent indicating e-mail users should not open particular e-mails because a virus is

\textsuperscript{38} See Riding the Web—Over 350 Million Surfers, at http://www.coe.int (last visited Nov. 5, 2002) [hereinafter Riding the Web]. The 350 million web users can be broken down to represent a large portion of the world: the United States counts for 158 million users, Europe has 95 million users, Asia and the Pacific contribute 90 million users, there are 14 million users in Latin America, and 3.5 million users in Africa. See id.

\textsuperscript{39} See id.

\textsuperscript{40} See id. In fact, more than 60 million computers were sold across the world in the year 2000, demonstrating a growth rate of fifteen percent annually. See id. Internet sales account for $650 billion in 2000 and it is estimated that this figure will have tripled by 2002. See id. In the last few years, well over twenty-eight million websites were designed and implemented. See Riding the Web, supra note 38.

\textsuperscript{41} See id.

\textsuperscript{42} See id.

\textsuperscript{43} See Running the Gamut, at http://www.coe.int (last visited Nov. 5, 2002).

\textsuperscript{44} See id.

\textsuperscript{45} See id.

\textsuperscript{46} A computer virus is a “mini-programme which multiplies automatically through another programme and spreads at epidemic speed without the user’s knowing it.” Running the Gamut, supra note 43.
attached. Computer viruses are capable of mass destruction such as eliminating files, damaging hardware, or worse, incapacitating entire networks. The total damage done around the world has been estimated at approximately ten billion dollars. The Federal Bureau of Investigation (FBI) estimates that there are at least fifty viruses, worms, and Trojan horses per week that affect computer users in all forms. These computer viruses, worms, and Trojan horses often render systems useless, leaving the victims wondering how this criminal be punished, especially when the criminal is hard to trace.

Another major criminal activity involving the use of computers is child pornography. Child pornography is actively increasing on the Internet. The head of the French police division responsible for investigating offenses against persons and property, Inspector Jean-Francois Cosse, estimates there are anywhere from three hundred thousand to five hundred thousand pornographic photos of children on the Internet that are easily accessible and available for distribution.

Though not widely reported or even an actual criminal activity, the issue of racism on the Internet is addressed on the Council of Europe’s webpage under the section for the Convention. Reports indicate that the number of racist sites on the Internet has increased from 160 in 1995 to 2,500 in 2000.

---

47. See id.
48. See id. For example, the popular “I Love You” virus was sent via the Internet to infect computers, and the destruction that occurred was overwhelming. See id. Sent on May 4, 2000 from the Philippines, the “Love Bug” bit computer users all around the world, including Asia, Europe, and the United States. See id. Targets hit ranged from individual computer users to businesses and governments. See id. In fact, sixty-five percent of American businesses with over two hundred employees were infected with the virus; in addition, the Swiss Government’s e-mail system was rendered useless for over twenty-four hours. See id. This was just a sampling of the damage done and those affected by it.
49. See Kelly Cesare, Comment, Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution, 14 TRANSNAT’L LAW. 135, 145 (2001).
50. See Running the Gamut, supra note 43. “Worms,” similarly to viruses, “spread from computer to computer, without even needing to transmit through another programme.” Id. “Trojan horses” are described as “full-scale programme[s], which can take your computer over at long range.” Id.
51. See id.
52. See id.
53. Child pornography is also known as pedophilia or pedopornography. See Lyombe Eko, Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation, 6 COMM. L. & POL’Y 445, 457 (2001).
54. See Running the Gamut, supra note 43.
55. See id.
in the United States alone.57 Worldwide, the number of Internet sites that “openly encourage racial violence” has been estimated at 4,000.58 Although some countries have created and implemented safeguards to eradicate racism on the Internet, these safeguards are becoming less and less effective as each day passes.59

Another type of cyber-crime that is growing exponentially is the use of the Internet by pirates and Mafiosi.60 This new wave of criminals targets the weakest points in the computer systems of the world.61 Online fraud is leading to disorder on the Internet and destruction via the Internet.62 Although many countries, such as Russia, Japan, Switzerland and France, now have specialized police units to trace and capture these computer hackers, each of these countries has yet to beat such a new, high-tech crime wave.63

Although anyone can be a target and/or victim of cyber-crime, a survey of businesses in the United States indicates that the prime targets of computer hackers are business firms.64 Although big business seems to be the prime target, criminal computer hackers often go after individuals and public agencies as well.65 In the United States, the FBI has concluded that some five thousand of its computer systems are “highly vulnerable to cyber-crime, which has according to Ronald L. Dick, the FBI’s new

57. See id.
58. Id.
59. See id.
60. See Running the Gamut, supra note 43. For example, four hackers recently broke into the confidential files of fourteen hundred participants of the World Economic Forum in Davos. See id. These cyber-criminals gained access to a wealth of information of the world’s leading economic experts including credit card numbers and their respective expiration dates, private addresses, and cell phone numbers. See id. The potential damage that could come to these economic experts is disturbing and overwhelming, and the threat that remains to the rest of the world is potentially devastating. See id.
61. See id. For example, not long ago an organized gang of hackers from Russia and the Ukraine accessed over forty sites in the United States alone. See id. These hackers gained access to at least one million random credit card numbers. See id.
62. See id.
63. See id.
64. See Cyber-Crime—The Targets it Hits, the Damage it Does, at http://www.coe.int (last visited Nov. 5, 2002) [hereinafter Cyber-Crime—The Targets it Hits]. After being questioned, eighty-five percent of United States businesses say they have at some point been the targets of computer hackers. See id. In fact, The Communications Management Association completed a report in Great Britain, which concluded that one-third of the major businesses and public authorities in Great Britain have been victims of computer hackers. See id.
65. See id.
director, the capacity ‘to destabilize a country’s whole economy.’”66 In addition to the threat the FBI faces, the Pentagon’s systems were not only threatened, but actually invaded more than twenty-two thousand times in one year alone.67

Cyber-crime poses major problems not only because it is high-tech and its offenders are often anonymous and difficult to trace, but also because very few victims actually report the crimes.68 Major studies were performed in the United States and in Europe, which suggested that only one-third of victims actually report offenses.69 Cyber-crime is also an extremely expensive offense for those whose privacy is violated.70

As the offenses of cyber-crime increase, the public develops more concern for the threats this type of crime presents.71 “The calls for international co-operation between governments, police forces and courts are becoming more insistent ….”72 With the request for international cooperation in mind, one must first consider what each individual country is doing to declare its own war on cyber-crime.73 The European Union has responded to cyber-crime by issuing several legal instruments to the European Union Member States.74 There is clearly no debate that there is a growing need and a strong demand for legislation regulating computer crimes and prosecuting criminals.75 Last March, at the Council of Europe’s Parliamentary Meeting, an American expert brought two key points to the Council of Europe’s attention: “[L]aws are needed to make cyberspace safe, and countries with inadequate laws will be less competitive on the

66. See id.
67. See id.
68. See Cyber-Crime—The Targets it Hits, supra note 64.
69. See id. This means that the offenses that are reported are just the beginning of a long list of offenses likely committed. See id.
70. See id. Fraudulent use of credit cards leads to over $400 million in damages each year, and virus attacks result in losses of approximately $12 million annually. See id. One report indicates that firms that have patents and trademarks stolen are incurring costs of $250 billion dollars per year. See id.
72. Id.
73. See id. A United States firm, McConnell International, surveyed fifty-two countries around the world in order to determine what each respective country’s laws were regarding direct and indirect prosecution of cyber-crimes. See id. McConnell International’s survey concluded that only ten countries of the fifty-two had significantly altered their laws in order to prosecute cyber-crime, another ten of the fifty-two countries had only partially updated their laws, and thirteen others have intentions to update their laws in order to better respond to cyber-crime. See id.
74. See Communication from the Commission, supra note 25.
75. See id.
new economic markets." There is an obvious desire for international legislation because the Internet has no frontiers or no barriers; criminals in one country can create victims in another country. Without international cooperation it would be very difficult, if not impossible, to prosecute those criminals who commit offenses in other countries via the Internet. While there is a great demand for an instrument like the Convention, whether or not this piece of legislation is effective is still being debated by many.

Although the list of various types of cyber-crimes is an extensive one, this article will focus on the cyber-crimes that the Convention expressly mentions. The cyber-crimes mentioned by the Convention will be elaborated upon in greater detail later in this Note.

C. The Council of Europe and the Convention on Cyber-crime.

1. Who is the Council of Europe?

Once suggested by Winston Churchill, among others, the Council of Europe is an international organization located in Strasbourg. The Council of Europe is comprised of forty-three democratic countries, each of which is located in Europe. An intergovernmental organization, the...
Council of Europe aims “to protect human rights, pluralist democracy and the rule of law; to promote awareness and encourage the development of Europe’s cultural identity and diversity.” The work of the Council of Europe fosters European Conventions and agreements in which member states may then “harmonize and amend their own legislation to comply with” the European Conventions or agreements formulated by the Council of Europe. The Council of Europe covers many important issues that are prominent in European society today.

2. How/Why Was the Convention on Cyber-crime Created?

The very first recommendation and report on cyber-crime, Recommendation No. R. (89) 9, was presented to the Council of Europe in 1989. Subsequently, the Council of Europe issued a recommendation concerning the substantive law of computer crimes. Recommendation No. R. (89) 9 asked member states to consider computer crimes when developing their domestic legislation. The report on cyber-crime, which was also included in Recommendation No. R. (89) 9, gave legislators guidelines to follow when considering computer crimes. In fact, the recommendation contained what has been referred to as a “Minimal List” and an “Optional List.” Recommendation No. R. (89) 9 resulted in a plethora of computer laws across the member states of the Council of
Europe.91 Recommendation No. R. (89) 9 also opened the door for the second recommendation, Recommendation No. R. (95) 13.92 Recommendation No. R. (95) 13 was presented to and adopted by the Council of Europe in 1995, bringing to life the idea of the Convention.93 For four years, the Council of Europe has been working on a convention to attack cyber-crime.94 During these four years, numerous experts have not only been consulted, but have played a key role in the drafting of the Convention.95 In February of 1997, the Council of Europe created a new committee: the Committee of Experts on Crime in Cyberspace.96 The Council of Europe’s Committee of Ministers, sought out to create a “binding legal instrument, and to consider questions relating to offenses, substantive criminal law, the use of coercive powers and jurisdiction in cyber-crime cases.”97 The Committee of Members sought out for the Committee of Experts on Crime in Cyberspace to evaluate each of the above referenced issues on an international level as well.98 After the draft was created, the text of the draft was “declassified” making the draft available to the public via the Internet.99 The Council of Europe “declassified” the draft Convention in hopes of gaining the relevant and valuable opinion of those closely affected by the Convention, such as professionals in the computer industry as well as the opinion of Internet users.100 In March of 2001, the Parliamentary Assembly contributed to the creation and adoption of the draft by extending an invitation to experts from around the globe to a special hearing.101 Subsequently, in its April 2001 session, the Committee of Ministers asked the Assembly for an

91. See id.
92. See Sussmann, supra note 86.
93. See id.
94. See The Convention, supra note 2 and accompanying text.
95. See Budapest, supra note 3. Such experts have come from the Council of Europe countries as well as the United States, Canada, Japan and many other countries outside of the Council of Europe. See id.
97. See id.
98. See id. The Committee of Experts on Crime in Cyberspace held ten plenary meetings during the span of two and one half years, April 1997 and December 2000; the drafting committee met roughly fifteen times during this period. See id.
100. See id.
101. See id.
opinion on the draft. After several amendments were in place, the Assembly adopted the draft convention on Cyber-crime at this April 2001 session. The Assembly’s vote to adopt the draft allowed for the draft to be given back to the Committee of Experts on Crime in Cyberspace to write a final draft. After twenty-seven drafts and four years, the Committee of Ministers of the Council of Europe approved, thereby adopting the Convention on November 8, 2001. However the Convention will not be effective or enforceable until five states, three of which must be Council of Europe members, ratify the treaty. In fact, the Council of Europe has extended an invitation to all member states and non-member states that participated in the creation of the Convention.

3. What’s the Point: The Purpose and Objectives of the Convention on Cyber-crime

Although the Convention is said to have a plethora of purposes, its main focus is to combat cyber-crime on an international scale, to unify the nations against computer crimes, and to harmonize laws universally regarding offense, prosecution, and punishment. The apparent need for an international treaty is founded on the premise on which many experts concur: cyber-crime is a new category of crime that requires a separate legal framework in order to address emerging technologies that are being utilized to commit traditional crimes. Supporters of the Convention believe the Convention is the only way to bring countries together against cyber-criminals in hopes of creating a more effective way to combat cyber-
crime. The Convention is said to maintain such successful law enforcement because the Convention standardizes computer crime statutes and requires all signatory states to work with one another. The text of the Convention is intended to protect network and user security. The Convention covers not only substantive and procedural law, but also provides for international instruments to be implemented, including international levels of jurisdiction and the international use of coercive powers.

The main objective of the Convention, which is stated in the preamble, “is to pursue a common criminal policy aimed at the protection of society against Cybercrime, especially by adopting appropriate legislation and fostering international cooperation.” The Convention is said to allow many countries to work together against defendants who affect many nations at one time or defendants who commit crimes in one nation while physically present in another nation. The Convention addresses substantive law, procedural law, and jurisdictional aspects for all signatory states.


The Convention covers a wide range of substantive criminal law in Chapter II, Section I. Such criminal offenses are separated into five main “Titles,” covering crimes such as illegal access, illegal interception, data interference, system interference and misuse of devices; criminal activity such as forgery and computer fraud; crimes such as producing,
possessing, or making available to others child pornography;\textsuperscript{121} as well as “wide scale distribution of pirated copies of protected works;”\textsuperscript{122} and finally, this section covers responsibilities of signatories of the Convention in relation to any attempt to aid or abet criminals under the Convention.\textsuperscript{123} It is important to note that for an activity to be considered criminal, the activity must satisfy two conditions: first, the activity or offense must be committed deliberately, and second, the activity or offense must be committed “without right.”\textsuperscript{124}

Only when these two conditions are met will an activity be deemed a criminal offense under the Convention.\textsuperscript{125}


Section 2 of the Convention addresses the procedural law, which will govern all signatory states.\textsuperscript{126} This section of the Convention is divided up into five main titles.\textsuperscript{127} The procedural law section includes rules, which the Convention supporters say, make it easier for police to investigate and solve cyber-crime.\textsuperscript{128} These rules include the new idea of “mutual
assistance” among the signatory states. Such new forms of “mutual assistance” are the subject matter of Title 1 through Title 5. Title 1 covers the common provisions of Section 2. Title 1 discusses the legislation signatories must adopt, when and what types of procedures will be applied to criminal offenses by signatories, and conditions and safeguards. Title 2 focuses on the expedited preservation of stored computer data and partial disclosure of traffic data. Title 3 addresses when and how signatories will adopt proper legislation to allow authorities to order production of certain items, such as: subscriber information from service providers, specified computer data, etc. Title 4 addresses the search and seizure of stored computer data by signatories. Finally, Title 5 discusses the real-time collection of computer data, including the real-time collection of traffic data and the real-time interception of content data. In order to further the mutual assistance and international cooperation necessary, the Convention “will enforce cooperation corresponding to powers defined in the convention and as a consequence the legal authorities and police in one country will be able to collect computer-based evidence for police in another ….” Such information will have to be transferred between signatories quickly in order to ensure success. Therefore, a contact network will be established and will operate around the clock to provide fast paced assistance to investigators. The provisions of mutual assistance within the Convention further support such a network.

c. Who Can Play? The Jurisdiction of the Convention on Cyber-crime

Section 3 of the Convention covers the complex matter of
Signatories must establish jurisdiction over any offense via legislative or any other necessary means. Such jurisdiction will apply when the offense is committed in the territory of the signatory’s country, on board a ship of the signatory, on board an aircraft of the signatory, or by one of the signatory’s nationals, “unless another state has territorial jurisdiction.”

\[198\]

\textit{i. The U.S. and the Council of Europe: The Role of the United States in Drafting the Convention on Cyber-Crime}

The United States Department of Justice and the United States Department of State, in addition to other government agencies, have played an important role in drafting the Convention. The Council of Europe extended an invitation to the United States originally to participate as an observer in 1989 and 1995 when the first recommendations were occurring. The United States was merely an observer at that time of the creation of the Convention.

Subsequently, the Council of Europe requested the United States actually participate in the negotiations regarding the Convention, and the United States agreed. Because the United States participated in the negotiations of the Convention, the Council of Europe has given the United States the right to become a signatory to the Convention. However, it is important to note that the United States is not required or bound to sign the Convention. Because the United States was an active participant in the negotiations of the drafting of the Convention, the Department of Justice concludes that “the United States has had a real voice in the drafting process.”

\begin{enumerate}
\item[139.] See The Convention, supra note 2, at ch. 2, § 3. See also Main Lines of the Convention, supra note 80.
\item[140.] See The Convention, supra note 2, at ch. 2, § 3. See also Main Lines of the Convention, supra note 80.
\item[141.] See The Convention, supra note 2, at ch. 2, § 3. See also Main Lines of the Convention, supra note 80.
\item[142.] See Frequently Asked Questions, supra note 124.
\item[143.] See id.
\item[144.] See id.
\item[145.] See id.
\item[146.] See id.
\item[147.] See id.
\item[148.] Frequently Asked Questions, supra note 124.
\end{enumerate}
III. ARE “THE PEOPLE” IMPACTED?: THE CONVENTION ON CYBER-CRIME AND UNITED STATES CONSTITUTIONAL RIGHTS

Many organizations have spoken out actively against the Convention. Groups such as the Global Internet Liberty Campaign, the American Civil Liberties Union, as well as Privacy International each agree that the Convention poses a serious threat to several constitutional rights that many American citizens hold dear.

The Global Internet Liberty Campaign, which consists of twenty-two associations in nine European Countries, the United States, Japan, Australia and South Africa, is campaigning against the Convention. The Global Internet Liberty Campaign appreciates the need to harmonize laws worldwide in order to address the growth in cyber-crime. However, the Global Internet Liberty Campaign also believes the draft as it stands will jeopardize the protection of personal data and the right to anonymity. Privacy International and the American Civil Liberties Union support the concerns of the Global Internet Liberty Campaign. The concerns of these groups will be discussed in the next two sections.

149. See David Banisar et al., Comments of the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International on Draft 27 of the Proposed CoE Convention on Cybercrime, at http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm (last visited Nov. 5, 2002). See also Cesare, supra note 49, at 167.

150. The Global Internet Liberty Campaign is composed of numerous organizations coming together under this name to oppose the ratification of the Convention due to the lack of privacy assurances. See Mark Ward, Treaty Could Stifle Online Privacy, at http://news.bbc.co.uk/2/hi/sci/tech/1378482.stm (last visited Nov. 5, 2002).

151. The American Civil Liberties Union, founded in 1920, is a nonprofit and nonpartisan organization whose mission is to fight civil liberties violations all over the country. See Freedom is Why We’re Here, at http://www.aclu.org (last visited Nov. 5, 2002).

152. Privacy International, formed in 1990, is a human rights group based out of London, England. See http://www.privacyinternational.org (last visited Nov. 5, 2002). Privacy International considers itself a “watchdog” on governments and corporations trying to ensure that privacy rights of individuals, as well as other human rights, are not adversely affected. See id. Privacy International has organized campaigns all over the world “on issues ranging from wiretapping and national security activities, to ID cards, video surveillance, data matching, police information systems, and medical privacy.” Id.

153. See Banisar, supra note 149. See also Cesare, supra note 49, at 169.


155. See id.

156. See id.

157. See Banisar, supra note 149. See also Cesare, supra note 49, at 169.

158. See infra notes 159-248.
A. Does the Convention on Cyber-Crime Infringe Upon Privacy Rights of United States Citizens?

Before we can discuss whether the Convention infringes upon privacy rights of the United States citizens we must first consider the source of the right to privacy, whether the right to privacy is fundamental, and if the right to privacy is an enumerated right. The Supreme Court in *Griswold v. Connecticut* established the right to privacy.\(^{159}\) *Griswold v. Connecticut* is a 1965 case involving the criminal prosecution of Estelle Griswold, the Executive Director of Planned Parenthood and a physician.\(^{160}\) Griswold was prosecuted for providing married women with contraceptives; such distribution was illegal under a Connecticut statute at that time.\(^{161}\) In an opinion written by Justice Douglas, the Supreme Court held that the Connecticut law prohibiting the distribution and use of contraceptives was unconstitutional.\(^{162}\) Justice Douglas stated the basis for finding the Connecticut law unconstitutional was that the Connecticut law violated the right to privacy.\(^{163}\) The Supreme Court found that the right to privacy was a fundamental right, a right implicit in the “penumbra” of the Bill of Rights.\(^{164}\) Justice Douglas cited the First, Third, Fourth, Fifth, and Ninth Amendments; stating that together they create the right to privacy.\(^{165}\) When discussing the importance in recognizing the right to privacy, Justice Douglas stated: “Various guarantees create zones of privacy … [w]e have had many controversies over these penumbral rights of privacy and repose. These cases bear witness that the right of privacy which presses for recognition here is a legitimate one.”\(^{166}\)

Having now established that the right to privacy, although implied in the Constitution, is a fundamental right created through several amendments of

\(^{159}\) *Griswold v. Connecticut*, 381 U.S. 479 (1965). *See also* Erwin Chemerinsky, *Constitutional Law: Principles and Policies* § 10.3.2 (1st ed., 1997). It is significant to note that the right to privacy is recognized worldwide. *See* David Banis and Simon Davies, Article: Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1, 3 (1999). Most countries recognize privacy as a right in their constitutions. *Id.* “Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional treaties.” *Id.*

\(^{160}\) *See* Griswold, 381 U.S. at 480. *See also* Chemerinsky, *supra* note 159, at 658.

\(^{161}\) *See* Griswold, 381 U.S. at 480. *See also* Chemerinsky, *supra* note 159, at 658.

\(^{162}\) *See* Griswold, 381 U.S. at 485. *See also* Chemerinsky, *supra* note 159, at 659.

\(^{163}\) *See* Griswold, 381 U.S. at 485. *See also* Chemerinsky, *supra* note 159, at 659.

\(^{164}\) *See* Griswold, 381 U.S. at 484. *See also* Chemerinsky, *supra* note 159, at 659.

\(^{165}\) *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965). *See also* Chemerinsky, *supra* note 159.

\(^{166}\) *Griswold*, 381 U.S. at 484.
the Bill of Rights, now consider whether this right may be threatened by the Convention. Civil liberties groups, human rights groups, and many other individuals criticize the Convention, arguing that the method used to regulate the Internet may be detrimental to the right to privacy. Three groups sent a letter to the draft committee: the American Civil Liberties Union, the Electronic Privacy Information Center, and Privacy International. These three civil liberties groups expressed their concerns with the Convention and urged the Council of Europe to open the redrafting of the treaty to non-governmental organizations, such as themselves. These groups argue that the Council of Europe has “ignored” the imperative concerns many have regarding privacy. In fact the civil liberties groups stated “the treaty’s recommendations on protecting privacy are vague and do not go far enough.” More specifically, the civil liberties groups desire a greater separation of powers thereby creating distance between the police, who, for example, request the ability to obtain records from Internet service providers and the government officials who grant the police such powers. Under the Convention, the United States and European law enforcement agencies will be armed with new powers, allowing them to investigate and prosecute computer crimes. The concern is that giving these new powers to law enforcement will inevitably give the government, according to civil liberties organizations, too much power, and thereby violate the privacy rights of individuals. For example, the Convention will allow authorities to require individual persons to disclose their passwords, which allow them to access various encrypted material and databases. The Convention achieves this forced disclosure by requiring each signatory State to pass laws that guarantee “any person who has knowledge about … measures applied to secure

167. See id. at 484. See also CHEMERINSKY, supra note 159, at 659.
169. See Ward, supra note 150.
170. See id.
171. See id.
172. Id.
173. See id.
175. See id. This idea is supported by Gus Hosein, a senior fellow of Privacy International, who was quoted as saying, “[t]he increase of the powers of law enforcement waters down the protection of human rights.” See Joris Evers, Council of Europe Wraps Up Cybercrime Treaty, at http://www.cnn.com/2001/TECH/internet/05/29/cybercrime.treaty. idg/index.html (last visited Nov. 5, 2002).
176. See McCullagh, supra note 174.
computer data can be ordered to ‘provide all necessary information’ to allow law enforcement to access that data.” 177 The forced disclosure of passwords to law enforcement officials is currently only practiced in two countries: Malaysia and Singapore. 178 The Global Internet Liberty Campaign, in a letter to the draft committee of the Convention, referred to the Convention as “‘appalling,’ and warned that it handed law enforcement agencies sweeping powers to snoop and could seriously erode online privacy.” 179 It appears that an argument could be made that allowing little balance between these powers gives police easier access to private information and, with easier access, a greater potential for the abuse of various fundamental rights of United States citizens, rights that extend past the right to privacy and into other rights guaranteed to us through the Constitution, such as the protection against self-incrimination, fourth amendment search and seizure issues and due process of law. For example, if you are now required to turn over your password in order for the government to obtain information from your computer, e-mail account, or web page in order to prosecute you, how should this be reconciled with the privilege against self-incrimination? 180 This is a concern of many of the civil liberties groups opposing the enactment of the Convention. 181 “Forc[ing] ordinary Internet users to turn over decryption keys and other personal information to the government—[] will not only erode online privacy, but may also violate the right against self-incrimination.” 182 “The

177. David Banisar, *Love Letter’s Last Victim*, at http://online.securityfocus.com/news/39 (last visited Nov. 5, 2002). In his article, David Banisar argues that once the Convention is ratified, the “biggest victim of the ILOVEYOU worm … [is] … everyone’s basic right to privacy.” Id. Banisar argues further that “[w]hen the U.S. government cannot get a controversial policy adopted domestically, they pressure an international group to adopt it, and then bring it back to the U.S. as an international treaty—which obliges Congress to enact it.” Id. David Banisar is an attorney in the Washington D.C. area and the Deputy Director of Privacy International. See id.

178. See id.


180. See Cyber-Rights Groups Join Forces to Oppose Anti-Privacy Cybercrime Treaty, at http://www.aclu.org/Privacy/Privacymain.cfm (last visited Nov. 5, 2002) [hereinafter Cyber-Rights Groups].

181. See id.

182. Id. In a letter of comments to the U.S. Department of Justice and the Council of Europe in an effort to voice their concerns with the Convention, the American Civil
new document would permit government agents to invade the privacy of law-abiding citizens." Many groups are concerned, that we are heading in the direction of having “Big Brother” become a reality, in fact they believe the Convention is one step closer to a “global Big Brother.”

Another problem, various groups argue, is that the Convention will also require Internet providers and companies maintaining websites to accumulate various information about their users. Such provisions of the Convention would seemingly violate privacy rights of the affected individuals. One could argue that no longer would individuals be able to remain anonymous on the web, no longer would individuals be able to subscribe to various websites or mailings without the fear of another finding out. “What,” some will ask, “is the point in having passwords to protect private information, if the government can force you to reveal what it is you are maintaining as private?” When asked a similar question, Barry Steinhardt, the associate director of the ACLU and co-founder of the Global Internet Liberty Campaign, stated: “I think it’s [referring to the Convention] dangerous for the Internet. I think it will interfere with the ability to speak anonymously.”

Another problem with the Convention involving Internet service providers, argues Privacy International, is that the Convention will create situations where United States Internet service providers can be forced to comply with government officials regarding user information relating to matters legal in the United States, yet illegal in other states. The Privacy

Liberties Union, the Electronic Privacy Information Center, and Privacy International urged that the Convention be changed to protect against self-incrimination. See Banisar, supra note 149. These groups argued that the privilege against self-incrimination, a privilege that has been in existence since the Romans and later adopted by the United States through the Constitution, prohibits the government from forcing an individual to testify against himself. Id. The letter further argues that forcing an individual to testify against himself violates the European Convention on Human Rights. Id.

183. Cyber-Rights Groups, supra note 180.
185. See McCullagh, supra note 174.
186. See id. When discussing in their letter to the Department of Justice and the Council of Europe the provisions of the Convention that place heavy requirements on Internet service providers, the civil liberties group stated, “[w]ithout sufficient privacy and due process protections, which are noticeably lacking in the Treaty, these provisions threaten human rights.” Banisar, supra note 149.
188. Id.
189. See Evers, supra note 175. In their letter to the Department of Justice and the Council of Europe, the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International, expressed great concern for the mutual assistance provisions of the Convention:
International spokesperson, Gus Hosein, cites hate speech as an example of such a situation. Mr. Hosein indicates that an Internet service provider, under the Convention, can be required to cooperate with German authorities by giving them information about a customer, meanwhile the customer is protected here in the United States by the Constitution. Such a requirement for Internet service providers is rather burdensome. Internet service providers, according to The World Information Technology and Services Alliance, could also be held responsible for third party actions, in addition to the heavy data-preservation requirements of Article Seventeen of the Convention. Requiring so much of Internet service providers could inevitably lead to more restrictive sign up policies for individuals to use the web or for individuals and companies to maintain their own webpage. In turn, are we looking at the Convention as a body of law that will restrict the use of the Internet all together? Unfortunately, we will have to wait and see how the impact of the Convention will affect individual usage of the Internet in the United States.

Even though the drafters of the Convention, after receiving great pressure from civil liberties and human rights groups such as the Global Internet Liberty Campaign, the American Civil Liberties Union, and Privacy International, incorporated a few provisions in the Convention which “limit[ed] surveillance to criminal investigations and added some safeguards to civil liberties, the groups are still dissatisfied. ‘But it’s still not enough,’” said the Deputy Director of Center the for Democracy and Technology. The Director added, “[u]nfortunately, it remains a

We remain deeply concerned with the draft treaty’s failure to consistently require dual criminality as a condition for mutual assistance. No nation should ask another to interfere with the privacy of its citizens or to impose onerous requirements on its service providers to investigate acts, which are not a crime in the requested nation. Governments should not investigate a citizen who is acting lawfully, regardless of whatever mutual assistance conventions are in place.

Banisar, supra note 149.

190. See Evers, supra note 175.
191. See id.
193. See id. Article Seventeen of the Convention requires Internet service providers to log traffic data and to maintain logs for government agencies to use when pursuing cybercriminals. See id.
194. Lemos, supra note 105.
195. Id.
196. James X. Dempsey is Deputy Director of the Center for Democracy and
fundamentally imbalanced document. While privacy issues received somewhat more attention in the final stages of the process, the treaty does not have the specificity needed for meaningful privacy protection in the face of increasing surveillance power of this new technology.”\(^\text{197}\)

The Global Internet Liberty Campaign, representing the American Civil Liberties Union, Privacy International, and twenty-one other civil and human rights groups, frustrated with the Council of Europe turns also to governments worldwide making a strong plea in the name of privacy: “We call on governments around the world to reject the treaty because it does not provide enough protection to fundamental human rights.”\(^\text{198}\)

**B. How will the Convention on Cyber-Crime Benefit the United States and her citizens?**

Although the civil liberties groups and human rights groups have many valid concerns with the Convention and have compelling arguments for why the Convention is detrimental to the right to privacy, is the Convention really all that bad? Why would forty-three European member states as well as Japan, Canada, South Africa, and the United States join together to create such an international coalition for the sake of increasing government powers in order to better regulate what individuals are doing, thereby violating privacy? There are many valid reasons why the Convention was drafted, namely the need to fight cyber-crime or succumb to this new-age criminal activity. The purpose for the Convention has been previously discussed, let us now turn to what benefits are in store for the United States as a result of the Convention.

The United States Department of Justice answered such a question in response to frequently asked questions about the Council of Europe Convention on Cybercrime.\(^\text{199}\) One must acknowledge how vital computers are now to our everyday lives, the running of our businesses, and our governments. Only after such an acknowledgement can we begin to understand the benefits and protections the Convention will bring to our

---

Technology in Washington D.C. See *id.*

197. *Id.*


199. See Frequently Asked Questions, supra note 124. The direct response given by the Department of Justice states:

If the United States were to become a party to this Convention, it would directly benefit by having better methods of obtaining international assistance from other parties in computer-related crime cases, particularly because the other parties to the Convention would have similar minimum definitions of computer crimes and the domestic procedural tools needed to investigate those crimes.

*Id.*
society as a whole. At this time cyber-crime poses serious threats to our lives and our country.\textsuperscript{200} For example, some types of computer crimes target our utilities, communication companies, and transportation abilities.\textsuperscript{201} In addition, cyber-criminals are also committing “traditional crimes, including fraud copyright infringement, and distribution of child pornography.”\textsuperscript{202} Therefore, an international tool, such as the Convention, can potentially eliminate many of the “procedural and jurisdictional obstacles” that prevent the prosecution of cyber-criminals.\textsuperscript{203} The Convention, according to the Department of Justice, “breaks new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of cyber-crime.”\textsuperscript{204} The Convention furthers the ability to prosecute cyber-criminals, and thereby deter cyber-crime, by requiring all signatory countries to implement minimum substantive offenses relating directly to computer crime, requiring all signatory countries to put into place procedural laws allowing the investigation of computer crimes, and finally the Convention establishes a means for international support during investigation and prosecution of cyber-criminals.\textsuperscript{205} 

[For example,] take the recent investigation of the Love bug virus. … Although our investigators continue to work closely with investigators in the Philippines, international coordination would have proceeded more quickly and effectively had there existed common computer crime laws between our countries.\textsuperscript{206}

Without an international tool to unify nations against cyber-crime, the criminals will have free reign when it comes to committing crimes across international boarders.

The civil liberties and human rights groups argue that the Convention may violate the protections against self-incrimination and the right to privacy by forcing individuals to surrender their passwords or other encrypted information to authorities.\textsuperscript{207} However, the Fourth Amendment,\textsuperscript{208} as well as the Fifth Amendment,\textsuperscript{209} still exist and are as

\begin{itemize}
  \item \textsuperscript{200} See id.
  \item \textsuperscript{201} See id.
  \item \textsuperscript{202} Id.
  \item \textsuperscript{203} Id.
  \item \textsuperscript{204} See id
  \item \textsuperscript{205} Frequently Asked Questions, supra note 124.
  \item \textsuperscript{207} See supra notes 168-184 and accompanying text.
  \item \textsuperscript{208} See U.S. CONST. amend. IV.
  \item \textsuperscript{209} See U.S. CONST. amend. V.
\end{itemize}
powerful as ever. Patricia Bellia argues “[t]he convention is not designed to undermine privacy protection.” In fact, the Convention maintains the privacy protections that exist via the Fourth Amendment of the Constitution and the penumbras of the Bill of Rights. Bellia further explained, “[f]or example, if the United States signed the treaty, it couldn’t do anything to undermine the Fourth Amendment.

Another argument advanced against the enactment of the Convention by civil liberties and human rights groups is that the Convention could require an individual to be prosecuted for something that is illegal in one country, yet legal in her own country. The groups opposing the Convention call for a dual criminality requirement with regard to mutual assistance. This would require that the activity be illegal in both the country affected and the country of citizenship before the individual is prosecuted. Keeping in mind, however, that the objective of the Convention is to create similar laws across the nations, it is hard to believe that such an occurrence is likely to happen. Once the Convention is enacted and signatory states enforce necessary laws to comply with the Convention, most states will be prosecuting for similar acts. Therefore, what is illegal in one country will most likely be illegal in another. However, there may still be occurrences where the laws differ. In such a situation one must reflect upon the meaning of “without right” and what the Convention requires in order for the activity to be deemed a criminal offense before making such hasty conclusions that individuals will be prosecuted for an act that is legal in their own country. “Without right” is defined in the Draft Explanatory Notes of the Convention as “conduct undertaken without authority.” Furthermore, committing the act “without right” is a condition that must be met before the activity is deemed a criminal offense. Therefore, if an

210. Patricia Bellia is an assistant professor of law at Notre Dame Law School and is a former attorney with the United States Department of Justice. See Lemos, supra note 105. Bellia is also an expert “in the jurisdictional problems in prosecuting Internet crimes.” Id. Bellia argues that privacy issues with the Convention are “overstated.” Id.
211. Id.
212. See id.
213. See id.
215. Lemos, supra note 105.
216. See supra notes 124, 189-93 and accompanying text.
217. See supra notes 124, 189-93 and accompanying text.
218. See supra notes 124, 189-93 and accompanying text.
219. See supra notes 124, 189-93 and accompanying text.
220. See supra notes 124, 189-93 and accompanying text.
221. See supra notes 124, 189-93 and accompanying text.
222. See supra notes 124, 189-93 and accompanying text.
individual commits an act that is undertaken with authority, an act that the individual’s nation does not consider illegal, then how can the Convention deem the act without right? The Convention will unlikely be be used in such a manner, therefore there is no apparent problem of mutual assistance.

The Convention is criticized for placing heavy burdens upon Internet service providers. Many critics argue that the Convention places heavy data-preservation requirements on Internet service providers via article seventeen. The critics once again argue that privacy rights are being violated by allowing government officials to obtain user information via a third party, the Internet service provider. However, if you refer directly to the explanatory notes of article seventeen, it clearly demonstrates that the so-called “burden” placed on Internet service providers is hardly a burden at all. As stated in the explanatory notes to article seventeen “this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data.” Here the Convention concedes to the right to privacy in the only way it can while still maintaining its effectiveness.

The Convention only requires the storage of such data for brief periods of time. Furthermore, as explained by the United States Department of Justice, the Convention does not require the Internet service provider to “retain” data, it merely allows for government officials to request that Internet service providers set aside “specified data that is already in the service provider’s possession.” In fact such preservation provisions are not new to the United States. According to the Department of Justice, data preservation has been good law in the United States for five years.

In practice, such a law requires the Internet service provider to set aside “only reasonably small amounts of specific data identified as relevant to a particular case where the service provider already has control over that data.” Obtaining such data is critical to the prosecution of individuals for criminal activity. It is required in order for the Convention to work;

223. See supra notes 185-93 and accompanying text.
224. See supra notes 185-93 and accompanying text.
225. See supra notes 185-93 and accompanying text.
227. Id.
228. See id.
229. Frequently Asked Questions, supra note 124.
230. See id.
231. See id. “18 U.S.C. § 2703(f) requires an electronic communications service provider to ‘take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process’ upon ‘the request of a governmental entity.’” Id.
232. Id.
otherwise such individuals can remain anonymous because prosecutors have no evidence against the offender.

Although the issue of privacy is rather compelling here, this situation seems no different from the government’s power to obtain private information in a prosecution for tax evasion. In such an instance, most individuals would not argue their right to privacy is being violated. If we allow the right to privacy to prevent Internet service providers from complying with the subpoena power of the government, we may as well discard the Convention because hardly anyone could be prosecuted for cyber-crime activities. There seems to be no other apparent method to obtain critical information and potential evidence for the necessary prosecution of cyber-criminals.

Another concern the civil liberties and human rights groups have expressed is that since there seems to be no exemption from liability for Internet service providers, such service providers may be held liable for third party actions. More specifically, critics presume that Internet service providers would be responsible for monitoring customers and user content and thereby held criminally liable when failing to do so, or for employees whose actions are offenses under the Convention. Such a presumption is false. The Convention does not require Internet service providers to monitor content, nor to be liable for failing to monitor content. The Convention only punishes offenses by Internet service providers who intend to transmit or store data with the knowledge of its contents. For example, as long as the Internet service provider only intends to transmit data and does not know that the data contains child pornography, the Internet service provider cannot be prosecuted criminally under the Convention.

Moreover, article twelve of the Convention, relating to corporate liability, addresses the issue of Internet service providers and their employees. Only if an individual “with significant authority within a corporation intentionally undertakes, or through a lack of supervision, permits the undertaking of criminal activity for the corporation’s benefit”

233. See supra notes 185-93 and accompanying text. See also Frequently Asked Questions, supra note 124.

234. See supra notes 185-93 and accompanying text. See also Frequently Asked Questions, supra note 124.

235. See Frequently Asked Questions, supra note 124. See also The Convention, supra note 2, at ch. 3, § 2.

236. See Frequently Asked Questions, supra note 124. See also The Convention, supra note 2, at ch. 3, § 2.

237. See Frequently Asked Questions, supra note 124. See also The Convention, supra note 2, at ch. 3, § 2.

238. See The Convention, supra note 2, at art. XII.
will the corporation or, in this example the Internet service provider, be criminally liable for the actions of its employees. Once again, the Convention is only holding those who are intentionally committing cyber-crime or those who are knowingly allowing cyber-crime to occur, even though they have the ability to prevent such activity. If we were to remove such provisions from the Convention or refine them anymore, the Convention would, again, lose its purpose and cyber-criminals would reign.

Although not a criticism or issue relating directly to privacy, it is important to discuss in this section, as a benefit to enacting the Convention in the United States, whether the Convention will require the United States to execute new legislation in order to comply with the Convention. According to the Department of Justice, the Convention will not require the United States to execute new legislation for the United States to become a signatory state to the Convention. As a result of the Department of Justice’s participation in drafting the Convention, the main lines of the Convention are consistent with the “framework” of current United States substantive and procedural law. For example, “the need to change domestic legislation or amend existing treaties in order to facilitate extradition becomes irrelevant because the [Convention] contains provisions that ameliorate the dilemma.” In addition, the Convention provides for signatories to take full or limited reservations to a limited number of provisions, when such provisions are inconsistent with United States law. Having to adjust or implement legislation is an important consideration when participating in international treaties. Knowing that the United States had a voice in the drafting of the Convention and that the subsequent Convention is, for the most part, consistent with United States law is significant. With such knowledge in mind, it is hard to imagine that our privacy rights will be easily violated, given that the United States may make reservations to the Convention where necessary.

239. Frequently Asked Questions, supra note 124. It is interesting to note that this provision in the Convention applies to a narrow group of individuals, whereas under United States federal law, a much greater number of individuals would face criminal prosecution. See id.

240. See id.

241. See id.

242. See id.


244. Frequently Asked Questions, supra note 124.

245. Another relevant point is that the United States already has several pieces of legislation in place that further the protection of privacy; such legislation includes the Privacy Act of 1974, the 1994 Electronic Communications Privacy Act, and the Privacy Protection Act. Nicole M. Buba, Note: Waging War Against Identity Theft: Should the United States Borrow from the European Union’s Battalion?, 23 Suffolk Transnat’l L.
With cyber-crime as “crimes biggest growth-area” international laws addressing such criminal activity are in demand. More specifically, individuals demand new training and resources for our government officials in order to apprehend cyber-criminals, and individuals demand laws addressing the crimes that cyber-criminals are committing. In order for such training and laws to come into play, our nations must cooperate. “When one country’s laws criminalize certain activities on computers and another country’s laws do not, cooperation in solving a crime and prosecuting the perpetrator may not be possible.” Cyber-criminals benefit by nations having various laws and little international cooperation with regard to regulation and prosecution; we must synchronize our laws to benefit society and the world by attacking the attacker as one. Only then can we truly begin to fight cyber-crime.

IV. RISK – BENEFIT ANALYSIS: DOES THE BENEFIT OF THE CONVENTION ON CYBER-CRIME OUTWEIGH THE POTENTIAL THREAT TO THE RIGHT TO PRIVACY?

Although the concerns that privacy rights may be adversely affected by the enactment of the Convention are valid, they are not certain. At this point the Convention may pose a threat to the privacy rights of individuals, this author believes such potential concerns do not rise above the more certain benefits the Convention has to offer the United States, and the international community. For example, the Convention will further the fight against child pornography, a major problem in the United States and

REV. 633, 644-46 (2000). The Privacy Act of 1974: “[t]he privacy act of 1974 (Privacy Act) attempts to provide protection for personal data by requiring federal adherence to limits and prohibitions regarding the collection, maintenance, use, and dissemination of information by the government.” Id. at 644. The 1994 Electronic Communications Privacy Act: “protect[s] any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectric or photooptical system.” Id. at 645 (quoting Electronic Communications Privacy Act, 18 U.S.C. 5, §§ 2510-2522, and §§ 2701-2711 (1994)). Finally, the Privacy Protection Act (PPA): “offers protection for the limited category of publishers’ work product materials. The PPA forbids government seizure of these materials unless there is probable cause showing that the person in possession of such information is committing an offense to which the materials relate.” Id. at 646. Considering the United States already has legislation in place to further the protection of privacy rights, the Convention, if enacted, will work with the current United States privacy protections, thereby ensuring protection of privacy, as well as a fight against cyber-crime.

246. See A New Sense of the Dangers, supra note 71.
247. See id.
248. Mariano, supra note 206.
249. See The Convention, supra note 2, at ch. 2, § 1, tit. III, at art. 9.
an issue that the international community must address regularly. The Convention, by helping to reduce cyber-crime, will also cut expenses incurred by victims of cyber-crime, expenses paid all too often by big business and our government. Such benefits should have a significant impact on this new ring of terror called cyber-crime. When considering the privacy issues brought up by civil liberties groups and human rights activists, first consider the benefits the Convention will provide.

Meet “Niki” and “Nadia,” teenage sisters living in St. Petersburg, Russia. Niki, fourteen, and Nadia, seventeen, enjoy going to the beach and listening to classical music. But, these sisters do not enjoy all the normal activities of teenage girls, as they have been posing nude for Internet sites for over three years now. At the ages of fourteen and eleven, Nadia and Niki began posing nude for “Lolita” sites. Niki and Nadia work for a site that is only one of thousands; in fact the United States Customs Services states there are 100,000 or more of these sites. “Boris,” the owner and operator of the site that Niki and Nadia pose for, owns at least three more sites like this one. The site the girls pose for sells pictures of nude girls ranging in age from ten to sixteen. Boris justifies the young girls posing nude by stating the girls “feel better about themselves emotionally when they are naked.”

Many operators of such “Lolita sites,” whose photos of nude children in

---

250. See id.

251. See id. See also Cyber-Crime—The Targets It Hits, supra note 64.

252. See generally The Convention, supra note 2.


254. See id.

255. See id.

256. See id. The United States Federal Bureau of Investigation refers to sites featuring nude photos of children from the ages of three years old to seventeen as “Lolita sites.”

“My mother was on vacation and accidentally discovered a nudist beach,” explains Nadia. The next day, their mother returned to the beach with her daughters. “On the beach I met an artist and started posing for him,” says Nadia. “Soon I started working as a photographer’s model for Internet pictures.”

_Id._ It is important to note that Niki and Nadia’s parents were aware that nude photos were being taken of their daughters for Internet sites and approved of their daughters’ posing.

257. See id.

258. See id. It is interesting to note that “Boris,” working from Russia, requested anonymity and that his exact location not be disclosed, including the name of the sites he operates, for fear of “shakedown from local authorities.” _Id._ Although Boris has managed to avoid prosecution because of his claim that his photos are “art.” _Id._

259. See id. at 48.

260. _Id._ at 53.
sexual poses are sold internationally, can be located anywhere in the 
world.261 For example, when Red Herring investigated “The Lolita 
Problem,” they discovered sites such as Illegalheat.com, where upon entry 
you are taken to Pedoland.262 This site guarantees its members 5,000 new 
photos and movies.263 Upon further investigation Red Herring “clicked on 
a link to Sexteens’ only to discover photographs of adult males posing with 
young girls.264 Red Herring reported that “one child, about three years old, 
held a cookie in one hand and an adult male in the other.”265 Other photos 
on the site revealed an eight-year-old child tied to a table, naked and 
blindfolded.266 Some of the sites that maintain these pictures are making up 
to $40,000 per month.267 The responsibility of taking down these “Lolita 
sites” falls upon law enforcement officials who regularly face conflicting 
regulations, which leaves such officials with little ability to shut down 
“Lolita sites.”268 Another problem in bringing down such sites is that the 
volume of child porn online is so large that the United States officials 
cannot investigate and prosecute these criminals without help.269 The 
United States is heading in the right direction to fight child pornography 
online, as John Ashcroft, the United States Attorney General, has made 
child pornography a priority for law enforcement officials and the Bush 
Administration.270 However, as the Red Herring article indicates, the 
United States must attack child pornography on an international level, as 
well, in order to properly address the issue, and prosecute the appropriate 
criminals.271

Activities related to child pornography are one of the more monstrous 
offenses the Convention directly addresses.272 The victims of child 
pornography are young, innocent, and easily impressionable. They cannot 
defend themselves, so they rely on others to fight for their protections. The 
government officials of the United States and the international community 
must step in and stop the victimization of those directly and adversely 
affected by child pornography. Often times the victims’ parents are either 
unaware of the offense being committed upon their children or they see

261. See id. at 48.
262. See id.
263. See id.
264. Id.
265. Id. at 48.
266. See id.
267. See id.
268. See id. at 52.
269. See id. at 53.
270. See id.
271. See id. at 53.
272. See The Convention, supra note 2, at ch. 2, § 1, tit. 3, art. 9.
nothing wrong with it.

Article 9 of the Convention, which comes under Title 3’s “Content-related offences,” deals directly with “Offences related to child pornography”:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally and without right, the following conduct:
   a. producing child pornography for the purpose of its distribution through a computer system;
   b. offering or making available child pornography through a computer system;
   c. distributing or transmitting child pornography through a computer system;
   d. procuring child pornography through a computer system for oneself or for another;
   e. possessing child pornography in a computer system or on a computer data storage medium.

2. For the purpose of paragraph 1 above “child pornography” shall include pornographic materials that visually depicts:
   a. a minor engaged in sexually explicit conduct;
   b. a person appearing to be a minor engaged in sexually explicit conduct;
   c. realistic imagers representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however require a lower age limit, which shall not be less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).273

The explanatory notes to the Convention further explain the objectives of Title 3, Article 9 as follows: “Article 9 on child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offenses against children.”274 The explanatory notes state further:

Most States already criminalise the traditional production and physical distribution of child pornography, but with the ever-increasing use of

---

273. See id.

the Internet as the primary instrument for trading such material, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children.\footnote{275}

The Convention is the best possible solution to the international problem that child pornography presents to the United States and the rest of the world. The Convention equalizes the laws across the signatory states.\footnote{276} With equal laws on the international level, it will be easier for the United States to prosecute people like Boris, who provide child pornography materials across the Internet to purchasers in the United States. The problem of child pornography is simply too large for the United States to attack alone.\footnote{277} But with the Convention, international barriers come down and the number of those seeking to attack the problem could greatly increase. With an increase in states fighting cyber-crime, more resources may become readily available, and the exchange of information necessary to prosecute offenders may flow more freely between the states. It will be easier for all signatory states to combat child pornography with the cooperation of authorities when investigating and prosecuting criminals that the Convention provides.\footnote{278}

Knowing just how large the problem of child pornography is, how can anyone not promote a Convention that provides a solution to the prosecution of such offenders? The problem of child pornography must be addressed, and what the signatory states, including the United States, have done up to now to address the problem is simply not enough. At this point, the Convention is the best solution to fighting child pornography offenders worldwide and in the United States. The equalization of laws across the signatory states is fundamental to the fight against child pornography. This is a fight in which the United States must be ready to do battle and that it must win. The Convention not only prepares the United States for this battle; the Convention makes victory a reality.

As discussed earlier, the cost to big business and the government when they are hit by cyber-criminals is atrocious.\footnote{279} If the United States does not act now, who knows just how adversely our society will be affected? At this point, cyber-criminals feel they can remain anonymous; they evade the law and avoid prosecution, thus the growth in cyber-crime is steady and strong.\footnote{280} We must, as a country, send a message to cyber-criminals that

\footnote{275. Id.} \footnote{276. See The Convention, supra note 2.} \footnote{277. See Grove & Zerega, supra note 253, at 53.} \footnote{278. See The Convention, supra note 2.} \footnote{279. See Cyber-Crime—The Targets it Hits, supra note 64.} \footnote{280. See Cesare, supra note 49, at 164.}
we can and will prosecute. In order for such a message to register with cyber-criminals we must enact an international doctrine that will allow the United States to prosecute someone in another country who commits a crime via the Internet. The only solution available for the United States is to work with the other countries’ authorities. The Convention provides similar laws around the world and helps mitigate jurisdictional problems so that the United States may prosecute an offender, even if he is in another part of the world.  

The Convention also collects and makes the exchange of evidence between the victim’s countries and the offender’s country. We can no longer remain victims, we can no longer open the pockets of big business and force them to continue to suffer financial blows every time cyber-crime hits simply because we lack the means to track down and punish offender. Not only will the Convention help deter future cyber-criminals, but it will also provide punishment for offenders. Although punishment does not give the stolen money back to big business or the government, punishment will assure such entities that the particular offender will not strike again.

The benefits of the Convention are vital to the United States’ fight against international cyber-crime. The United States must fight cyber-crime on an international level or we will succumb to offenders throughout the world. The right to privacy is important; in fact this author considers herself an advocate of privacy rights. However, when innocent children, big business, the government of the United States, and society as a whole stand to be victimized by cyber-crime, the benefits of the Convention outweigh the potential threat to privacy. Even Constitutional rights are not absolute rights; the right to privacy has been infringed upon in appropriate cases where a heightened state interest exists. Many opponents of the Convention argue that it gives the police too much power and that a greater separation of power is needed between the police who obtain information from Internet service providers and those agencies who authorize the police to gather this information. However, if the police are not given subpoena power, how will they properly fight cyber-crime? If the police are unable to determine the name and location of an offender, how will they protect the victims of cyber-crime? By preventing the police from obtaining such information, we allow the offenders to continue to enjoy

281. See Main Lines of the Convention, supra note 80.
282. See id.
283. See The Convention, supra note 2.
284. See, e.g., Boy Scouts of America v. Dale, 530 U.S. 640, 678 (2000) (holding that the First Amendment’s freedom of association, inter alia, is not an absolute right).
286. See Ward, supra note 150.
anonymity while they commit their crimes. The anonymity of cyber-crime helps explain the increase in the number of cyber-crimes.\textsuperscript{287} We must give the police the power to subpoena information such as the names and locations of offenders (provided the police have probable cause) so that the United States and the international community can effectively fight cyber-crime.\textsuperscript{288} If we refuse the police such power, we might as well hand over our children and open our pockets and because there will be no effective way to cross international borders to investigate and prosecute cyber-criminals who hide behind their computers.

Opponents of the Convention are also concerned that giving the police such power may allow the police to force individuals to provide their passwords to officials.\textsuperscript{289} However, if the police have the necessary probable cause to obtain a search warrant, you must unlock the door and let them in.\textsuperscript{290} When you allow the police to search your home, is that not your own private space? How is this any different from allowing the police, who have probable cause and a valid search warrant, to “search” your computer or e-mail inbox? You must give them your password and allow them access in the same way you would unlock your door and allow them into your home. Once the police have established probable cause and have the proper authority, what is it that you are trying to hide? What is it that you are doing that you need to remain anonymous? In the United States the Constitution still applies, thus the Fourth Amendment still stands.\textsuperscript{291} We must be mindful of the fact that our own United States Department of Justice participated in drafting the Convention.\textsuperscript{292} As long as the police are in compliance with the Constitution, they should be allowed to conduct an investigation, and the government should be allowed to prosecute those who break the law. The Convention does not, on its face, seem to provide for any violations of our constitutional rights, it only increases the ability of the United States to prosecute those in other countries who commit cyber-crimes against United States citizens.\textsuperscript{293} Civil libertarians and human rights activists are concerned that we will no longer remain anonymous on the

\textsuperscript{287} See Running the Gamut, supra note 43.
\textsuperscript{288} As one author has noted, “the citizens of the United States place greater value on rights and freedoms other than the right to privacy, which are guaranteed by the Constitution. These other rights diminish the importance of privacy.” Julia Gladstone, The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy, 7 Willamette J. Int’l L. & Disp. Resol. 10, 32 (2000).
\textsuperscript{289} See McCullagh, supra note 174.
\textsuperscript{290} See U.S. Const. amend. IV.
\textsuperscript{291} See id.
\textsuperscript{292} See Frequently Asked Questions, supra note 124.
\textsuperscript{293} See The Convention, supra note 2.
This argument is a stretch. The government has no desire to regulate what every Internet user is doing, nor would it be possible for the government to maintain such information. Between the Constitution and the Convention, the only individuals who face a threat to their privacy while online will be the individuals who are breaking the law.

We must be mindful of the fact that the Convention itself specifically addresses privacy and human rights. The Preamble of the Convention states:

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impact information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

Given that the Convention specifically addresses human rights and privacy, there is no support for the argument that the Convention directly violates the right to privacy.

V. RECOMMENDATION AND CONCLUSION

After careful consideration of the issues regarding human rights, privacy, and self-incrimination, the United States become a party to the Convention. The United States played an important role in drafting the Convention, which should dispel fears that the Convention could negatively affect the constitutional rights of United States citizens. Realizing the United States Justice Department was privy to drafting the Convention makes it more likely than not that the concerns of United States citizens were addressed during the drafting process. Realizing just how much cyber-crime has grown demonstrates the need for a doctrine specific to cyber-crime. Realizing further that cyber-crime is not and cannot be

294. See McCullagh, supra note 174.
295. The Convention, supra note 2.
296. See id.
297. See Frequently Asked Questions, supra note 124.
298. See Democracy at Risk, supra note 35.
confined to the United States, the need for an international tool becomes
greater. United States citizens, businesses, government and society are
being victimized regularly by cyber-criminals all over the world who
anonymously hide behind their computer.299 This is causing our businesses
to lose money, costing our government and thereby the taxpayers hundreds
of thousand of dollars, and we currently have no resolution to the problem
of cyber-criminals in other countries.300 We must protect the United States
and her citizens from continued victimization, and the Convention is a step
in that direction.

The right to privacy is a fundamental right.301 Human rights must be
accorded the highest respect, but the potential threat to them is not definite
enough to continue allowing cyber-criminals to violate the innocence of
children, or to steal money from our businesses, government, and
taxpayers. The nations of the world must come together to fight cyber-
crime, as it is a global problem. The nations of the world must work
together by implementing similar laws to ensure that cyber-crime is illegal
in all nations. Finally, the nations of the world must come together to
eliminate jurisdictional problems and must open international borders in
order to better work together when investigating and collecting evidence to
use against cyber-criminals. We must prevent these anonymous criminals
from continuing to victimize United States citizens and citizens of the
world. The only way to ensure cyber-criminals are punished and cyber-
crime deterred is to enact an international tool, bringing together nations so
that the world can fight cyber-crime as one. The Convention on Cyber-
Crime is the treaty that will bring our nations together and the international
tool that has the power to effectively fight cyber-crime. The United States
should enact the Convention; the benefit that will be conferred heavily
outweighs the possible threat to the right to privacy.

Sara L. Marler

299. See Cyber-Crime—The Targets it Hits, supra note 64.
300. See id.