Florida State University Journal of Transnational Law & Policy

Volume 12 | Issue 2 Article 5

2003

The Council of Europe Convention on Cybercrime

Mike Keyser

The Council of Europe Convention on Cybercrime

Cover Page Footnote

J.D. candidate, Seattle University School of Law (May 2003); B.A., Washington State University (May 2000).

The author would like to thank Bob Menanteaux, reference librarian at Seattle University School of Law, for all of his help and guidance.

THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

MIKE KEYSER*

Table of Contents

I. INTRODUCTION

The Internet is often referred to as the new "Wild West."[1] This maxim holds true, because the Internet is so similar to the turn of the century Western Frontier.[2] Like the Wild West, the Internet has brought with it opportunity and millions of new jobs.[3] The Internet also brings with it very real dangers. Although the specific dangers may be different from those faced on the American Frontier, a web surfer's exposure to dangers which are new, difficult to police, and difficult to prevent, is very similar.[4] The only significant difference may be that the Internet is a virtual society

---

* J.D. candidate, Seattle University School of Law (May 2003); B.A., Washington State University (May 2000). The author would like to thank Bob Menanteaux, reference librarian at Seattle University School of Law, for all of his help and guidance.

1. Henry E. Crawford, *Internet Calling: FCC Jurisdiction over Internet Telephony*, 5 COMM. L. CONSPECTUS 43, 43 (1997) (discussing the Internet and analogizing it to the Wild West).

2. *Id.*

3. Mohit Gogna, *The World Wide Web Versus the Wild Wild West*, *at* http://home.utm.utoronto.ca/~mohit/ (last visited Dec. 4, 2002). For example, in 1996, 1.1 million jobs were created. *Id.*

4. *Id.*

rather than a tactile one; a virtual society existing only in networks and information packets.[5] However, the harms committed against both individual citizens and businesses are very real.[6] These citizens are extremely vulnerable as criminal activity on the Internet continues to run rampant.[7]

This article is intended to expand upon the existing wealth of knowledge regarding cybercrimes. However, it takes the analysis one step further. This is the first article to consider the impact of a new, powerful, and timely piece of international legislation: The Council of Europe's Convention on Cybercrime.[8] Section II of this comment begins with a survey of the cyber-landscape. It illustrates citizenry and critical infrastructures extremely vulnerable to international, as well as domestic, cyber attacks. Section II ends with a case example—the case of Raymond Torricelli and his Internet exploits. Section III is an in-depth analysis of the newly signed, but not yet ratified, Cybercrime Convention. Section III examines the entire Convention, article by article, taking into account critical opinion, as well as drafter intent. Select provisions of importance are analyzed in greater depth by looking at their improvements upon existing law, in addition to their pitfalls. The fourth and final section concludes the comment by projecting toward the future, forecasting some aspects of the Convention's impact upon our lives as it enters into force, as well as the likely objections individuals, businesses, and interest groups will have to treaty provisions.

---

5. Joginder S. Dhillon & Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Governmental Investigative Techniques*, 50 A.F. L. REV. 135, 138 (2001) (explaining the composition of the Internet and how information is transferred).

6. Many of the crimes committed against individuals and businesses are legislated against in the European Convention on Cybercrime, and include identity theft, child pornography, and fraud, among others. Convention on Cybercrime, *opened for signature* Nov. 23, 2001, Europ. T.S. No. 185 [hereinafter Convention], *available at* http://conventions.coe.int/ Treaty/EN/ projets/FinalCybercrime.htm (last visited Dec. 4, 2002).

7. Aaron Craig, *Gambling on the Internet*, 1998 COMPUTER L. REV. & TECH. J. 61 (1998) (discussing the seriousness of the effects of crime on the Internet), *available at* http://www.smu.edu/csr/Spring98-2-Craig.PDF.

8. Convention, *supra* note 6.

II. YOUR NETWORK NEIGHBORHOOD

A. Crime on the "Net"

The 2001 Computer Crime and Security Survey, conducted by the Computer Security Institute and the FBI's San Francisco office, is prime evidence of the extent of lawlessness on the Internet:

> 1. 47 percent of the companies surveyed had their systems penetrated from the outside;[9]
>
> 2. 90 percent reported some form of electronic vandalism;[10]
>
> 3. 13 percent reported stolen transaction information (meaning personal data and credit card numbers).[11]

This figure is daunting since only a small percentage of companies responded, while hundreds of companies whose systems have been compromised, and whose information has been stolen, remain in the dark.[12] Numerous reasons exist which explain why businesses are reluctant to report system intrusions.[13] Most commonly, this reluctance is attributed to the fear that a public report would compromise a competitive position in their respective market.[14] In other words, they may lose business if the public perceives the company as vulnerable to attack or unable to keep personal identification secure.[15] The FBI estimates that the cost of electronic crime exceeds ten billion dollars per year.[16]

Cybercrimes are not limited to businesses. The Federal Trade Commission reported that identity theft and bogus Internet scams topped the list of consumer fraud complaints in 2001.[17] Identity theft, arguably the most prevalent crime on the Internet, comprised 42 percent of the total complaints.[18] With figures like these, it is no

---

9. John Galvin, *Meet the World's Baddest Cyber Cops*, ZIFF DAVIS SMART BUS. FOR THE NEW ECON. (Oct. 1, 2001), *at* 78 (on file with the Journal of Transnational Law & Policy).

10. *Id.*

11. *Id.*

12. *Id.*

13. Dhillon & Smith, *supra* note 5, at 140 (discussing the reluctance of companies to report intrusions on its systems).

14. *Id.*

15. *Id.*

16. *Id.* at 139.

17. Jay Lyman, *ID Theft and Web Scams Top Consumer Complaints*, NEWSFACTOR NETWORK (Jan. 24, 2002), *at* http://www.newsfactor.com/perl/story/15965.html.

18. *Id.*

secret that cybercrimes pose an ongoing and significant threat to the security of the United States and its citizens.[19]

B. Greater Dependency on Technology

As our lives become more advanced, we depend on computers and technology to even greater degrees. For example, one should consider the increasing trend of Internet sales. The convenience and privacy of online consumer spending is leading towards a growing use of the Internet as a consumer's primary purchasing location. In the year 2000, online retail sales totaled $5 billion, while total sales were $42.4 billion.[20] "Total U.S. spending on online sales increased from $4.9 billion in November to $5.7 billion in December" of 2001.[21] Consumer online sales for the third quarter of 2002 reached $17.9 billion, a 35 percent increase over the third quarter of 2001.[22] Online sales through the third quarter of 2002 totaled $52.5 billion.[23] As online sales continue to increase, and personal and credit card information is transferred over the Internet, the American public also increases its chances that it will become the victim of a "cybercrime."

C. What is a Cybercrime & Who are Cybercriminals?

"The Department of Justice ("DOJ") defines computer crimes as 'any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution.'"[24] The types of people who commit cybercrimes vary as much as the multitude of crimes that can be committed.[25] "Computer criminals can be youthful hackers, disgruntled employees and company insiders, or international terrorists and spies."[26] These criminals become "cybercriminals" when their crimes involve the use of a computer. "[A] computer may be the 'object' of a crime," or in other words, "the criminal targets the computer itself."[27] "[A] computer may [also] be the 'subject' of a crime," or in other words, it "is the

19. Galvin, *supra* note 9.

20. CyberAtlas Staff, *December Rakes in the E-Commerce Dough*, *at* http://cyberatlas.internet.com/markets/retailing/article/0,,6061_961291,00.html (last visited Feb. 11, 2003).

21. *Id.*

22. Robyn Greenspan, *Shoppers Gearing Up for Season*, *at* http://cyberatlas.internet.com/markets/retailing/article/0,,6061_1494231,00.html#table1 (last visited Feb. 11, 2003).

23. *Id.*

24. Sheri A. Dillon et al., Note, *Computer Crimes*, 35 Am. Crim. L. Rev. 503, 505 (1998) (defining "computer crime") (*quoting* National Institute of Justice, U.S. Dep't of Justice, Computer Crime: Criminal Justice Resource Manual 2 (1989)).

25. Dillon et al., *supra* note 24, at 506.

26. *Id.*

27. *Id.* at 507.

physical site of the crime, or the source of, or reason for, unique forms of asset loss."[28] Examples of this type of crime are viruses, logic bombs, and sniffers.[29] Finally, "a computer may be [the] 'instrument' used to commit traditional crimes."[30] For example, a computer might be used to commit the most common type of cybercrime to date—identity theft.[31]

D. Identity Theft

Identity theft is now being called "the signature crime of the digital era."[32] "Identity theft is the illegal use of another's personal identification numbers."[33] Examples include a person using a stolen "credit card, or social security number to purchase goods,"[34] withdraw money, apply for loans, or rent apartments.[35] While these types of crimes have existed for a long time in the form of pick pocketing, the Internet facilitates their frequency and ease.[36] Without faces or signatures, the only thing preventing a person from posing as another is a password, which can be intercepted without much difficulty by an experienced criminal.[37]

E. Taking a Bite out of Crime, Domestically Speaking

In the United States, laws intended to combat cybercrimes are already in place.[38] Congress treats cybercrimes as distinct federal offenses through a multitude of acts, most notably the Computer

---

28. *Id.*
29. *Id.*
30. *Id.*
31. *See* Lyman, *supra* note 17.
32. Michael McCutcheon, *Identity Theft, Computer Fraud and 18 U.S.C. § 1030(G): A Guide to Obtaining Jurisdiction in the United States for a Civil Suit Against a Foreign National Defendant*, 13 LOY. CONSUMER L. REV. 48, 48 (2001) (discussing identity theft).
33. *Id.*
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.* at 49.
38. *See, e.g.*, 18 U.S.C. § 875 (2000) (originally enacted as Act of June 25, 1948, ch. 645, 62 Stat. 741) (interstate communications: including threats, kidnapping, ransom, and extortion); 18 U.S.C. § 1029 (2000) (possession of access device); 18 U.S.C. § 1030 (2000) (fraud and related activity in connection with computers); 18 U.S.C. § 1343 (2000) (originally enacted as Act of July 16, 1952, ch. 879, § 18(a), 66 Stat. 722, and *amended* by Act of July 11, 1956, ch. 561, 70 Stat. 523) (fraud by wire, radio, or television); 18 U.S.C. § 1361 (2000) (based on Act of Mar. 4, 1909, ch. 321, § 35, 35 Stat. 1095; Act of Oct. 23, 1918, ch. 194, 40 Stat. 1015; Act of June 18, 1934, ch. 587, 48 Stat. 996; Act of Apr. 4, 1938, ch. 69, 52 Stat. 197) (injury to government property or contracts); 18 U.S.C. § 1362 (2000) (based on Act of Mar. 4, 1909, ch. 321, § 60, 35 Stat. 1099) (communication lines, stations, or systems); Economic Espionage Act of 1996, 18 U.S.C. § 1831, *et seq.* (2000).

Fraud and Abuse Act of 1986[39] and the National Information Infrastructure Protection Act of 1996.[40] These laws are designed to incriminate domestic hackers. A good example is the case of twenty-year old Raymond Torricelli, known by the hacking code name, "rolex."[41]

Torricelli was the head of a notorious hacking group known as "#conflict."[42] Operating out of his New Rochelle, New York home, Torricelli "used his personal computer to run programs designed to search the Internet, and seek out computers which were vulnerable to intrusion."[43] Once a computer was "located, Torricelli's computer obtained unauthorized access . . . by uploading a program known as 'rootkit.'"[44] When run on a foreign computer, rootkit "allows a hacker to gain complete access to all of a computer's functions without having been granted these privileges by the authorized users of that computer."[45]

"One of the computers Torricelli accessed was used by NASA [the National Aeronautics and Space Administration] to perform satellite design and mission analysis concerning future space missions."[46] Another computer Torricelli accessed was used by NASA's Jet Propulsion Laboratory "as an e-mail and internal web server."[47]

After gaining unauthorized access to these computers, Torricelli "used many of the computers to host chat-room discussions."[48] "[I]n these discussions, he invited other chat participants to visit a website which enabled them to view pornographic images."[49] "Torricelli earned 18 cents for each visit a person made to that website," ultimately netting $300-400 dollars per week from this activity.[50]

Torricelli's criminal activities were far from over. He also intercepted "usernames and passwords [by] traversing the computer networks" of San Jose State University.[51] In addition, he stole

---

39. Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986) (amending 18 U.S.C. § 1030).

40. Pub. L. No. 104-294, tit. 2, § 201, 110 Stat. 3488, 3491-94 (1996) (amending 18 U.S.C. § 1030). For a discussion of laws currently in place, see Dillon et al., *supra* note 24, at 508.

41. Press Release, United States Dep't of Justice, *Hacker Sentenced in New York City for Hacking into Two NASA Jet Propulsion Lab Computers Located in Pasadena, California* (Sept. 5, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/ torricellisent.htm.

42. *Id.*

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.*

passwords and usernames from numerous other sources "which he used to gain free Internet access, or to gain unauthorized access to still more computers."[52] When Torricelli "obtained passwords which were encrypted, he would use a password cracking program known as 'John-the-Ripper' to decrypt the passwords."[53]

Torricelli was still not finished. He also obtained stolen credit card numbers and "used one such credit card number to purchase long distance telephone service."[54]

> [M]uch of the evidence obtained against Torricelli was obtained through a search of his personal computer. . . . [I]n addition to thousands of stolen passwords and numerous credit card numbers, investigators found transcripts of chat-room discussions in which Torricelli and members of '#conflict' [his hacker group] discussed, among other things, (1) breaking into other computers . . . (2) obtaining credit card numbers belonging to other persons and using those numbers to make unauthorized purchases . . . and (3) using their computers to electronically alter the results of the annual MTV [Music Television] Movie Awards.[55]

52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*

III. TAKING A BITE OUT OF CRIME

A. *The Internationalization of Cybercrime*

Due to the nature of cybercrimes and an undeveloped international body of law on the topic, cybercrimes often occur internationally. For example, perpetrators "across the United States and Europe were indicted by a federal grand jury [in May, 2000] for allegedly conspiring to infringe the copyright of more than 5,000 computer software programs. . . ."[56] These programs were "made available through a hidden Internet site located at a university in Quebec, Canada."[57]

Some of the perpetrators:

> allegedly were members . . . of an international organization of software pirates known as "Pirates with Attitudes," ["PWA"] an underground group that disseminates stolen copies of software, including programs that are not yet commercially available.... [Others] were employees of Intel Corp., four of whom allegedly supplied computer hardware to the piracy organization in exchange for obtaining access . . . to the group's pirated software, which had a retail value in excess of $1 million.[58]

PWA is "one of the oldest and most sophisticated networks of software pirates anywhere in the world."[59] Officials are aware of this because "previous software piracy investigations that have focused on smaller sites have turned up numerous copyrighted software files bearing annotations reflecting that the files were supplied to the sites through PWA."[60]

International crime syndicates often communicate "in real time on private Internet Relay Chat ["IRC"] channels," or in code via open Internet chat rooms.[61] "PWA allegedly maintained numerous File Transfer Protocol ["FTP"] sites configured for the transfer of

---

56. Press Release, United States Dep't of Justice, *U.S. Indicts 17 in Alleged International Software Piracy Conspiracy* (May 4, 2000), *available at* http://www.cybercrime.gov/pirates.htm.

57. *Id.*

58. *Id.*

59. *Id.* (*quoting* Scott R. Lassar, United States Attorney for the Northern District of Illinois).

60. *Id.*

61. *Id.*

software files and stored libraries of pirated software on each of these sites."[62]

PWA's website "was not accessible to the general public, but instead was configured so that it was accessible only to" those people who knew its Internet Protocol ("IP") address.[63] In order for users to maintain their ability to access the website and download pirated software, they were required "to 'upload,' or provide files, including copyrighted software files obtained from other sources and, in return, were permitted to 'download'" pirated files provided by other users.[64] At one point, "more than 5,000 copyrighted computer software programs were available for downloading. . . ."[65]

Software pirates are often assigned different tasks, which shields the overall organization from a governmental "bust."[66] PWA followed this organizational scheme assigning some members to the role of "cracker," which are people who strip "away the copy protection that is embedded in [the] . . . software."[67] Others were assigned as "couriers" whose job it was to transfer software to PWA, or as "suppliers" who were funneling "programs from major software companies to the group."[68]

In this case, the United States had jurisdiction over those nationals involved in the piracy scheme.[69] But what about PWA members that live outside U.S. borders in countries that do not have an extradition treaty with the United States? It seems that United States laws might not apply to those international criminals or cannot reach their criminal actions. This problem poses a serious concern for many government officials because many computer systems can be easily accessed through a "global telecommunications network from anywhere in the world."[70] Furthermore, it becomes a roll of the dice as to whether the criminal's host country has laws stringent enough to bring the criminal to justice, or if the host country is even willing to cooperate in the first place.[71] Thus, in order to successfully combat cybercrime, it is clear that the world needs a better international legal system in which to catch and convict cybercriminals.

---

62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. Dillon et al., *supra* note 24, at 539 (discussing computer systems and ease of access).
71. *Id.*

B. The Council of Europe Cybercrime Convention

The forty-one nation Council of Europe ("COE") drafted the Cybercrime Convention[72] after four years and twenty-seven drafts.[73] It was adopted by the Committee of Ministers during the Committee's 109th Session on November 8, 2001.[74] The Convention was opened for signature in Budapest, on November 23, 2001.[75] Thirty-five countries have signed the treaty, with Albania and Croatia having ratified it as well.[76] The Convention will come into force when five states, three of which must be COE members, have ratified it.[77] The treaty is intended to create a common cross-border "criminal policy aimed at the protection of society against cybercrime . . . by adopting appropriate legislation and fostering international co-operation."[78]

1. Importance

The COE's Convention on Cybercrime is important international legislation because it binds countries in the same way as a treaty. "An international convention, or treaty, is a legal agreement between governments that spells out a code of conduct."[79] Once a large number of states have ratified a treaty, then it becomes acceptable to treat it as general law.[80] Treaties are the only machinery that exist for adapting international law to new conditions and strengthening the force of a rule of law between states.[81] Thus, it seems very important for an international regime to be set up to combat these types of crimes in a growing and

---

72. Convention, *supra* note 6.

73. Peter Piazza, *Cybercrime Treaty Opens Pandora's Box*, SECURITY MGMT. (Sept. 2001), *available at* http://www.securitymanagement.com/library/001100.html.

74. Convention, *supra* note 6.

75. *Id.*

76. Council of Europe, *Chart of Signatures and Ratifications*, *available at* http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (last visited Dec. 6, 2002) (signatories include: United States; Albania; Armenia; Austria; Belgium; Bulgaria; Canada; Croatia; Cyprus; Estonia; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Italy; Japan; Malta; Moldova; Netherlands; Norway; Poland; Portugal; Romania; Slovenia; Spain; Sweden; Switzerland; South Africa; Ukraine; United Kingdom; and the former Yugoslav Republic of Macedonia).

77. Wendy McAuliffe, *Council of Europe Approves Cybercrime Treaty*, ZDNET UK NEWS (Sept. 21, 2001), *at* http://news.zdnet.co.uk/story/0,,t269-s2095796,00.html.

78. Convention, *supra* note 6, pmbl.

79. UNICEF, *Laws and International Conventions*, *at* http://www.unicef.org/turkey/laws_i_c/ (last visited Feb. 11, 2003).

80. JAMES LESLIE BRIERLY, THE LAW OF NATIONS: AN INTRODUCTION TO THE INTERNATIONAL LAW OF PEACE 57 (Humphrey Waldock ed., Oxford Univ. Press 6th ed. 1963) (1928).

81. *Id.*

integrated global society, which is becoming ever more vulnerable to cyber attacks.

2. Objectives

The Convention is intended to be the "first international treaty on crimes committed via the Internet and other computer networks."[82] Its provisions particularly deal with infringements of copyrights, computer-related fraud, child pornography, and violations of network security.[83] Its main objective, set out 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 co-operation."[84]

3. Parties Involved

The Convention is open to worldwide membership.[85] Instrumental in its drafting were the forty-one COE "countries, which cover most of Central and Western Europe."[86] In addition, the United States, Canada, Japan, and South Africa also aided in its drafting.[87] As stated earlier, as of the date of this publication, thirty-five countries have signed the treaty.[88]

4. Scope

The Convention is broken up into four main segments, with each segment consisting of several articles. The first section outlines the substantive criminal laws and the common legislation all ratifying countries must adopt to prevent these offenses.[89] The second section delineates the prosecutorial and procedural requirements to which individual countries must adhere.[90] The third section sets out guidelines for international cooperation that most commonly involve joint investigations of the criminal offenses set out in section one.[91] Finally, the fourth section contains the articles pertaining to the signing of the Convention, territorial application of the Convention,

---

82. Convention, *supra* note 6, pmbl.
83. *Id.*
84. *Id.*
85. Lawrence Speer, *Computer Crime: Council of Europe Cybercrime Treaty Attacked by ISPs, Business at Hearing*, 6 COMPUTER TECH. L. REP. 100 (Mar. 16, 2001).
86. Robyn Blumner, *Cyberfear Leading to International Invasion of Privacy*, MILWAUKEE J. SENTINEL, June 6, 2000, at 17A.
87. *Id.*
88. Council of Europe, *Chart of Signatures*, *supra* note 76.
89. Convention, *supra* note 6.
90. *Id.*
91. *Id.*

declarations, amendments, withdrawals, and the ever-important, federalism clause.[92]

5. Convention Section 1 – Definitions and Criminal Offenses

Article 1 initially defines four terms vital to the treaty.[93] These terms are vital because they are heavily relied upon throughout the treaty. The treaty first defines "Computer system" as a device consisting of hardware and software developed for automatic processing of digital data.[94] For purposes of this Convention, the second term, "computer data," holds a meaning different than that of normal computer lingo.[95] The data must be "in such a form that it can be directly processed by the computer system."[96] In other words, the data must be electronic or in some other directly processable form.[97]

The third term, "service provider" includes a broad category of entities that play particular roles "with regard to communication or processing of data on computer systems."[98] This definition not only includes public or private entities, but it also extends to include "those entities that store or otherwise process data on behalf of" public or private entities.[99]

The fourth defined term is "traffic data," which has created some controversy in this Convention. "Traffic data" is generated by computers in a "chain of communication in order to route" that communication from an origin to its destination.[100] Thus, it is auxiliary to the actual communication.[101] When a Convention party investigates a criminal offense within this treaty, "traffic data" is used to trace the source of the communication.[102] "Traffic data" lasts for only a short period of time and the Convention makes Internet Service Providers ("ISPs") responsible for preservation of this data.[103] The increased costs placed upon ISPs as a result of the Convention's stricter rules regarding preservation of "traffic data" is one issue of concern for many ISPs. Another concern is the

92. *Id.*
93. *Id.* art. 1.
94. *Explanatory Report of the Comm. of Ministers [of the Convention on Cybercrime]*, 109th Sess. (adopted on Nov. 8, 2001), art. 1(a), ¶ 23 [hereinafter *Explanatory Report*] (on file with the Journal of Transnational Law & Policy).
95. *Id.* art. 1(b), ¶ 25.
96. *Id.*
97. Id.
98. *Id.* art. 1(c), ¶¶ 26, 27.
99. *Id.*
100. *Id.* art. 1(d), ¶¶ 28-31.
101. *Id.*
102. *Id.*
103. *Id.*

requirement of rapid disclosure of "traffic data" by ISPs.[104] While rapid disclosure may be necessary to discern the communication's route, in order to collect further evidence or identify the suspect, some civil libertarians express concern over its infringement upon individual rights—namely the right to privacy.

The drafters intended that "Convention parties would not be obliged to copy [the definitions] verbatim into their domestic laws...."[105] It is only required that the respective domestic laws contain concepts that are "consistent with the principles of the Convention and offer an equivalent framework for its implementation."[106]

After defining the vital terms, Article 1 lays out the Convention's substantive criminal laws. The purpose of these criminal laws is to establish a common minimum standard of offenses for all countries.[107] Uniformity in domestic laws prevents abuses from being shifted to a Convention party with a lower standard.[108] The list of offenses is based upon the work of public and private international organizations, such as the United Nations and the Organization for Economic Cooperation and Development.[109]

"All of the offenses contained in the Convention must be committed 'intentionally' for criminal liability to apply."[110] In certain cases, additional specific intentional elements form part of the offense.[111] The drafters have agreed that the exact meaning of "intentional" will be left to the Convention parties to interpret individually.[112] A mens rea requirement is important to filter the number of offenders and to distinguish between serious and minor misconduct.

The criminal offenses in Articles 2 thru 6 were intended by the drafters "to protect the confidentiality, integrity and availability of computer systems or data."[113] At the same time, however, the drafters did not criminalize "legitimate and common activities inherent in the design of networks, or legitimate . . . practices."[114]

---

104. Convention, *supra* note 6, arts. 17, 30.
105. *Explanatory Report*, *supra* note 94, art. 1, ¶ 22.
106. *Id.*
107. *Id.* ch. 2, § 1, ¶ 33.
108. *Id.*
109. *Id.* ch. 2, § 1, ¶ 34.
110. *Id.* ch. 2, §1, ¶ 39.
111. *Id.*
112. *Id.*
113. *Id.* tit. 1, ¶ 43.
114. *Id.*

a. Article 2 – Illegal Access[115]

Article 2 relates to "illegal access," or access to a computer system without right.[116] Examples of unauthorized intrusions are hacking, cracking, or computer trespassing; like those our friend Raymond Torricelli had demonstrated earlier. Intrusions such as these allow hackers to gain access to confidential data, such as passwords and identification numbers.[117] "Access" deals with the entering of any part of a computer system such as hardware components and stored data, but it "does not include the mere sending of an e-mail message" to a file system.[118] Convention parties are granted great latitude with respect to the legislative approach they take in criminalizing this action.[119] Parties can take a wide approach, or a more narrow one, by attaching such qualifying elements as infringing upon security measures, requiring specific intent to obtain computer data, or requiring a dishonest intent justifying criminal culpability.[120]

The analogous United States law to this Article is the Computer Fraud and Abuse Act of 1986 ("CFAA").[121] This Act makes it unlawful to either knowingly access a computer without authorization or to exceed authorization and obtain protected or restricted data.[122] The case of *United States v. Ivanov*,[123] is an example of the way in which courts would be able to utilize Article 2 in international prosecutions. Ivanov, a Russian computer hacker, was "charged with conspiracy, computer fraud and related activity, extortion, and possession of unauthorized access devices" after hacking into a Connecticut e-commerce corporation's computer files and stealing passwords and credit card information.[124] He then threatened the corporation with extortion while he was in Russia.[125] Ivanov moved to dismiss the indictment "on the ground that court lacked subject matter jurisdiction."[126] Essentially, Ivanov contended that because he was in Russia, the laws of the United States did not apply extraterritorially to him. The district court held that the taking of the corporation's data occurred in Connecticut, the

115. *Id.*
116. Convention, *supra* note 6, art. 2.
117. *Explanatory Report*, *supra* note 94, art. 2, ¶ 47.
118. *Id.* art. 2, ¶ 46.
119. *Id.* art. 2, ¶ 49.
120. *Id.* art. 2, ¶ 50.
121. 18 U.S.C. § 1030 (2000).
122. 18 U.S.C. § 1030(a)(1).
123. 175 F. Supp. 2d 367 (D. Conn. 2001).
124. *Id.* at 368.
125. *Id.*
126. *Id.*

violation of the CFAA occurred when his email was received in Connecticut, and thus the CFAA applied to Ivanov.[127] It would appear on its face that the CFAA is the United States equivalent to this Article. However, the Convention improves upon the CFAA by applying an across the board rule to all signatories thereby ensuring compliance. For instance, in this case, Russia cooperated with United States authorities in extraditing Ivanov to the United States for trial. But if Russia was not so cooperative, Ivanov would have broken a United States law, caused serious damage to a United States corporation and hundreds of citizens, and would be a free man living in another country. This is a situation in which the Convention's global law enforcement network would succeed.

b. Article 3 – Illegal Interception

Article 3, "illegal interception," outlaws the interception, without right, of nonpublic transmissions of computer data, whether it be by telephone, fax, email, or file transfer.[128] This provision is aimed at protecting the right to privacy of data communication.[129] One element of this offense is that the interception occur through "technical means," which is the surveillance of communications "through the use of electronic eavesdropping or tapping devices."[130] The offense also only applies to "nonpublic" transmissions of computer data.[131] This qualification relates only to "the nature of the transmission . . . and not the nature of the data" being transferred.[132] In other words, the data being transmitted may be publicly available, but the parties communicating may wish to remain confidential.[133] This communication can take place from computer to printer, between two computers, or from person to computer (such as typing into a keyboard).[134] For example, the use of common commercial practices, such as "cookies" used to track an individual's surfing habits, are not intended to be criminalized because they are considered be "with right."[135]

This provision does not exhaustively define what sorts of interception are lawful and which ones are unlawful. Therefore, according to the DOJ cybercrime website, nothing in this provision

127. *Id.* at 374.
128. Convention, *supra* note 6, art. 3.
129. *Explanatory Report*, *supra* note 94, art. 3, ¶ 51.
130. *Id.* art. 3, ¶ 53.
131. Convention, *supra* note 6, art. 3.
132. *Explanatory Report*, *supra* note 94, art. 3, ¶ 54.
133. *Id.*
134. *Id.* art. 3, ¶ 55.
135. *Id.* art. 3, ¶ 58.

"would change the U.S. wiretap statute (18 U.S.C. 2511(2)(a)(I)), which specifically allows monitoring by a service provider of traffic on its own network undertaken to protect its rights and property."[136]

c. Article 4 – Data Interference

Article 4, criminalizing the destruction of data, aims "to provide computer data and computer programs with protection similar to that enjoyed by" tangible objects against the intentional infliction of damage.[137] The input of malicious codes, viruses, and Trojan horses is thus covered under this criminal code.[138] Convention parties are granted the freedom to require that "serious harm" be committed when legislating this crime, in which the interpretation of what constitutes "serious harm" is left to the respective government.[139]

The United States' statutory equivalent is the Computer Fraud and Abuse Act of 1986.[140] This section prohibits a person from knowingly transmitting "a program, information, code, or command, and as a result of such conduct, intentionally" causing "damage without authorization, to a protected computer."[141] A "protected computer" is defined as a computer "which is used in interstate or foreign commerce or communication."[142] Damage must also occur to "one or more persons,"[143] but courts have held that "one or more persons" includes corporations.[144] In *United States v. Middleton*, a disgruntled former employee obtained illegal access to his former company's computer system, changed all the administrative passwords, altered the computer's registry, deleted the entire billing system (including programs that ran the billing software), and deleted two internal databases.[145] In response, company employees spent a considerable amount of time repairing the damage and buying new software.[146] The former employee, arrested under section 1030(a)(5)(A), moved to dismiss by alleging that the company was not an "individual" for purposes of the statute.[147] The

136. United States Dep't of Justice, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime*, *at* http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (last visited Feb. 13, 2003) [hereinafter *Frequently Asked Questions*].
137. *Explanatory Report*, *supra* note 94, art. 4, ¶ 60.
138. *Id.* art. 4, ¶ 61.
139. *Id.* art. 4, ¶ 64.
140. Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986) (amending 18 U.S.C. § 1030).
141. 18 U.S.C. §1030(a)(5)(A).
142. *Id.* §1030(g)(e)(2)(B).
143. 18 U.S.C. § 1030(e)(8)(A).
144. United States v. Middleton, 231 F.3d 1207, 1210-1211 (9th Cir. 2000).
145. *Id.* at 1209.
146. *Id.*
147. *Id.*

Court of Appeals disagreed, holding that Congress intended the word "individual" to include corporations.[148]

d. Article 5 – System Interference

Article 5, criminalizing "system interference," aims to prevent "the intentional hindering of the lawful use of computer systems."[149] "Hindering," as used in this Article, must be serious enough to rise to the level of criminal conduct.[150] "The drafters considered as 'serious' the sending of data to a particular system in such a form, size, or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems. . . ."[151] A common example of a hack criminalized under this section would be a "denial of service attack," a malicious code, such as a virus, that prevents or substantially slows the operation of a computer system leaving the common web surfer unable to access a web page.[152] A questionable example is "spamming," a practice whereby a person or program sends huge quantities of email to a voluminous amount of recipients for two possible purposes: (1) to block the communicating function of the system,[153] or (2) to over-expose enough consumers to advertising that sales of a product are generated.[154] It is arguable that spamming could fall under Article 5 when it reaches the point of computer sabotage in the slowing or shutting down of a computer network or service provider. However, a violation under Article 5 must be committed intentionally, and whether a "spammer" who merely mass advertises has the requisite mens rea will be an important issue that the Council and individual countries will need to resolve.[155]

Besides invoking Article 4 (Data Interference), the spreading of a computer virus would fall under this Article as well. One should consider, for example, the "Melissa" virus, which was launched in 1999 and ultimately caused eighty billion dollars in damage.[156] The virus was set to invade a person's address book and send up to fifty

148. *Id.* at 1211.
149. *Explanatory Report*, *supra* note 94, art. 5, ¶ 65.
150. *Id.* art. 5, ¶ 67.
151. *Id.*
152. *Id.*
153. *Id.*
154. Arosnet Policies, *Newsgroup and Email Spamming: What is Spamming?* at http://www.aros.net/policies/spam.shtml (last visited Feb. 12, 2003).
155. *Explanatory Report*, *supra* note 94, art. 5, ¶ 69.
156. Damien Whitworth & Dominic Kennedy, *Author Could Escape Arm of the Law*, TIMES (LONDON), May 5, 2000, at A1, *available at* 2000 WL 2888574.

e-mail messages to addresses stored on the computer.[157] With the rapid spread of the virus and subsequent massive strings of e-mails being sent and received by infected users, companies were forced to shut down their servers.[158]

e. Article 6 – Misuse of Devices

Article 6 establishes, as separate and independent offenses, the intentional commission of illegal acts regarding certain devices that are used in the commission of the named offenses of this Convention.[159] In many cases, black markets are established to facilitate the sale or trade of "hacker tools," or tools used by hackers in the commission of cybercrimes.[160] By prohibiting the production, sale, or distribution of these devices, this Article intends to combat these black market activities.[161] This Article not only covers tangible transfers but also the creation or compilation of hyperlinks facilitating hacker access to these devices.[162] A troubling issue arose with regard to "dual-use devices," or devices that have both a good and evil purpose.[163] In order for the dragnet not to sweep up devices that serve a useful purpose, the drafters intended this Article to relate to devices that "are objectively designed, or adapted, primarily for the purpose of committing an offen[s]e."[164] Finally, in order to avoid overcriminalization, the Article requires both a general intent and also a "specific . . . intent that the device is used for the purpose of committing any of the offen[s]es established in Articles 2 [thru] 5 of the Convention."[165]

f. Article 7 – Computer-Related Forgery

Article 7 outlaws computer-related forgery, or the intentional "input, alteration, deletion, or suppression of computer data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic. . . ."[166] The purpose of this Article is to create a parallel offense to the forgery

157. Kelly Cesare, *Prosecuting Computer Virus Authors: the Need for an Adequate and Immediate International Solution*, 14 TRANSNAT'L LAW. 135, 143 (2001) (discussing the impact of the Melissa virus).
158. *Id.*
159. *Explanatory Report*, *supra* note 94, art. 6, ¶ 71.
160. *Id.*
161. *Id.* art. 6, ¶ 72.
162. *Id.*
163. *Id.* art. 6, ¶ 73.
164. *Id.*
165. *Id.* art. 6, ¶ 76.
166. Convention, *supra* note 6, art. 7.

of tangible documents."[167] National concepts of forgery differ greatly.[168] Some countries base forgery on the "authenticity as to the author of the document," others base forgery on "truthfulness of the statement contained in the document."[169] In either case, the drafters intended that the minimum standard be the authenticity of the issuer of the data, regardless of the correctness of the actual data.[170] Convention parties are permitted to further define the genuineness of the data if they so choose.[171]

g. Article 8 – Computer-Related Fraud

Article 8 makes computer-related fraud illegal.[172] Computer-related fraud is the intentional causing of a loss of property by deletion or alteration of computer data, "interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring without right, an economic benefit for oneself or for another person."[173] Assets such as electronic funds, deposit money, and credit card numbers have become the target of hackers, who feed incorrect data into the computer with the intention of an illegal transfer of property.[174] This Article is specifically intended to criminalize a direct economic or possessory loss of property if the "perpetrator acted with the intent of procuring an unlawful economic gain. . . ."[175] In addition to the general intent requirement, this Article also "requires a specific fraudulent or other dishonest intent to gain an economic or other benefit. . . ."[176] This specific intent requirement is another effort by the drafters to filter serious misconduct from minor crimes.

This Article is an international tool of legislation that is greatly needed. Computer-related fraud in online auction houses, such as eBay, is a growing business for many criminals. The Internet Fraud Complaint Center ("IFCC"), a partnership between the Federal Bureau of Investigation ("FBI") and the National White Collar Crime Center ("NW3C"), reported that 1.3 million transactions per day take place on Internet auction sites.[177] Auction fraud through

167. *Explanatory Report*, *supra* note 94, art. 7, ¶ 81.
168. *Id.* art. 7, ¶ 82.
169. *Id.*
170. *Id.*
171. *Id.*
172. Convention, *supra* note 6, art. 8.
173. *Id.*
174. *Explanatory Report*, *supra* note 94, art. 8, ¶ 86.
175. *Id.* art. 8, ¶ 88.
176. *Id.* art. 8, ¶ 90.
177. INTERNET FRAUD COMPLAINT CENTER, FEDERAL BUREAU OF INVESTIGATION, INTERNET AUCTION FRAUD, May 2001, *at* http://www1.ifccfbi.gov/strategy/AuctionFraud Report.pdf (last

the Internet ranks as the most prevalent type of fraud committed over the Internet, and it comprises sixty-four percent of all fraud reported.[178] This fraud results in a loss of almost four million dollars per calendar year.[179] The creation of a uniform criminal structure that outlaws the practice of fraud across the globe and facilitates the cooperation of countries in policing and preventing fraud in the sales of merchandise online, is a positive step toward securing the Internet as a safe place to do business. This Article will strengthen consumer confidence on the Internet and promote greater usage and integration into our lives.

h. Article 9 – Offenses Related to Child Pornography

Article 9 seeks to strengthen protective measures against sexual exploitation of children by modernizing current criminal law provisions.[180] Many countries, like the United States, already criminalize the traditional production and distribution of child pornography.[181] However, unlike the United States, some countries fail to expand this prohibition to electronic transmissions.[182] The treaty uses the term "minor" to refer to children under the age of eighteen.[183] This is in accordance with the definition of child under the United Nations Convention on the Rights of the Child.[184] However, the drafters recognized that some countries have a lower age for "minors" and allow Convention parties to set "a different age-limit, provided it is not less than 16 years [of age]."[185]

The United States already has a law on the books dealing with child pornography.[186] The Protection of Children from Sexual Predators Act makes it illegal to knowingly possess one or more child pornographic images that have been transmitted in interstate or foreign commerce, which includes possession of such images on a computer.[187] If the treaty were to be ratified, it is likely the defenses attempted by defendants to prosecution under United States law would also be attempted in prosecutions under the Convention. Defendants have argued, albeit unsuccessfully, that

---

visited Feb. 12, 2003).

178. *Id.*

179. *Id.*

180. *Explanatory Report*, *supra* note 94, art. 9, ¶ 91.

181. *Id.* art. 9, ¶ 93.

182. *Id.*

183. *Id.* art. 9, ¶ 104.

184. *Id.*

185. *Id.*

186. 18 U.S.C. § 2252 (2000), *as amended by* Protection of Children from Sexual Predators Act of 1998, Pub. L. No. 105-314, § 203(a)(1), 112 Stat. 2977, 2978 (1998).

187. *See id.* § 2252(a)(4)(B).

computer files are not "visual depictions" as defined in the United States Code.[188] This apparently would not change, since the treaty makes it a crime to possess child pornography on a computer system, thus making any child pornographic image on a computer a criminal offense.[189] Defendants have also argued that the images had been deleted, and thus, the images were not in their "possession" within the meaning of section 2252.[190] However, the government can point to other sources of evidence to prove possession, such as floppy disks, CD-Roms, and computer logs.[191]

Article 9 also makes virtual child pornography unlawful. Virtual child pornography is similar to real child pornography in that it appears to depict minors in sexually explicit situations, but it has one significant difference: it is produced through means that do not involve the use of children.[192] This can be accomplished through the use of adult actors that look like children, through computer-generated images, or through a process known as "morphing."[193] Morphing is the alteration of innocent pictures of children into sexually explicit depictions.[194]

The production, possession, and distribution of virtual child pornography was unlawful under 18 U.S.C. §§ 2252 and 2256. However, in *Ashcroft v. Free Speech Coalition*, the United States Supreme Court held that two key provisions of § 2256 were overbroad and unconstitutional.[195] This holding has tremendous impact on any future ratification of the Convention into United States law. *Ashcroft* held that the statute criminalized speech that is protected under the First Amendment.[196] The government, in arguing in favor of criminalizing virtual child pornography, made similar arguments to those of the drafters of the Convention.[197] First, the government argued that virtual child pornography can be used to lure or seduce children into performing illegal acts.[198] The Court found this argument unpersuasive because it was not the least restrictive means necessary to accomplish the government's objective.[199] The Court stated that many inherently innocent objects could be used to seduce children, including candy and video games,

188. United States v. Hocking, 129 F.3d 1069, 1070 (9th Cir. 1997).
189. Convention, *supra* note 6, art. 9.
190. United States v. Lacy, 119 F.3d 742, 747 (9th Cir. 1997).
191. *Id.*
192. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 239 (2002).
193. *Id.* at 242.
194. *Id.*
195. *Id.* at 258 (holding 18 U.S.C. §§ 2256(8)(B), 2256(8)(D) unconstitutional as overbroad).
196. *Id.* at 256-58.
197. *Explanatory Report*, *supra* note 94, art. 9, ¶ 93.
198. *Ashcroft*, 535 U.S. at 251.
199. *Id.* at 252-54.

and therefore it is axiomatic that the government cannot ban speech intended for adults merely because it may fall into the hands of children.[200] Next, like the Convention's drafters, the government argued that virtual child pornography whets the appetites of pedophiles and encourages them to engage in illegal conduct.[201] The Court responded that this is also not a justification for the statute, because the government "cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts."[202] This is a cornerstone upon which the First Amendment was built.[203] The government next argued that virtual images are indistinguishable from real ones, part of the same market, and often exchanged.[204] The Court found this unpersuasive as well, stating that virtual images cannot be "virtually indistinguishable," because otherwise the illegal images would be driven from the market by the indistinguishable substitutes. The Court reasoned that "few pornographers would risk prosecution by abusing real children if fictional, computerized images would suffice."[205]

Finally, the government argued that the "possibility of producing images by using computer imaging makes it . . . difficult . . . to prosecute those who produce pornography by using real children."[206] The government felt it would have difficulty in saying whether the pictures were made by using real children or by using computer imaging, and therefore the only solution is to prohibit both kinds of images.[207] The Court was unpersuaded by this argument as well, holding that the government cannot prohibit lawful speech as a means to ensnare unlawful speech.[208]

The application of the arguments made in *Ashcroft* are extremely relevant to the justifications for Article 9, as their policy justifications and prohibitions run parallel. As the situation currently stands, with sections 2256(8)(B) and 2256(8)(D) unconstitutional, the United States would be forced to take a limited reservation to Article 9 should it decide to ratify the Convention.

---

200. *Id.*
201. *Id.* at 253.
202. *Id.* (*quoting* Stanley v. Georgia, 394 U.S. 557, 566 (1969)).
203. *Ashcroft*, 535 U.S. at 253.
204. *Id.* at 254.
205. *Id.*
206. *Id.*
207. *Id.*
208. *Id.*

i. Article 10 – Offenses Related to the Infringements of Copyright and Related Rights

Additionally, Article 10 relates to those offenses that "are among the most commonly committed offen[s]es on the Internet. . . . The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent."[209] Copyright offenses "must be committed 'willfully' for criminal liability to apply."[210] "Willfully" was substituted for "intentionally," because this term is employed in the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"), which governs the obligations to criminalize copyright violations.[211]

j. Article 11 – Attempt and Aiding or Abetting

Article 11 establishes offenses related to attempting or aiding and abetting "the commission of the offenses defined in the Convention."[212] Liability under this Article arises when "the person who commits a crime established in the Convention is aided by another who also intends that the crime be committed."[213] For example, the transmission of a virus is an act that triggers the operation of a number of articles of the Convention. However, transmission can only take place through an ISP. "A service provider that does not have the requisite criminal intent cannot incur liability under this section."[214] Therefore, there is no duty under this section for an ISP to actively monitor content in order to avoid criminal liability under this section.[215]

k. Article 12 – Corporate Liability

This Article "deals with the liability of legal persons."[216] Four conditions must be met in order to establish liability.[217] First, a described offense must have been committed.[218] Second, it must have been committed to benefit a legal person.[219] Third, a person who is in a "leading position" must be the one who committed the

209. *Explanatory Report*, *supra* note 94, art. 10, ¶ 107.
210. *Id.* art. 10, ¶ 113.
211. *Id.*
212. *Id.* art. 11, ¶ 118.
213. *Id.* art. 11, ¶ 119.
214. *Id.*
215. *Id.*
216. *Id.* art. 12, ¶ 123.
217. *Id.* art. 12, ¶ 124.
218. *Id.*
219. *Id.*

offense, which could include a director.[220] Finally, "the person who has a leading position must have acted . . . within the scope of his or her authority to engage the liability of the legal person."[221] In the case of an offense committed by an agent or employee of the corporation, the offense must have been made possible by the leading person's "failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the [corporation]. . . ."[222] Appropriate and reasonable measures are determined by examining the type of business, its size, the standards or established business practices, and other like factors.[223] However, liability of a corporation does not exclude individual liability.[224]

l. Article 13 – Sanctions and Measures

Article 13 completes Section 1 of the Convention by requiring Convention parties to provide criminal sanctions that are "effective, proportionate, and dissuasive" and "include the possibility of imposing prison sentences."[225] The drafters intended that this Article leave discretionary power to Convention parties "to create a system of criminal offences and sanctions" that are compatible with their existing national legal systems.[226]

6. Convention Section 2 – Prosecutorial and Procedural Requirements

The articles in this section describe procedural measures that Convention parties must take "at the national level for the purpose of criminal investigation of the offences established in Section 1."[227] This section is intended to overcome some of the challenges associated with policing the ever-expanding information highway.[228] Some of those challenges are: (1) the difficulty in identifying the perpetrator, (2) the difficulty in determining "the extent and impact of the criminal act," (3) the difficulty in dealing with the volatility of electronic data, and (4) the difficulty in maintaining the speed and secrecy vital in the success of a cybercrime investigation.[229]

---

220. *Id.*
221. *Id.*
222. *Id.* art. 12, ¶ 125.
223. *Id.*
224. *Id.* art. 12, ¶ 127.
225. *Id.* art. 13, ¶ 128.
226. *Id.* art. 13, ¶ 130.
227. *Id.* art. 13, § 2, ¶ 131.
228. *Id.* art. 13, § 2, ¶ 132.
229. *Id.* art. 13, § 2, ¶ 133.

These challenges pose major problems for investigators since electronic data can be altered, moved, or deleted within seconds, which may very well be the only evidence in a criminal investigation.[230]

One way in which the Convention overcomes these problems is by adapting traditional procedures, like search and seizure, to an ever-changing technological landscape.[231] However, in order to make these traditional crime investigation methods effective, new measures have been created.[232] Examples of those measures include the expedited preservation of data, "[the] real-time collection of traffic data, and the interception of content data."[233]

a. Article 15 – Conditions and Safeguards

Article 15 establishes minimum safeguards upon the procedures instituted within Convention party legal systems, which may be provided constitutionally, legislatively, or judicially.[234] Parties are to ensure that their safeguards provide for the adequate protection of human rights and liberties.[235] However, the Convention only refers to parties who have human rights obligations under previously signed treaties.[236] The Convention seemingly leaves the point moot for parties that have not signed any international human rights treaties.[237] Opponents to the Convention argue that the treaty infringes upon basic human rights and liberties, most notably the right to privacy.

b. Article 16 – Expedited Preservation of Stored Computer Data

Article 16 relates to the expedited preservation of stored computer data, a new measure implemented in order to facilitate the investigation of cybercrimes.[238] This Article applies only to data that has already been collected and retained by ISPs.[239] One must not confuse "data preservation" with "data retention."[240] For purposes of this Article, data retention merely relates to the protection from deterioration of data already existing in stored

230. *Id.*
231. *Id.* art. 13, § 2, ¶ 134.
232. *Id.*
233. *Id.*
234. *Id.* art. 15, ¶ 145.
235. *Id.*
236. Convention, *supra* note 6, art. 15.
237. *Id.*
238. *Id.* art. 16.
239. *Explanatory Report*, *supra* note 94, tit. 2, ¶ 149.
240. *Id.* art. 15, tit. 2, ¶ 151.

form.[241] On the other hand, data retention, or the process of storing and compiling data, does not apply under this Article.[242] The concept of "data preservation" is a new legal power in many domestic laws, brought about by because of the ability for computer data to be destroyed or lost through careless handling and storage processes.[243] The statute operates in one of two ways: (1) the competent authorities in the Convention party country simply access, seize and secure the relevant data, or (2) where a reputable business is involved, competent authorities can issue an order to preserve the relevant data.[244] Convention parties are thus required to introduce a power that would enable law enforcement authorities to order the preservation of data for a particular period of time not exceeding 90 days.[245] Data such as this is frequently stored only for short periods of time, since these laws are designated to protect privacy and because the costs are high when preserving this type of data.[246]

c. Article 17 – Expedited Preservation and Partial Disclosure of Traffic Data

Article 17 establishes specific obligations with respect to the preservation of "traffic data" under Article 16. In addition, it provides for quick disclosure of some "traffic data," so authorities can identify the person or persons who have distributed such things as child pornography or computer viruses.[247] Recall that "traffic data" merely indicates where and how a virus or email was transmitted, but not who transmitted it or what it contained.[248] This section is most important when considering the following example. Often, more than one service provider is

> involved in the transmission of a communication. Each service provider may possess some 'traffic data' related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the

241. *Id.*
242. *Id.* art. 15, tit. 2, ¶¶ 151, 152.
243. *Id.* art. 15, tit. 2, ¶ 155.
244. *Id.*
245. *Id.* tit. 2, ¶ 156.
246. *Id.* art. 17, ¶ 166.
247. *Id.* art. 17, ¶¶ 165, 166.
248. *Id.* art. 1(d), ¶¶ 28-31.

> [actual] passage of the communication through its system or has been provided [by] other [ISPs].[249]

For commercial, security or technical purposes, sometimes "traffic data" is shared among the service providers involved.[250]

> In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the [important 'traffic data'] to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.[251]

The preferred method for accomplishing the expedited preservation and partial disclosure of "traffic data" is to enact legislation enabling authorities to obtain a single order, the scope of which would apply to all ISPs involved in a communication and "[t]his comprehensive order could be served sequentially on each service provider identified in the order."[252]

d. Article 18 – Production Order

Article 18 relates to production orders, which specifically allow "competent authorities to compel a person in its territory to provide specified stored computer data" or to compel an ISP to provide subscriber information.[253] This Article strictly relates to production of stored or existing data, not "traffic data" or "content data related to future communications."[254] Production orders precede search and seizure as a means of obtaining specific data.[255]

e. Article 19 – Search and Seizure of Stored Computer Data

Article 19, which relates to search and seizure, aims at modernizing and harmonizing differing domestic laws.[256] In many

249. *Id.* art. 17, ¶ 167.
250. *Id.*
251. *Id.*
252. *Id.* art. 17, ¶ 168.
253. *Id.* art. 18, ¶ 170.
254. *Id.*
255. *Id.* art. 18, ¶ 175.
256. *Id.* art. 19, ¶ 184.

countries, stored computer data is not considered a tangible object, and thus, cannot be searched and seized in the same manner as a tangible object.[257] This Article aims to establish an equivalent search and seizure power ranging from tangible objects to stored computer data.[258] The preconditions required to search and seize traditional property, such as probable cause, will remain the same.[259]

However, additional procedural provisions are necessary "to ensure that computer data can be obtained in a manner . . . equally effective to a search and seizure [for] a tangible data carrier."[260] There are a number of reasons for this:

> [F]irst, the data is in intangible form. . . . Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as [tangible goods]. . . . Third, due to [interconnected networks], data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system.[261]

In the second case, either the physical medium on which the intangible data is stored must be seized or taken away, or a copy of the data must be made in either tangible form, such as a computer printout, or in intangible form, such as a diskette, before the tangible or intangible medium containing the copy can be seized and taken away.[262]

f. Article 20 – Real-Time Collection of Traffic Data

Article 20 takes into account the importance of collecting "traffic data" to determine the source or destination of the cybercrime being committed.[263] "Like real-time interception of content data, real-time collection of 'traffic data' is only effective if undertaken without the knowledge" of the suspect.[264] Therefore, ISPs knowledgeable about the interception must be required to maintain complete secrecy in order for this to be successful.[265] One way to achieve the necessary

257. *Id.*
258. *Id.*
259. *Id.* art. 19, ¶ 186.
260. *Id.* art. 19, ¶ 187.
261. *Id.*
262. *Id.*
263. *Id.* art. 20, ¶ 216.
264. *Id.* art. 20, ¶ 225.
265. *Id.*

secrecy is by relieving the service provider of any contractual or legal obligation to notify its customers about the data being collected.[266] This can be accomplished through a law requiring confidentiality, or by threatening an obstruction of justice charge against the ISP should it fail.

g. Article 21 –Interception of Content Data

Article 21, "interception of content data," has traditionally been carried out through governmental monitoring of telephone conversations.[267] However, recently, the rising popularity of communication through the Internet has made "tapping the net" a priority for law enforcement officials. The fact that computers are capable of transmitting not only words but also visual images and sounds makes it even easier for crimes to be committed.[268] "Content data refers to the communication content of the communication," or in other words, the gist of the message.[269]

h. Article 22 – Jurisdiction

Article 22 simply establishes that member countries must enact laws enabling them to have jurisdiction over all the previous crimes described above should they occur in any one of four places: (1) in the member country's territory, (2) on board a ship flying the flag of that country, (3) on board an aircraft registered under the laws of that country, or (4) outside the territory of the country but committed by one of its nationals.[270] A party would establish territorial jurisdiction if the person attacking the computer system and the victim were located within the country, or where the victim was inside the territory but the attacker was not.[271] The remaining jurisdictional sections are rather self-explanatory.

7. Convention Section 3 – International Cooperation

This section contains a series of provisions relating to the mutual legal assistance member countries must afford each other under the Convention.[272] This section causes grave concern for many United States businesses and interest groups.[273] This concern

266. *Id.* art. 20, ¶ 226.
267. *Id.* art. 21, ¶ 228.
268. *Id.*
269. *Id.* art. 21, ¶ 229.
270. Convention, *supra* note 6, art. 22.
271. *Explanatory Report*, *supra* note 94, art. 22, ¶ 233.
272. *Id.* ch. 3, ¶ 240.
273. *See* Mike Godwin, *International Treaty on Cybercrime Poses Burden on High Tech*

stems from the fact that although it may not be such a big deal to have the United States government wield greater power, the same new powers will also be given to member countries that may not "have a strong tradition of checks and balances on police power."[274] United States companies do not want foreign investigators searching through domestic computer systems based on a warrant issued under the Convention.[275]

The following example illustrates why United States companies should have cause for concern. Suppose a Seattle University law student, while researching a potential research topic, corresponds by e-mail with an Al-Qaeda member in Italy. A few days later the unknowing student finds federal agents examining the files on his home computer. The agents also visit the student's ISP, Seattle University, to retrieve records of the student's computer usage. The agents are basing their authority on a warrant that was issued by Italian authorities, which allows them to search for Al Qaeda locations and documents. Italian officials framed their warrant in terms of "suspected terrorist activity." Maybe the student should have anticipated this scenario, given the vigor with which the world is cracking down on Al-Qaeda members. Even if the law student is willing to run the risk, and bear the burden, of this kind of search, should Seattle University?

Larger ISPs, such as America Online, get dozens of search warrants and subpoenas every month. This treaty would change everything by not only requiring them to respond to those submitted by United States law enforcement officials, they would also have to respond to warrants and court orders from dozens of nations. All ISPs, phone companies, and other businesses would be forced into cooperating with investigations. This equates to higher storage, investigative and retrieval costs for this extra data. These higher costs would likely be passed down to the consumer in the form of higher monthly service rates.

The opposing argument is plausible, however; ISPs should expect this sort of intrusion as a cost of doing business in the Internet era. The problem again lies in the fact that these added costs will be passed down to the consumer. Additionally, if two companies have cabled together two computers, the second company could be forced to comply with investigations of other ISPs, which would cause even more problems.

Companies, IP WORLDWIDE, Apr. 4, 2001, *at* http://www.law.com/servlet/ContentServer?pagename=OpenMarket/Xcelerate/View&c=LawArticle&cid=1015973978355&live=true&cst=1&pc=0&pa=0.

274. *Id.*

275. *Id.*

a. Article 23 – General Principles Relating to International Cooperation

Article 23 begins this section by outlining "general principles" of mutual legal assistance. Cooperation is to be extended for all crimes described above, as well as for the collection of data and evidence in electronic form for the criminal offense.[276]

b. Article 24 – Extradition

Article 24 deals with extradition of criminals between member countries. "The obligation to extradite applies only to" those crimes committed in Articles 2 thru 11.[277] A threshold penalty also exists to minimize the massive extradition of criminals.[278] Under certain offenses, like illegal access (Article 2) and data interference (Article 4), member countries are permitted to impose short periods of incarceration.[279] Accordingly, extradition can only be sought where the maximum penalty is at least one year in jail.[280]

Important policy considerations are furthered by adding an extradition provision. By all the countries prosecuting the same crimes and sending criminals from one jurisdiction to another, criminals effectively cannot hide from the law when committing a crime within the Convention's jurisdiction. Because the deterrence of crime is an important policy goal of any criminal law statute, as well as this Convention, the extradition provision strengthens the entire Convention. In fact, extradition laws governing computer crimes are "hopelessly outdated and therefore, lagging behind the forces they are trying to regulate."[281] This lack of uniformity results in lax treatment of cybercriminals, allowing them to escape law enforcement officials by fleeing to countries unwilling to extradite a suspected criminal. This Convention provision is an important step in harmonizing extradition laws between member countries and bringing reluctant countries up to date.

---

276. *Explanatory Report*, *supra* note 94, art. 23, ¶ 243.
277. *Id.* art. 24, ¶ 245.
278. *Id.*
279. *Id.*
280. *Id.*
281. Cesare, *supra* note 157, at 153 (*quoting* John T. Soma et. al., *Transnational Extradition for Computer Crimes: Are New Treatises and Laws Needed?* 34 HARV. J. ON LEGIS. 317, 317-18 (1997)).

c. Article 25 – General Principles Relating to Mutual Assistance

Article 25 requires mutual assistance "to the widest extent possible."[282] Provisions from this Article include communications which are made through email and other means. For the most part, this treaty section is considered harmless, and therefore this section is uncontested by civil libertarians.

d. Article 26 – Spontaneous Information

Article 26 discusses "spontaneous information" and refers to those times when a member country obtains vital information to a case that it believes may assist another member country in a criminal investigation or proceeding.[283] In these situations, the member country that does not have the data may not even know it exists, and thus will never generate a request for such data. This section empowers the country with the "spontaneous information" to forward it to applicable foreign officials without a prior request.[284] While this might seem obvious and needless to a United States citizen, this provision is very useful in an multilateral treaty such as this, because under the laws of some member states, "a positive grant of legal authority is needed in order to" effectuate the provision of assistance absent a request.[285]

e. Article 27 – Procedures Pertaining to Mutual Assistance Requests In the Absence of Applicable International Agreements

Article 27 relates to mutual assistance in the absence of applicable international agreements. In other words, it establishes a mutual set of rules when parties are not already obliged under the European Convention on Mutual Assistance in Criminal Matters and its Protocol, or other similar treaties.[286] The terms of applicable agreements can be supplemental to the Convention as long as member countries continue to also apply the terms of this provision.[287] Parties must establish a central authority "responsible for sending and answering requests for [assistance]."[288] This is particularly helpful in expediting the rapid transmission of information in combating and prosecuting cybercrimes.[289]

---

282. *Explanatory Report*, *supra* note 94, art. 25, ¶ 253.
283. *Id.* art. 26, ¶¶ 260, 261.
284. *Id.* art. 26, ¶ 260.
285. *Id.*
286. *Id.* art. 27, ¶ 262.
287. *Id.* art. 27, ¶ 263.
288. Convention, *supra* note 6, art. 27.
289. *Explanatory Report*, *supra* note 94, art. 27, ¶ 265.

One important objective of this section "is to ensure that its domestic laws governing the admissibility of evidence are fulfilled," so that the evidence can be used before the court.[290] To ensure that this result is accomplished, member countries are required to "execute requests in accordance with procedures specified by the requesting party" so its domestic laws are not infringed.[291] This is required, unless the request violates the host country's domestic laws, then the county is not obliged to follow.[292] For example, a procedural requirement of one party may be that a witness statement be given under oath. "Even if the requested party does not" have this requirement, "it should honur [sic] the requesting party's request."[293]

f. Article 28 – Confidentiality and Limitation on Use

Article 28 specifically provides for confidentiality and limitations on use of information in order to preserve sensitive materials of a host country. This Article only applies when no mutual assistance treaty exists.[294] When such a treaty already exists, its provision apply in lieu of this provision, unless the countries agree otherwise.[295] Two types of confidentiality requests can be made by member countries. First, a party "may request that the information or material furnished be kept confidential where the request could not be complied with in the absence of such condition."[296] "Second, the requested party may make furnishing of the information or material dependent upon the condition that it not be used for investigations or proceedings other than those stated in the request."[297]

g. Article 29 – Expedited Preservation of Stored Computer Data

Article 29, mutual assistance related to the expedited preservation of stored computer data, is in most respects identical to Article 16, except that it relates to international cooperation. Drafters agreed that a mechanism needed to be in place to ensure the availability of this type of data when a lengthier and more involved process of a mutual assistance request is handled.[298]

---

290. *Id.* art. 27, ¶ 267.
291. *Id.*
292. *Id.*
293. *Id.*
294. *Id.* art. 28, ¶ 276.
295. *Id.*
296. *Id.* art. 28, ¶ 277.
297. *Id.* art. 28, ¶ 278.
298. *Id.* art. 29, ¶ 282.

h. Article 30 – Expedited Disclosure of Preserved Traffic Data

Likewise, Article 30, mutual assistance related to the expedited disclosure of preserved "traffic data," is the mutual assistance arm of Article 17.[299] Therefore, it needs little discussion.

i. Article 31 – Mutual Assistance Regarding Accessing of Stored Computer Data

Article 31 requires that each member country have the ability to search, access, or seize "data stored by means of a computer system located within its territory" for the benefit of another member country.[300] Paragraph one authorizes a member country to request this type of assistance, and paragraph two requires the host country to provide it.[301]

j. Article 32 – Trans-Border Access to Stored Computer Data With Consent or Where Publicly Available

Article 32 deals with "[t]rans border access to stored computer data with consent or where publicly available," which merely makes it permissible for a publicly available source of data to be available to a member country unilaterally and without a mutual assistance request, while at the same time, not preparing a comprehensive, legally binding system.[302]

k. Article 33 – Mutual Assistance Regarding the Real-Time Collection of Traffic Data

Article 33 makes it law that each party is obliged to collect real time "traffic data" for another member country.[303]

l. Article 34 – Mutual Assistance Regarding the Interception of Content Data

Article 34 is another hot button issue in this treaty because it discusses the cooperation and sharing of information obtained through means such as eavesdropping and wiretapping. In addition, it relates to the mutual assistance regarding the interception of content data.[304] The assistance provided in this

299. *Id.* art. 30, ¶ 290.
300. *Id.* art. 31, ¶ 292.
301. *Id.*
302. *Id.* art. 32, ¶ 293.
303. *Id.* art. 33, ¶ 295.
304. *Id.* art. 34, ¶ 297.

provision is limited by the mutual assistance regimes already in place and the domestic laws already enacted.[305]

m. Article 35 – 24/7 Network

Article 35 is a very interesting provision. The "24/7 network" is a way to effectively combat crimes committed through the use of computer systems when those crimes require a rapid response. This Article obligates each country to designate a point of contact that is available 24 hours per day, 7 days a week.[306] This Article was considered by the drafters to be one of the most important means of effectively responding to law enforcement challenges posed by cybercrimes.[307]

8. Convention Section 4 – Final Provisions

a. Article 36 – Signature and Entry Into Force

Article 36, entitled "Signature and entry into force," allows non-COE states to become signatories, in addition to COE states who had participated in drafting the Convention.[308] The Convention does not enter into force until five countries have ratified it, three of which must be COE states.[309]

b. Article 37 – Accession to the Convention

Article 37 deals with those states which have not participated in the drafting but, nevertheless, are interested in signing and ratifying the treaty.[310] A formal procedure is required "to invite a non-member State to accede" which requires a two-thirds majority to be present in addition to a "unanimous vote of the representatives of the contracting parties" in order for the state to accede.[311]

c. Article 38 – Territorial Application

Article 38, "territorial application," simply provides that a member country must express to which territories it intends the Convention to apply upon signature and ratification.[312]

---

305. *Id.*
306. *Id.* art. 35, ¶ 298.
307. *Id.*
308. *Id.* art. 36, ¶ 304.
309. *Id.* art. 36, ¶ 305.
310. *Id.* art. 37, ¶ 306.
311. *Id.*
312. Convention, *supra* note 6, art. 38(1).

d. Article 39 – Effects of Convention

Article 39 relates to the Convention's relationship with other international agreements, particularly how pre-existing conventions of the COE should relate to each other or to other treaties concluded outside the COE.[313] In particular, member countries should adhere to "the rule of interpretation lex specialis derogat legi generali," or in other words, precedent should be given to the rules contained in this Convention.[314]

e. Article 40 -- Declarations

Article 40, "[d]eclarations," refers to certain articles contained within the Convention that permit parties to include specific "additional elements which modify the scope of the provisions."[315] Also, these elements were added to accommodate certain legal differences between member countries.[316] These "should be distinguished from 'reservations,' which permit a party to exclude or modify the legal effect of certain obligations set forth in the Convention."[317]

f. Article 41 – Federalism Clause

Article 41 is another important clause added to the Convention. The "federalism clause" allows for a special kind of declaration that is intended to accommodate the difficulties certain countries might face with regimes that distribute power between central and regional authorities.[318] The Convention was originally crafted with countries that had non-federalist governmental regimes in mind. In other words, the Convention was crafted with European countries in mind, which have one single police power. Countries such as the United States that have federal—as well as state—laws, would have been unable to sign the treaty without a federalism clause.[319] The reason is that some computer crimes committed wholly within a state would be considered state crimes, even though the federal government could ratify the treaty. Additionally, if the individual states did not consent to the Convention application, or consent to the new federal law, then the treaty would not extend to all

313. *Explanatory Report*, *supra* note 94, art. 39, ¶ 308.
314. *Id.* art. 39, ¶ 309.
315. *Id.* art. 40, ¶ 315.
316. *Id.*
317. *Id.*
318. *Id.* art. 41, ¶ 316.
319. *Id.* art. 41, ¶ 317.

territories within a state.[320] The COE added this clause so countries, such as the United States, would ratify this agreement. This clause is a source of controversy for many non-federalist countries because they are skeptical of the extent to which non-federalist countries can convince their constituent state governments to adhere to the treaty provisions.

g. Articles 42 & 43 – Reservations and Status and Withdrawal of Reservations

Articles 42 and 43 allow certain reservations to be made at the time of signature or ratification for those allowable reservations enumerated within the Convention.[321]

h. Article 44 -- Amendments

Article 44 allows for amendments to be made to the Convention.[322] Any amendments adopted would come into force only when all of the member countries "have informed the Secretary General of their acceptance."[323]

i. Article 45 – Settlement of Disputes

Article 45 "provides that the European Committee on Crime Problems ("CDPC") should be kept informed about the interpretation and application of the provisions of the Convention."[324] Three means of dispute resolution are provided within this section, which are the CDPC, "an arbitral tribunal or the International Court of Justice" ("ICJ").[325]

j. Article 46 – Consultation of the Parties

Article 46 creates a framework for the Parties to consult regarding implementation of the Convention, the effect of significant legal, policy or technological developments pertaining to the subject of computer or computer related crime and the collection of evidence in electronic form, and the possibility of supplementing or amending the Convention.[326]

---

320. See id.
321. *Id.* art. 42, ¶¶ 320, 321.
322. Convention, *supra* note 6, art. 44.
323. *Explanatory Report*, *supra* note 94, art. 44, ¶ 325.
324. *Id.* art. 45, ¶ 326.
325. *Id.* art. 45, ¶ 327.
326. *Id.* art. 46, ¶ 328.

k. Article 47 -- Denunciation

Article 47 permits a member country to denounce the Convention.[327] A country's denunciation would "become effective on the first day of the month following the expiration of a period of three months after the date of receipt" and notification by the Secretary General.[328]

l. Article 48 – Notification

Article 48 requires notification to member countries of signatories and ratifications when they occur.[329]

m. Secret "Second Protocol"

Additionally, the COE may add a secret 'Second Protocol' to the treaty, which would cover the decoding of terrorist messages on the Internet.[330] It is certain that this new addition will come under heavy attack, particularly since privacy groups and civil libertarians have strongly voiced their opposition to the "existing cybercrime treaty for the last two years."[331]

IV. THE ROAD AHEAD

Before ratification by the United States, the Convention will face a myriad of oppositional forces. Those opposing the Convention make a number of compelling arguments: (1) the Convention curtails freedom of expression online, (2) the Convention overextends the investigative powers of police and governmental organizations, (3) the Convention demands too much of companies and individuals by requiring them to provide law enforcement with far greater information than is now the norm under most telecommunications laws, and (4) the Convention infringes upon citizen civil liberties.

The second argument made by those opposed to the Convention is that the government is granted an excessive amount of investigatory power, which is best illustrated in the example of call data vs. "traffic data." Presently, law enforcement agencies are allowed to seek call related data, which includes the phone numbers that are dialed and the duration of the calls. However, under the

---

327. Convention, *supra* note 6, art. 47(1).
328. *Id.* art. 47(2).
329. *Id.* art. 48.
330. *Council of Europe—Treaty Change May Allow Greater Surveillance of Terrorists,* PERISCOPE-DAILY DEF. NEWS CAPSULES, Feb. 21, 2002, *available at* 2002 WL 5970273.
331. *Id.*

Convention, law enforcement authorities would have the right to wide-ranging "traffic data," which includes the source, destination, and duration of calls, as well as the type of traffic or the sort of services consulted. Such a request could force an ISP to inform law enforcement agencies that a client visited a particular website for thirty minutes, downloaded ten images, and then sent emails to three specific addresses. Whether this is a violation of a person's right to privacy is an issue hotly contested.

The third argument touches upon the corporate opponents' Convention concerns. ISPs and other related businesses are reluctant to divulge their confidential client records, known as "subscriber data," at the whim of an investigating governmental agency. Companies are also concerned with the increased costs associated with retaining and preserving data should an order be served upon the company to do so. In all likelihood, however, these costs will be passed along to the consumer in the form of higher connection and subscriber fees. Thus, it is ultimately the consumer that will need to weigh the importance of policing cybercrime with the increased cost associated with Internet access when deciding whether to support the Convention.

The fourth argument, that civil liberties will be infringed, appears to be an unfounded concern. Article 15 requires member countries "to establish conditions and safeguards to be applied to the" governmental powers established in Articles 16 thru 21.[332] Those conditions and safeguards are required "to protect human rights and liberties."[333] Article 15 in fact "lists some specific safeguards, such as requiring judicial supervision, that should be applied where appropriate in light of the power or procedure concerned."[334]

V. CONCLUSION

Cybercrimes are not confined within national borders. A criminal armed with a computer and a connection has the capability to victimize people, businesses, and governments anywhere in the world. The criminal can commit violent crimes, participate in international terrorism, sell drugs, commit identity theft, send viruses, distribute child pornography, steal intellectual property and trade secrets, and illegally access private and commercial computer systems. These criminals can hide their tracks by weaving their communications through numerous ISPs.

---

332. *Frequently Asked Questions, supra* note 136.
333. *Id.*
334. *Id.*

For example, consider a computer hacker in Vancouver, British Columbia, who disrupts a corporation's communications network in Seattle, Washington. Before accessing the corporation's computer, he routes his communication through ISPs in Japan, Italy, and Australia. In such a case, Canadian law enforcement would need assistance from authorities in Tokyo, Rome and Sydney before discovering that the criminal is right in their own backyard.

International crimes such as these have impeded law enforcement efforts in ways never before contemplated. While the Internet is borderless for criminals, law enforcement agencies must respect the sovereignty of other nations. Thus, cooperation with foreign law enforcement agencies in fighting cybercrimes is paramount to any effort to catch these criminals. Unfortunately, differing legal systems and disparities in the law often present major obstacles. This article is intended to be the first inclusive survey and analysis of the Council of Europe's Convention on Cybercrime; the first international legislation designed to harmonize legal systems and those disparities in the law that make combating cybercrime so difficult. This article analyzed critical opinion as well as the drafters' intent regarding specific Convention provisions, while also explaining the purpose of the different articles. It also examined a select number of provisions in depth, determining their impact upon existing United States cybercrime laws. Finally, the author of this article has intended to remain neutral on the topic of whether the Convention is ultimately a positive or negative step forward for both the United States and the world, with the intent that the reader can form his or her own educated opinion upon weighing some of the issues raised in this comment.