UIC John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 2 *Journal of Computer & Information Law - Winter 2005*
Article 4

Winter 2005

The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?, 23 J. Marshall J. Computer & Info. L. 329 (2005)

Miriam F. Miquelon-Weismann

THE CONVENTION ON CYBERCRIME: A HARMONIZED IMPLEMENTATION OF INTERNATIONAL PENAL LAW: WHAT PROSPECTS FOR PROCEDURAL DUE PROCESS?

MIRIAM F. MIQUELON-WEISMANN†

> [C]riminal law harmonization is indispensable where a national control is no longer possible . . .: where there is an antagonism between globally operating perpetrators and national criminal law systems . . . In this global area of 'cyberspace,'at least common minimum rules are necessary . . . . On the other hand, there is no urgency to harmonize the *organizational rules* of criminal procedural law . . . highly related to [national differences] in cultural and historical developments . . . .[1]

I. INTRODUCTION

A. THE OPERATIVE DOCUMENTS

The CoE Convention provides a treaty-based framework that imposes three necessary obligations on the participating nations to:

1. enact legislation criminalizing certain conduct related to computer systems;
2. create investigative procedures and ensure their availability to domestic law enforcement authorities to investigate cybercrime offenses, including procedures to obtain electronic evidence in all of its forms; and,
3. create a regime of broad international cooperation, including assistance in extradition of fugitives sought for crimes identified under

† Associate Professor, Southern New England School of Law, formerly United States Attorney Southern District of Illinois and served as Assistant Special Counsel to the Office of Special Counsel, John C. Danforth, WACO Investigation.

1. Prof. Dr. Ulrich Sieber, *Memorandum On A European Penal Code*, in Juristenzeitung 369, §§ C(1)(a), C(2)(b) (1997), (available at http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/article/EMPC/EMPC_englisch) (copy on file with Author).

the CoE Convention.[2]

Notably, the CoE Convention contains significant restrictive language in the areas of transborder search and seizure and data interception, deferring authority to domestic laws and territorial considerations.[3] Also, it does not supercede pre-existing mutual legal assistance treaties ("MLATs") or other reciprocal agreements between parties.

The Official Explanatory Report, accompanying the CoE Convention, was formally adopted by the CoE's Committee of Ministers on November 8, 2001 (the "CoE Explanatory Report").[4] The CoE Explanatory Report provides an analysis of the CoE Convention. Under established CoE practice, such reports reflect the understanding of the parties in drafting treaty provisions and are accepted as fundamental bases for interpretation of CoE conventions,[5] but they do not provide an authoritative interpretation.[6]

B. What is Cybercrime?

Both international cybercrime and domestic cybercrime embrace the same offense conduct, namely, computer-related crimes and traditional offense conduct committed through the use of a computer. International cybercrime expert, Dr. Professor Ulrich Sieber, observes that:

> The ubiquity of information in modern communication systems makes it irrelevant as to where perpetrators and victims of crimes are situated in terms of geography. There is no need for the perpetrator or the victim of a crime to move or to meet in person. Unlawful actions such as computer manipulations in one country can have direct, immediate effects in the computer systems of another country . . . ."[7]

However, the ongoing debate among experts about a precise definition for "computer crime" or a "computer-related crime" remains unresolved. In fact, there is no internationally recognized legal definition of these terms.[8] Instead, functional definitions identifying general offense

---

2. *Letter Of Submittal To President Bush From Secretary Of State Colin Powell*, United States Department of State, reprinted in Convention on Cybercrime, 108th Congress, 1st Session, Treaty Doc.108-11 (2003) at vi.

3. *See Id.* (The United States does not require implementing legislation once the treaty is ratified. According to the Secretary of State's Letter to the President, existing federal law is adequate to meet the requirements of the treaty).

4. Council of Europe *Convention On Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed May 25, 2005) [hereinafter Council of Europe, *Treaty*].

5. *Id.*

6. Council of Europe, *Glossary on the Treaties*, http://conventions.coe.int/Treaty/EN/Glossary.htm (accessed Jan. 17, 2005) [hereinafter Council of Europe, *Glossary*].

7. *See* Sieber, *supra* n. 1.

8. United Nations Crime and Justice Information Network, *International Review of Criminal Policy-United Nations Manual on the Prevention and Control of Computer Re-*

categories are the accepted norms.[9] Thus, the focus shifts away from reaching a global consensus over particular legal definitions, to identifying general categories of offense conduct to be enacted as penal legislation by each participating country.

The targeted unlawful conduct falls into several generally recognized categories. These categories, identified by the United Nations[10] as part of its study of cybercrime, include: fraud by computer manipulation,[11] computer forgery,[12] damage to or modifications of computer data or programs,[13] unauthorized access to computer systems and services,[14] and the unauthorized reproduction of legally protected computer pro-

---

lated Crime ¶ 7, http://www.uncjin.org/Documents/EighthCongress.html (accessed May 25, 2005) [hereinafter *U.N. Manual*].

9. *Id.*

10. *See id.* at ¶ 13 (Interestingly, the categories of computer crime identified in the *U.N. Manual* in 1995 appear to serve as the model for the same offense conduct targeted by the Council of Europe Convention on Cybercrime).

11. *See id.* at ¶¶ 13-14 (Intangible assets represented in data format, such as money on deposit and confidential consumer information, are the most common targets. Improved remote access to databases allows the criminal the opportunity to commit various types of fraud without ever physically entering the victim's premises. The *U.N. Manual* underscores the fact that computer fraud by input manipulation is the most common computer crime, as it is easily perpetrated and difficult to detect. Often referred to as "data diddling" it can be committed by anyone having access to normal data processing functions at the input stage. The *U.N. Manual* also identifies "program manipulation" through the use of a "Trojan Horse" covertly placed in a computer program to allow unauthorized functions and "output manipulation" targeting the output of computer information as other examples of unlawful manipulation).

12. *See id.* at ¶ 14 (Computer forgery can occur in at least two ways: 1) altering data in documents stored in a computerized form; and, 2) using the computer as a tool to commit forgery through the creation of false documents indistinguishable from the authentic original).

13. *See id.* at ¶ 15 (This is a form of "computer sabotage" perpetrated by either direct or covert unauthorized access to a computer system by the introduction of new programs known as viruses, worms or logic bombs. A "virus" is a program segment that has the ability to attach itself to legitimate programs, to alter or destroy data or other programs, and to spread itself to other computer programs. A "worm" is similarly constructed to infiltrate and harm data processing systems, but it differs from a virus in that it does not replicate itself. A "logic bomb" is normally installed by an insider based on a specialized knowledge of the system and programs the destruction or modification of data at a specific time in the future. All three can be used as an ancillary part of a larger extortionate scheme that can involve financial gain or terrorism).

14. *See id.* at ¶ 16 (The motives of the "cracker" or "hacker" may include sabotage or espionage. Access is often accomplished from a remote location along a telecommunication network. Access can be accomplished through several means including insufficiently secure operating system software, lax security, "cracker programs" used to bypass passwords or obtain access through the misuse of legitimate maintenance entry points in the system, or activating illicitly installed "trap doors on the system").

grams.[15] Recent additions to this list include child pornography[16] and the use of computers by members of organized crime and terrorist groups to commit computer-related crimes and/or a wide variety of crimes involving traditional offense conduct.[17]

C. Historical Development of International Cybercrime Law

United States Senator Ribikoff introduced the first piece of cybercrime legislation in the U.S. Congress in 1977.[18] While the legislation did not pass, it is credited for stimulating serious policy-making activity in the international community.[19] In 1983, the Organisation for Economic Co-operation and Development ("OECD")[20] conducted a study of existing cybercrime legislation in international states and considered the possibility of unifying these divers systems into a unitary international response.[21] On September 18, 1986, the OECD published *Computer-Re-*

15. *See Id.* (The problem has reached transnational dimensions through the trafficking of unauthorized reproductions over modern telecommunication networks at a substantial economic loss to the owners).

16. U.S. Department of Justice, Computer Crime and Intellectual Property Section, *International Aspects of Computer Crime* § C(6), http://www.cybercrime.gov/intl.html (accessed May 25, 2005) (In 1996, the Stockholm World Congress Against the Commercial Exploitation of Children examined the recommendations and proposed initiatives in many countries and regions. In September, 1999, the Austria International Child Pornography Conference drafted the Convention on the Rights of the Child, building on the Stockholm World Congress initiatives, to combat child pornography and exploitation on the Internet).

17. *See* International Narcotics Control Board, *Report of the International Narcotics Control Board for 2002* ¶ 121, http://www.incb.org/e/ind_ar.htm (accessed May 21, 2005) (2002) (reporting that narcotics traffickers are using computers and the Internet to conduct surveillance of law enforcement, to communicate, and to arrange the sale of illegal drugs); *see also* Bruce Swartz, Dep. Asst. Atty. Gen. Crim. Div., State. before Sen. Comm. on For. Rel., *Multilateral Law Enforcement Treaties* (June 17, 2004) (available at http://www.cybercrime.gov/swartzTestimony061704.htm) (stating that "criminals around the world are using computers to commit or assist a great variety of traditional crimes, including kidnapping, child pornography, child sexual exploitation identity theft, fraud, extortion and copyright piracy. Computer networks also provide terrorist organizations and organized crime groups the means with which to plan, coordinate and commit their crimes").

18. S.R. 1766, 95th Cong., vol. 123, part 17, p. 21,023.

19. Stein Schjolberg, *The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries*, http://www.mosstingrett.no/info/legal.html (last updated April 7, 2003) (Judge Schjolberg is the Chief Judge, Moss District Court, Norway).

20. *See generally* Organisation for Economic Development, *About OECD*, http://www.oecd.org (last visited Feb.29, 2005) (The OECD is an intergovernmental organization that promotes multilateral dialogue and international cooperation on political, social and economic issues. While it does not have legal authority, it has been a significant influence in policy making among member and non-member states and the United Nations. It is comprised of 29 countries, including the United States).

21. *See* Schjolberg, *supra* n. 19, at n.1 (A group of experts met in Paris on May 30, 1983 representing France, the United Kingdom, Belgium, Norway and Germany).

lated Crime: An Analysis of Legal Policy.[22] The report surveyed existing laws in several countries and recommended a minimum list of offense conduct requiring the enactment of penal legislation by participating international states.[23] The recommendations included fraud and forgery, the alteration of computer programs and data, the copyright and interception of the communications or other functions of a computer or telecommunication system, theft of trade secrets, and the unauthorized access to, or use of, computer systems.[24] The OECD envisioned this list as a "common denominator" of acts to be addressed through legislative enactment by each member country.[25]

Following the completion of the OECD report, the Council of Europe ("CoE")[26] initiated its own study to develop categories of proposed offense conduct and guidelines for enacting penal legislation, taking into account the immediate and critical need for enforcement without affronting due process and abrogating individual civil liberties.[27] The CoE issued Recommendation No. R(89)9 on September 13, 1989.[28] That Recommendation expanded the list of offense conduct proposed by the OECD to include matters involving privacy protection, victim identification, prevention, international search and seizure of data banks, and international cooperation in the investigation and prosecution of international crime.[29]

On September 11, 1995, the CoE adopted Recommendation No. R(95)13.[30] Significantly, this Recommendation goes beyond the identification of substantive offense categories and explores procedural issues

22. *U.N. Manual*, *supra* n. 8, at ¶ 9.

23. OECD Report, ICCP No. 10, *Computer Related Analysis of Legal Policy* (1986).

24. *Id.*

25. Schjolberg, *supra* note 19, at ¶ 118.

26. *See* U.S. Department of Justice, *Frequently Asked Questions and Answers about the Council of Europe Convention on Cybercrime*, http://www.usdoj.gov/criminal/cybercrime/new COEFAQs.html (The Council of Europe ("CoE") was established in 1949 to strengthen human rights, promote democracy and the rule of law in Europe. The organization currently consists of 46 member states, including all of the members of the European Union. The United States is not a member state; http://www.coe.int/DefaultEN.asp (last updated Mar. 24, 2005).

27. *U.N. Manual*, *supra* n. 8, at ¶¶ 144-45.

28. Council of Europe, *Computer Related Crime*, http://www.oas.org/juridico/english/89-9& Final%20Report.pdf (accessed May 22, 2005) (Recommendation No. R(89)9, adopted by the Committee of Ministers of the Council of Europe (1989) and Report by the European Committee on Crime Problems (1990)).

29. *U.N. Manual*, *supra* n. 8, at ¶¶ 119-22.

30. Council of Europe, Committee of Ministers, *Recommendation No. R(95)13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected With Information Technology*, www.coe.int/T/CM/home_en.asp, *select* Documents A-Z index/ Recommendations of the Committee of Ministers to member states/Results pg. 12/Rec(95)13/11 September 1995/PDF (Sept. 11, 1995) [hereinafter Council of Europe, *Recommendation (95)13*].

concerning the need to obtain information through conventional criminal procedure methods, including search and seizure, technical surveillance, obligations to cooperate with investigating authorities, electronic evidence, and the use of encryption. The Recommendation emphasizes a need to protect civil rights by minimizing intrusions into the privacy rights of individuals during an investigation, but offers no specific proposals.

The next important development in international law came in 1997, when the CoE appointed the Committee of Experts on Crime in Cyberspace ("PC-CY") to identify new crimes, jurisdictional rights and criminal liabilities related to Internet communications.[31] Canada, Japan, South Africa, and the United States were invited to meet with the PC-CY and participate in the negotiations.[32] In 2001, the PC-CY issued its Final Activity Report styled as the Draft Convention on Cyber-crime and Explanatory Memorandum Related Thereto.[33] The Report became the master blueprint for the first international treaty. Finally, after several years of intense effort, the Ministers of Foreign Affairs adopted the CoE Convention on November 8, 2001[34] and thereafter, it was opened for signature to member and non-member states.[35]

D. Practical Impediments to International Investigation and Enforcement

Historical impediments to the investigation and prosecution of cybercrime underscore the serious need for a global response to the problem. Cybercrime operates outside of any geographical constraints and light years ahead of national planning and implementation. Simply put,

---

31. Schjolberg, *supra* n. 19, § I.

32. The G-8 (United States, Japan, Germany, Britain, France, Italy, Canada and Russia) also convened in 1997 to discuss and recommend international cooperation in the enforcement of laws prohibiting computer crimes. United States Department of Justice, *Meeting of the Justice and Interior Ministers of the Eight, Communique*, http://www.cybercrime.gov/communique.htm (last updated Feb. 18, 1998).

33. European Committee on Crime Problems, *Final Activity Report*, http://www.privacy international.org/issues/cybercrime/coe/cybercrimefinal.html (accessed Dec. 13, 2004).

34. Council of Europe, *Treaty*, *supra* n. 4.

35. Other developments in the closely related fields of information security and information infrastructures overlap with CoE efforts. The Commission of European Communities (EC) issued the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach, COM (2001) 298 final (2001) (*available at* http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0298en01.pdf). The United States responded to the EC with formal comments on the proposal to protect information infrastructure on November 21, 2001. U.S. Dept. of Just., *Comments of the U.S. Government: Communication from the European Commission: "Network and Information Security: Proposal for a European Policy Approach"*, http://www.usdoj.gov/criminal/cybercrime/intl/netsec_USComm_Nov_final.pdf (Nov. 21, 2001).

the laws, criminal justice systems and levels of international cooperation have lagged behind escalating unlawful conduct despite the concerted efforts of the United Nations and the CoE.[36] The explanation for that lies, in part, in the magnitude and complexity of the problem when elevated from the national arena to the international venue,[37] particularly where many countries have yet to enact domestic legislation prohibiting the targeted offense conduct. Specific practical impediments to enforcement and prosecution[38] include:[39]

1. the absence of a global consensus on the types of conduct that constitute a cybercrime;
2. the absence of a global consensus on the legal definition of criminal conduct;
3. the lack of expertise on the part of police, prosecutors and courts in the field;
4. the inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to computerized data;
5. the lack of uniformity between the different national procedural laws concerning the investigation of cybercrimes;
6. the transnational character of many cybercrimes; and
7. the lack of extradition and mutual legal assistance treaties,[40] synchronized law enforcement mechanisms that would permit international cooperation in cybercrime investigations, and existing treaties that take into account the dynamics and special requirements of these investigations.

The United States, in its response to the "Cybercrime Communication Issued by the European Commission," emphasized the problem: "With the globalization of communications networks, public safety is increasingly dependent on effective law enforcement cooperation with foreign governments. That cooperation may not be possible, however, if a country does not have substantive laws in place to prosecute or extradite

36. *U.N. Manual*, *supra* n. 8, at ¶ 5.

37. According to INSEAD/World Economic Forum: The Network Readiness Index (2003-2004), by 2002 the number of Internet users worldwide increased to 600 million from only 300 million in 1999. A 2004 survey of 494 U.S. corporations found 20 percent had been subject to "attempts of computer sabotage and extortion among others through denial of service attacks." CBS News.com, *Cybercrime A Worldwide Headache*, http://www.cbsnews.com/stories/2004/09/16/tech/main643897.shtml (last updated Sept.16, 2004).

38. For an interesting discussion of the investigative and enforcement hurdles faced in the prosecution of two high profile cybercrime cases, the "Rome Labs" and "Invita" cases, *see* Susan Brenner and Joseph Schwerha, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. Marshall J. Computer & Info. L. 347 (2002).

39. *See U.N. Manual*, *supra* n. 8, at ¶ 7 (identifying these impediments to investigation and enforcement as a result of its in-depth study and analysis in 1995).

40. *See infra*, section III (discussing the availability and practical uses of MLATs).

a perpetrator."[41] Thus, in a very real sense, international cooperation is limited to the particular participants and/or treaty signatories who have affirmatively enacted domestic cybercrime legislation. Inadequate domestic legislation, combined with the failure of unanimous global cooperation, creates a gap in enforcement that provides "safe data havens"[42] for targeted conduct.[43] Meaningful international prosecutive efforts remain tenuous at best without a singular global consensus supported by the unanimous participation of all nations.[44]

II. THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

A. SUMMARY OF TREATY PROVISIONS

The CoE Convention consists of forty-eight articles divided among four chapters: (I) "Use of terms;" (II) "Measures to be taken at the national level;" (III) "International cooperation;" and, (IV) "Final provisions."[45]

Chapter II, Section 1, Articles two through thirteen address substantive law issues and include criminalization provisions and other related provisions in the area of computer or computer-related crime. Specifically, they define nine offenses grouped into four different categories. The offenses include: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography

41. U.S. Dept. of Just., *Comments of the United States Government on the European Commission Communication on Combating Computer Crime*, http://www.usdoj.gov, *search* Comments of the United States Government on the European Commission on Combating Computer Crime, *select* link No. 1 (accessed Dec. 17, 2004).

42. Dr. Prof. Ulrich Sieber, *Computer Crime and Criminal Information Law-New Trends in the International Risk and Information Society,* Hearings of the Permanent Subcommittee on Investigations, Committee on Government Affairs 19 http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html (accessed May 21, 2005).

43. Addressing the Southeastern European Cybersecurity Conference in Sophia, Bulgaria on Sept. 8, 2003, Lincoln Bloomfield said:

> Ensuring the safety and security of networked information systems – what we call cybersecurity – is very important to the United States . . . cybersecurity is very different from traditional national security issues. The government alone cannot ensure security – we must have partnerships within our societies and around the world.

Lincoln Bloomfield, *U.S. Says Cybersecurity is a Global Responsibility*, http://usinfo.org/wf-archive/2003/030909/epf213.htm (accessed May 25, 2005).

44. Yet, even with this recognition, the continuing slow response of the international community to act on the cybercrime problem seriously impedes meaningful international enforcement. At the CoE 2004 International Conference on Cybercrime, the forty-five nation participants agreed that governments are "dragging their heels" in implementing needed international reform through the final ratification of the treaty. CBS News, *supra* n. 37.

45. Council of Europe, *Treaty*, *supra* n. 4.

and offenses related to copyright.[46] Section 1 also addresses ancillary crimes and penalties.

Chapter II, Section 2, Articles fourteen through twenty-one address procedural law issues. Section 2 applies to a broader range of offenses than those defined in Section 1, including any offense committed *by means of* a computer system or evidence of which is in electronic form.[47] As a threshold matter, it provides for the common conditions and safeguards applicable to all procedural powers in the chapter.[48] Specifically, Article 15 requires the parties to provide for safeguards that are adequate for the protection of human rights and liberties. According to the CoE Explanatory Report, the substantive criteria and procedure authorizing an investigative power may vary according to the sensitivity of the data being sought in the investigation.[49]

The procedural powers include: expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, and interception of content data.[50] Traditional application of search and seizure methodology is provided for within a party's territory along with other procedural options, including real-time interception of content data.[51] The second chapter ends in Article twenty-two with an explanation of the jurisdictional provisions.[52]

Chapter III addresses traditional and cybercrime-related mutual assistance obligations as well as extradition rules.[53] Traditional mutual assistance is covered in two situations:

1. where no legal treaty, reciprocal legislation or other such agreement exists between the parties; and
2. where such pre-existing legal relationship exists between the parties.

In the former situation, the provisions of the CoE Convention apply. In the latter situation, however, pre-existing legal relationships apply "to provide further assistance" under the CoE Convention.[54] It bears em-

46. Council of Europe, Convention On Cybercrime, ETS 185, Explanatory Report, at 28, ¶ 18 (Nov. 2001) (*available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm) [hereinafter "CoE Explanatory Report"].

47. *See id.* at 29, ¶ 19.

48. The issue of providing adequate procedural safeguards to protect the civil rights and privacy of putative defendants was a major discussion point during treaty negotiations. Based on those discussions, the United States asserted "six reservations and four declarations" that qualify its participation as a party. *See* Powell, *supra* n. 2, at vi.

49. CoE Explanatory Report, *supra* n. 46, at 31, ¶ 31.

50. *See id.* at 29, ¶ 19.

51. *See id.* at 48, ¶ 143.

52. *See id.* at 29, ¶ 19.

53. The provisions addressing computer or computer related crime assistance provide the same range of procedural powers as defined in Chapter II.

54. CoE Explanatory Report, *supra* n. 46, at 29, ¶ 20.

phasizing that the three general principles of international cooperation in Chapter III do *not* supercede the provisions on international agreements on mutual legal assistance and extradition, reciprocal agreements between parties, or relevant provisions of domestic law applying to international cooperation.[55]

Finally, Chapter III provides transborder access to stored computer data not requiring mutual assistance because there is either consent or the information is otherwise publicly available.[56] There is also provision for the establishment of a "24/7 network" for ensuring speedy assistance between the parties.[57]

B. Application and Analysis of Significant Treaty Provisions

1. *Four Basic Definitions*

The drafters of the CoE Convention agreed that parties need not incorporate verbatim the particular definitions contained in the CoE Convention, provided that each nation's domestic laws cover these concepts in a manner "consistent with the principles of the convention and offer an equivalent framework for its implementation."[58] The United Nations identified uniformity in law and consensus over definitional terms as two of the impediments that had to be overcome in order to achieve meaningful cooperation and successful enforcement.[59] The CoE Convention accomplishes this goal using four principal definitions.

A "computer system" is defined,[60] *inter alia,* as a device consisting of hardware and software developed for automatic processing of digital data.[61] It may include input, output, and storage facilities. It may stand alone or be connected in a network. A "network" is an interconnection of two or more computer systems.[62] The Internet is a global network consisting of many interconnected networks, all using the same protocols. It

55. *See id.* at 69, ¶¶ 233-34. This basic principle of international cooperation is explicitly reinforced in Articles 24 (extradition), 25 (general principles applying to mutual assistance), 26 (spontaneous information), 27 (procedures pertaining to mutual legal assistance in the absence of applicable international agreements), 28 (confidentiality and limitations on use), 31 (mutual assistance regarding accessing of stored computer data), 33 (mutual assistance regarding the real-time collection of traffic data) and 34 (mutual assistance regarding the interception of content data).

56. *Id.*

57. *Id.*

58. *See id.* at 29, ¶ 22.

59. *See* Point I (d), *supra.*

60. Council of Europe, *Treaty*, *supra* n. 4, at art. 1(a).

61. "[P]rocessing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. CoE Explanatory Report, *supra* n. 46, at 29, ¶ 23.

62. Council of Europe, *Treaty*, *supra* n. 4, art. 1(a).

is essential that data is exchanged over the network.[63]

"Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.[64] Computer data that is automatically processed may be the target of one of the criminal offenses defined in the CoE Convention as well as subject to the application of one of the investigative measures defined by the CoE Convention.[65]

The term "service provider" encompasses a very broad category of persons and/or entities that provide users of its services with the ability to communicate by means of a computer system. Both public and private entities that provide the ability to communicate with one another are covered in the definition of "service provider."[66] The term also includes persons or entities that process or store computer data on behalf of such communication services or users of communication services.[67] However, a mere provider of content, such as a person who contracts with a web hosting company to host his Web site, is not included in the definition if the content provider does not also offer communication or related data processing services.[68]

Finally, "traffic data" means *any* computer data relating to a communication by means of a computer system, generated by a computer system that formed a part of the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.[69] Collecting traffic data in the investigation of a criminal offense committed in relation to a computer system is critical.[70] The traffic data is needed to trace the source of the communication as a starting point for the collection of further evidence, or as evidence of part of the offense.[71] Because of the short lifespan of traffic data, it is necessary to order its expeditious preservation and to provide rapid disclosure of the information to law enforcement to facilitate quick discovery of the communication's route before other evidence is deleted, or to

63. CoE Explanatory Report, *supra* n. 46 at 30, ¶ 24.

64. Council of Europe, *Treaty*, *supra* n. 4, art. 1(b).

65. CoE Explanatory Report, *supra* n. 46 at 30, ¶ 25.

66. *Id.* at 30, ¶ 26.

67. Council of Europe, *Treaty*, *supra* n. 4, art.1(c).

68. CoE Explanatory Report, *supra* n. 46, at 30, ¶ 27.

69. Council of Europe, *Treaty*, *supra* n. 4, art. 1(d).

70. CoE Explanatory Report, *supra* n. 46, at 30, ¶ 29. Specifically, the evidence that may be obtained from traffic data can include a telephone number, Internet Protocol address ("IP") or similar identification of a communication facility to which a service provider render service, the destination of the communication, and type of underlying service being provided (ie, file transfer, electronic mail, or instant messaging).

71. *Id.*

identify a suspect.[72] The collection of this data is legally regarded to be less intrusive because it doesn't reveal the content of communication that is viewed as more privacy sensitive.[73]

2. *Procedural Safeguards*

The CoE Convention addresses the complicated problem of guaranteeing civil rights protection to citizens living in different cultures and political systems.[74] Concluding that it was not possible to detail all of the conditions and safeguards necessary to circumscribe each power and procedure provided for in the CoE Convention, Article 15 was drafted to provide "the common standards or minimum safeguards to which Parties to the Convention must adhere."[75] These minimum safeguards reference certain applicable human rights instruments including: the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") and its additional Protocols No.1, 4, 6, 7 and 12;[76] the 1966 United Nations International Covenant on Civil and Political Rights; and "other international human rights instruments, and which shall incorporate the principle or mandates that a power or procedure implemented under the Convention shall be proportional to the nature and circumstances of the offense."[77] Thus, domestic law must limit the overbreadth of protection orders authorized, provide reasonableness requirements for searches and seizures, and minimize intrusion regarding interception measures taken with respect to the wide variety of offenses.[78]

The CoE Explanatory Report loosely identifies procedural safeguards "as [those] appropriate in view of the nature of the power or procedure, judicial or independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or duration thereof."[79] The bottom line is that "[n]ational legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular

72. *Id.*

73. *Id.*

74. *See id.* at 49, ¶ 145. This sensitivity to the differences in legal responses to criminality based upon different legal cultures and traditions was emphasized in the recommendations of the Association Internationale de Droit Penal ("AIDP") in the Draft Resolution of the AIDP Colloquium held at Wurrzburg on October 5-8, 1992. *U.N. Manual, supra* n. 8, at ¶¶ 270-3.

75. CoE Explanatory Report, *supra* n. 46, at 49, ¶ 145.

76. *See id.* at 49, ¶ 145, ETS Nos. 005, (4), 009, 046, 114, 117,& 117.

77. *See id.* at 50, ¶ 146.

78. *Id.*

79. *Id.*

conditions and safeguards."[80] Thus, other than aspirational language, couched in terms of legally non-binding human rights instruments, the treaty offers no specific minimal procedural guarantees of due process incident to treaty implementation.

3. *Methods of Collecting Evidence*

The four methods for securing evidence are found in Article 18 ("Production Order"), Article 19 ("Search and Seizure of Stored Computer Data"), Article 20 ("Real time collection of traffic data"), and Article 21 ("Interception of Collection Data").[81] While attempting to overcome the territorial sensitivity of each nation to transborder evidence collection, the CoE Convention carefully limits the scope of these powers by deferring to domestic legislative requirements as mandated by the CoE Convention, qualified by a strong admonition encouraging mutual cooperation between the parties as provided for in Article 23.[82] In short, transborder access to evidence will be whatever the participating nation decides is appropriate in conformity with the parameters of the treaty. Thus, uniformity of evidence gathering remains an unresolved issue among participating nations. However, the CoE Convention does require the enactment of certain minimal procedures by a party.

Under Article 18, a party must be able to order a person within its territory, including a third party custodian of data, such as an ISP, to produce data, including subscriber information, that is in the person's possession or control.[83] Production orders are viewed as a less intrusive measure than search and seizure for requiring a third party to produce information. A production order is similar to subpoena powers in the United States.[84] However, the Article does not impose an obligation on the service provider to compile and maintain such subscriber informa-

80. *Id.* This section is the subject of the due process analysis at point V, *infra.*

81. Notably, Articles 16 and 17 of the CoE Convention refer only to data preservation and not data retention. The CoE Explanatory Report observes that data preservation for most countries is an entirely new legal power or procedure in domestic law. Likewise, it is an important new investigative tool in addressing computer crime, especially committed through the Internet. Because of the volatility of computer evidence, it is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling or storage practices, intentional manipulation, or deletion designed to destroy evidence or routine deletion of data that is no longer required to be maintained. *See* CoE Explanatory Report, *supra* n. 46, at 51, ¶ 155.

82. Article 23 of the CoE Convention sets forth three general principles with respect to international co-operation. First, international co-operation is to be extended between the parties "to the widest extent possible." Second, co-operation is to be extended to all criminal offenses described in paragraph 14. Finally, co-operation is to be carried out through the provisions of the CoE Convention along with all pre-existing international mutual assistance and reciprocal agreements.

83. CoE Explanatory Report, *supra* n. 46, at 56-57, ¶ 177.

84. *See id.* at 55, ¶ 170.

tion in the ordinary course of their business. Instead, a service provider need only produce subscriber information that it does in fact keep, and is not obliged to guarantee the correctness of the information.[85] The application of the "proportionality principle," that is, the scope of the intrusion being limited to its purpose, is reemphasized in the CoE Explanatory Report.[86]

Significantly, the provision does not contain any minimal requirements concerning confidentiality of materials obtained through a production order. Except in the area of real-time interception of communications, there are no confidentiality provisions attendant to any of the evidence gathering tools provided for in the CoE Convention, nor are there any proposed minimal requirements.[87] Again, this is an area left to the domestic legislative discretion of the parties, leaving the issue of uniformity in the method of handling confidential information between nations unresolved. Standards of protection in one nation may differ materially from those in another nation and may impact dissemination of seized evidence. The legal contours of information dissemination remain unresolved by the treaty.

Article 19 is intended to enable investigating authorities, within their own territory, to search and seize a computer system, data stored in a computer system and data stored in storage mediums, such as diskettes.[88] However, two significant limitations curb the power to search and seize. First, and most important, Article 19 does not address "transborder search and seizure" whereby one country could search and seize data in the territory of other countries without first having to go through usual channels of mutual legal assistance.[89] Second, the measures contained in Article 19 are qualified by reference to the wording "in its territory," as a "reminder" that this provision – which qualifies all of the articles in this section – concerns only measures that are required to be taken at the national level.[90] Again, these measures operate between parties either through the tool of "international cooperation," or through channels of pre-existing mutual legal assistance arrangements.

Article 19 addresses the hugely problematic absence in many jurisdictions of laws permitting the seizure of intangible objects, such as stored computer data, which is generally secured by seizing the data medium on which it is stored. Such national domestic legislation is necessary, not only to protect the preservation of easily destroyed data, but also to provide available enforcement tools to assist other countries.

85. *See id.* at 57, ¶¶ 181 & 188.
86. *See id.* at 56, ¶ 174.
87. *See id.* at 56, ¶ 175.
88. *See id.* at 58, ¶¶ 187-89.
89. CoE Explanatory Report, *supra* n. 46, at 60, ¶ 195.
90. *See id.* at 59, ¶ 192.

Without these laws, a nation investigating a transborder crime is effectively prevented from seeking international cooperation in a country that fails to authorize lawful search and seizure within its territory.

Accordingly, paragraph 1 requires the parties to empower law enforcement authorities to access and search computer data, which is contained either within a computer system or part of it or on an independent data storage medium (such as a CD-ROM or diskette).[91] Paragraph 2 allows investigating authorities to extend their search or similar access to another computer system if they have grounds to believe that the data required is stored in the other system. However, this system must also be within the party's own territory.[92] Paragraph 3 authorizes the seizure[93] of computer data that has been accessed under the authority of paragraphs 1 and 2.[94] Paragraph 4 is a "coercive measure" that allows law enforcement authorities to compel systems administrators to assist during the search and seizure as may reasonably be required.[95]

While Article 19 applies to "stored computer data,"[96] Articles 20 and 21 provide for the real-time collection of traffic data and the real-time interception of content data associated with specified communications transmitted by a computer system.[97] Additionally, confidentiality considerations are addressed here.[98]

Specifically, Articles 20 and 21 require parties to establish measures to enable their competent authorities to collect data associated with specified communications in their territory at the time of the data's communication, meaning in "real time." However, Article 20 contains a provision allowing a party to make a "reservation" to the CoE Convention limiting the types of crimes to which Article 20 applies.[99]

Under Articles 20 and 21, subject to the party's actual technical capabilities,[100] a party is generally required to adopt measures enabling its

91. *See id.* at 59, ¶ 190.

92. *See id.* at 59, ¶ 193.

93. In the Convention, seizure means "to take away the physical medium upon which data or information is recorded, or to make and retain a copy of such data or information." Seize also means, in this context, the right to secure data. *See id.* at 59, ¶ 197.

94. *See id.* at 59, ¶ 196.

95. CoE Explanatory Report, *supra* n. 46, at 61, ¶ 200.

96. *Id.*

97. *See id.* at 61-62, ¶ 205.

98. *Id.*

99. Greater limitations may be employed with respect to the real-time collection of content data than traffic data. *See id.* at 62-63, ¶ 210. The United States has taken the position that a formal reservation is not needed because federal law already makes the mechanism generally available for criminal investigations and prosecutions. *See* Powell, *supra* n. 2, at xv.

100. CoE Explanatory Report, *supra* n. 46, at 65, ¶ 221. There is no obligation to impose a duty on service providers to obtain or deploy new equipment or engage in costly reconfiguration of their systems in order to assist law enforcement.

competent authorities to:

1. collect or record data themselves through application of technical means on the territory of that party; and
2. compel a service provider, to either collect or record data through the application of technical means or cooperate and assist competent authorities in the collection or recording of such data.[101]

The CoE Explanatory Report recognizes a critical distinction in the nature and extent of the possible intrusions into privacy between traffic data and content data.[102] With respect to the real-time interception of content data, laws often limit interception to investigations of serious offenses or serious offense categories, usually defined by certain maximum periods of incarceration.[103] Whereas, the interception of traffic data, viewed as less intrusive, is not so limited and in principle applies to every offense described by the CoE Convention.[104] In both cases, the conditions and procedural safeguards specified in Articles 14 and 15 apply to qualify the use of these interception provisions.[105]

4. *Crimes*

Section 1, Articles 2-13 of the CoE Convention establish a "common minimum standard of relevant offenses."[106] The Convention requires that all of the offenses must be committed "intentionally,"[107] although the exact meaning of the word will be left to national interpretation.[108] Laws should be drafted with as much clarity and specificity as possible in order to guarantee adequate forseeability regarding the type of conduct that will result in a criminal sanction.[109] As noted above, the United States maintains that its legislative structure adequately covers the offenses described in the CoE Convention and that no further implementing legislation will be required for ratification.[110]

---

101. *Id.*

102. *See id.* at 66, ¶ 227.

103. *See id.* at 63, ¶ 212.

104. *See id.* at 63, ¶ 214.

105. *See id.* at 63-64, ¶ 215.

106. CoE Explanatory Report, *supra* n. 46, at 31, ¶¶ 33-34. Notably the list is based on the guidelines developed earlier by the CoE in Recommendation No. R(89)9. *See U.N. Manual*, *supra* n. 8.

107. CoE Explanatory Report, *supra* n. 46, at 32, ¶ 39.

108. *Id.*

109. *See id.* at 33, ¶ 41.

110. The Computer Fraud and Abuse Act ("CFAA") was originally enacted in 1984 as the "Counterfeit Access Device and Computer Fraud and Abuse Act." Pub. L. No. 98-473, 2101(a), 98 Stat. 2190 (1984) (codified at 18 U.S.C. § 1030). In 1986 the statute was substantially revised and the title was changed to CFAA. The Act was revised and the scope of the law was expanded in 1988, Pub. L. No. 100-690, 102 Stat. 4404 (1988); 1989, Pub. L. No. 101-73, 103 Stat. 502 (1989); 1990, Pub. L. No. 101-647, 104 Stat. 4831, 4910, 4925 (1990); and 1994, Pub. L. No. 103-322, 108 Stat. 2097-99 (1994). In 1996, the CFAA was

The offenses described in Chapter II, Section I of the CoE Convention include:

Title 1, Articles 2-6, *Offenses against the confidentiality, integrity and availability of computer data and systems:* illegal access, illegal interception, data interference, system interference, misuse of devices;

Title 2, Articles 7-8, *Computer-related offenses*: computer-related forgery and computer-related fraud;

Title 3, Article 9, *Content-related offenses*: offenses related to child pornography;

Title 4, Article 10, *Offenses related to infringements and related rights:* offenses related to infringements of copyright and related rights; and

Title 5, Articles 11-13, *Ancillary Liability and sanctions*: attempt and aiding or abetting, corporate liability, and sanctions and measures.

The CoE Explanatory Report includes several caveats regarding the intent and application of these provisions. For example, criminal offenses defined under Articles 2-6 are intended to protect the confidentiality, integrity and availability of computer systems or data, and are not intended to criminalize legitimate and common activities inherent in the design of networks, or legitimate and common operating and commercial practices.[111] Each section is also subject to Article 8 of the ECHR, guaranteeing the right to privacy where applicable.[112] Again, these provi-

amended by the National Information Infrastructure Protection Act of 1996 ("NIIPA"), Pub. L. No. 104-294, tit. II, § 201, 110 Stat. 3488, 3491-96 (1996) (Economic Espionage Act of 1996, Title II). The CFAA proscribes 7 areas of offense conduct: (a)(1) knowing and willful theft of protected government information, (a)(2) intentional theft of protected information, (a)(3) intentional gaining of access to government information, (a)(4) fraud through a protected computer, (a)(5)(A) intentionally causing damage through a computer transmission, (a)(5)(B) recklessly causing damage through unauthorized access, (a)(5)(c)) causing damage through unauthorized access, (a)(6) fraudulent trafficking in passwords, and (a)(7) extortion. Portions of § 1030 were amended and expanded by provisions of the antiterrorism legislation entitled Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 814 (d)(1), 115 Stat. 272 (2001) (also referred to as the USA Patriot Act of 2001). Congress also enacted the Cybersecurity Enhancement Act of 2002, Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2156 (2002). These provisions are discussed in more detail in section VII of this article, *infra*. Additionally, other traditional federal criminal laws may be used to prosecute computer related crimes, such as charges of copyright infringement, 17 U.S.C. § 506 (1997); conspiracy, 18 U.S.C. § 371 (1994); wire fraud, 18 U.S.C. § 1343 (2002); illegal transportation of stolen property, 18 U.S.C. § 2314 (1994); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-21, 2701-10 (2002); illegal interception devices and equipment, 18 U.S.C. § 2512 (2002); and unlawful access to stored communications, 18 U.S.C. §§ 2701 et. seq. (2002).

111. CoE Explanatory Report, *supra* n. 46, at 33, ¶ 43.

112. *See id.* at 34, ¶ 51 (The "catch" is that signatories who are non-member countries are not bound by the ECHR which is itself closed for signature to non-member countries).

sions are the minimum offense categories that each party is obliged to implement through domestic legislation.

5. *Jurisdiction and Extradition*

Article 22 undertakes the monumental task of resolving the question of "who has jurisdiction" over the commission of computer-related offenses committed both within a territory and across sovereign borders. First, a series of criteria, grounded in international law principles,[113] is applied under which the parties are then obligated to establish jurisdiction over the criminal offenses enumerated in Articles 2-11.[114]

Article 22(1)(a) provides that each party "shall adopt" legislative measures to establish jurisdiction to prosecute the offenses listed in Articles 2-11 when committed "in its territory."[115] This provision is grounded upon the principle of territoriality[116] which is based on mutual respect of sovereign equality between States and is linked with the principle of nonintervention in the affairs and exclusive domain of other States.[117]

The "ubiquity doctrine" may also apply to determine the "place of commission of the offense."[118] Under this doctrine, a crime is deemed to occur "in its entirety" within a country's jurisdiction if one of the constituent elements of the offense, or the ultimate result, occurred within that country's borders. Jurisdiction applies to co-defendants and accomplices as well.[119]

Article 22(d) requires the parties to establish jurisdictional principles when the offense is committed by one of a party's nationals, if the offense is punishable under criminal law where it was committed, or if the offense is committed outside the territorial jurisdiction of any state. This provision is based on the principle of nationality, a different jurisdictional principle from the other subsections of the article.[120] It provides that nationals are required to abide by a party's domestic laws even when they are outside its territory. Under subsection (d), if a national commits an offense abroad, the party must have the ability to prosecute even if the conduct is also an offense under the law of the coun-

113. For an in depth discussion of international jurisdictional principles, *see* Julie O'Sullivan, *Federal White Collar Crime*, 735-50 (2d ed. 2003).

114. CoE Explanatory Report, *supra* n. 46, at 67, ¶ 232.

115. Council of Europe, *Treaty*, *supra* n. 4, at art. 22(1)(a).

116. CoE Explanatory Report, *supra* n. 46, at 67, ¶ 233. Note that subparagraph (b) and (c) are based upon a "variant of the principle of territoriality" where the crime is committed aboard a ship or aircraft registered under the laws of the State. *See id.* at 68, ¶ 235.

117. *U.N. Manual*, *supra* n. 8, at ¶ 249.

118. CoE Explanatory Report, *supra* n. 46, at 70-71, ¶ 250.

119. *Id.*

120. *See id.* at 67, ¶ 236.

try in which it was committed.[121]

However, the treaty does not resolve the central jurisdictional dilemma where more than one country has a "jurisdictional claim" to the case. The CoE Explanatory Report, interpreting Article 22(5) addresses this situation as follows:

> In the case of crimes committed by use of computer systems, there will be occasions when more than one Party has jurisdiction over some or all of the participants in the crime. . .the affected parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. . . . Finally, the obligation to consult is not absolute, but is to take place "where appropriate."[122]

Additionally, in those instances where a party refuses a request to extradite on the basis of the offender's nationality[123] and the offender's presence in the territory of a party, (where the request is made under Article 24), paragraph 3 of Article 22 requires the party to enact jurisdictional provisions enabling prosecution domestically.[124] Ostensibly, this provision should avoid the possibility of offenders seeking safe havens from prosecution by fleeing to another country. The bottom line is that a party must either extradite or prosecute.[125]

Article 24, entitled "Extradition," does not provide any mechanism to implement or expedite extradition when a request is made by a party. Instead, subparagraph 5 merely provides that "[e]xtradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the Party may refuse extradition."[126] However, the treaty does require each party to include as extraditable offenses those contained in Articles 2-11 of the CoE Convention.[127]

---

121. *Id.*

122. *See id.* at 68, ¶ 239.

123. *See* Powell, *supra* n. 2, at xvii. United States law permits extradition of nationals, accordingly no implementing legislation is required.

124. CoE Explanatory Report, *supra* n. 46, at 68, ¶ 237.

125. This article resembles the text of Articles 15(3) and 16 (10) of the UN Convention on Transnational Organized Crime, which is incorporated by reference into the Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children Supplementing the United Nations Convention Against Transnational Organized Crime (*available at* http://untreaty.un.org/English/notpubl/18-12E.doc and http://untreaty.un.org/English/TreatyEvent2005/List.asp) (accessed Feb.29, 2005). Those provisions require the views of the requesting nation to be taken into account and require the prosecuting nation to act diligently.

126. Council of Europe, *Treaty*, *supra* n. 4, at art. 24(5).

127. *See id.* at art. 24(2).

Finally, Article 35 requires each party to designate a point of contact available on a 24 hours, 7 days per week basis. This ensures co-operation in the investigation of crimes, collection of evidence or other such assistance.

III. MUTUAL LEGAL ASSISTANCE TREATIES ("MLATS") AND OTHER INTERNATIONAL COOPERATION AGREEMENTS

A. THE RELATIONSHIP TO THE COE CONVENTION

As explained above, the CoE Convention addresses both the situation where a traditional pre-existing legal relationship either in the form of a treaty, reciprocal legislation, memorandum of understanding ["MOU"][128] or other such agreement exists between the parties, and the situation where there is no such pre-existing relationship. Where there is a pre-existing relationship, that legal relationship applies "to provide further assistance" under the CoE Convention.[129] Traditional pre-existing legal relationships are not superceded by the CoE Convention.

Additionally, the three general principles of international cooperation in Chapter III of the CoE Convention do not supercede the provisions of international agreements on mutual legal assistance and extradition, reciprocal agreements between parties, or relevant provisions of domestic law applying to international cooperation.[130]

The U.S. Department of State describes Mutual Legal Assistance Treaties or "MLATs" as a means of "impro[ving] the effectiveness of judicial assistance and to regularize and facilitate procedures" with foreign nations.[131] The treaties typically include agreed upon procedures for summoning witnesses, compelling the production of documents and

128. For example, the Securities and Exchange Commission has "case-by-case" informal MOUs to facilitate production with Switzerland, Japan, Canada, Brazil, Netherlands, France, Mexico, Norway, Argentina, Spain, Chile, Italy, Australia, the United Kingdom, Sweden, South Africa, Germany, Luxembourg and Hungary, as well as Joint Statements of Cooperation with the European Union (EU). *See* U.S. Dept. of St., *Mutual Legal Assistance in Criminal Matters Treaties (MLATs) and Other Agreements*, http://travel.state.gov/law/mlat.html (accessed May 21, 2005) [hereinafter *MLAT*].

129. CoE Explanatory Report, *supra* n. 46, at 29, ¶ 20.

130. *See id.* at 69, ¶¶ 233-34. This basic principle of international cooperation is explicitly reinforced in Articles 24 (extradition), 25 (general principles applying to mutual assistance), 26 (spontaneous information), 27 (procedures pertaining to mutual legal assistance in the absence of applicable international agreements), 28 (confidentiality and limitations on use), 31(mutual assistance regarding accessing of stored computer data), 33 (mutual assistance regarding the real-time collection of traffic data) and 34 (mutual assistance regarding the interception of content data).

131. *See MLAT*, *supra* n. 128.

other evidence, issuing search warrants and serving process.[132]

B. Remedial Imbalances

Notably, these remedies are available only to prosecutors. The Office of International Affairs ("OIA"), Criminal Division, United States Department of Justice, is responsible for administering procedures under the MLATs and assisting domestic prosecutions by the respective United States Attorneys Offices. Thus, to the extent that the MLATs "supercede" the CoE Convention,[133] defense attorneys are effectively excluded from participating in that part of the process of international enforcement activity.

The operative provisions of MLATs often have the effect, whether intended or not, of limiting international enforcement efforts. Many such agreements require "dual criminality," that the crime for which information is being sought by a requesting country must also be offense conduct in the nation possessing the needed information. Where the nation has not criminalized targeted conduct, the investigation cannot proceed. For example in 1992, the United States requested information from Switzerland in connection with its investigation of a Swiss-based hacker who attacked the San Diego Supercomputer Center. Switzerland had not criminalized hacking and was, therefore, unable to assist in the investigation.[134]

In any event, the CoE Convention does not refer to the role or participation of defense counsel in the process at all. Defense attorneys must obtain evidence in criminal cases from foreign or "host" countries, pursuant to the laws of the host nation, through a procedure known as "Letters Rogatory."[135] To the extent that the United States maintains agreements with the various host nations, the State Department publishes "country specific information" to enable a litigant to avail himself of ex-

132. *Id.* The United States has bilateral Mutual Legal Assistance Treaties with Anguilla, Antigua/Barbuda, Argentina, Austria, Bahamas, Barbados, Belgium, Brazil, British Virgin Islands, Canada, Cayman Islands, Cyprus, Czech Republic, Dominica, Egypt, Estonia, Greece, Grenada, Hong Kong, Hungary, Israel, Italy, Jamaica, South Korea, Latvia, Lithuania, Luxembourg, Mexico, Montserrat, Morocco, Netherlands, Panama, Philippines, Poland, Romania, St. Kitts-Nevis, St. Lucia, St. Vincent, Spain, Switzerland, Thailand, Trinidad, Turkey, Turks and Caicos Islands, Ukraine, United Kingdom and Uruguay.

133. CoE Explanatory Report, *supra* n. 46, at 29, ¶ 20 & 67, ¶¶ 233-34. The three general principles of international co-operation in Chapter III of the CoE Convention do *not* supercede the provisions on international agreements on mutual legal assistance and extradition, reciprocal agreements between parties, or relevant provisions of domestic law applying to international co-operation.

134. ABA Privacy and Computer Crime Committee, *International Cybercrime Project*, http://www.abanet.org/scitech/computercrime/cybercrimeproject.html (accessed May 21, 2005).

135. *See MLAT*, *supra* n. 128.

traterritorial discovery.[136] There are strict requirements for the form of the request submission,[137] and the requesting party must pay all expenses associated with the process.[138] It is unclear if and to what extent the CoE Convention affects the rules with respect to treaties governing Letters Rogatory.

Letters Rogatory usually requires preauthorization by a judicial or administrative body and also requires transmission by a designated "central authority."[139] The process may be "cumbersome and time consuming"[140] and the treaties generally do not provide time lines for production of the requested information.[141] The Letters Rogatory was codified under 28 U.S.C. § 1781 (2000).[142] Under this section, the State Department is vested with the power in both civil and criminal cases to transmit the request for evidence to "a foreign or international tribunal, officer or agency to whom it is addressed."[143] The request may be used for providing notice, serving summons, locating individuals, witness examination, document inspection and other evidence production. The foreign tribunal can only honor requests that fall within its procedures and jurisdiction. Again, if criminal activity does not fall within the domestic legislation of the foreign country, then the Letters Rogatory request cannot be honored.

There are some limited international tools available to side step time-consuming and complicated procedures for obtaining information where the charge involves drug trafficking. For example, Article 7 of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and

---

136. *See* United States Department of State, International Judicial Assistance, *Notarial Services and Authentication of Documents*, http://travel.state.gov/law/judicial_assistance.html (accessed May 21, 2005).

137. Organization of American States, *Additional Protocol to the Inter American Convention on Letters Rogatory*, art. 3 http://www.oas.org/juridico/english/treaties/b-46.html (accessed May 21,2005).

138. *Id.* at art. 5.

139. *E.g., id.* at art. 1 & 2.

140. *See MLAT*, *supra* n. 128.

141. *See* Organization of American States, *supra* n. 137.

142. *See* 28 U.S.C. § 1781 (2005). The section provides in pertinent part:

> (a) The Department of State has power, directly, or through suitable channels–
>
> . . .
>
> (2) to receive a letter rogatory issued, or request made, by a tribunal in the United States, to transmit it to the foreign or international tribunal, officer, or agency to whom it is addressed, and to receive and return it after execution. . .
>
> (b) This section does not preclude–
>
> . . .
>
> (2) the transmittal of a letter rogatory or request directly from a tribunal in the United States to the foreign or international tribunal, officer, or agency to whom it is addressed and its return in the same manner.

Id.

143. *Id.* at § 1781(a)(2).

Psychotropic Substances,[144] provides a procedure to obtain evidence from other participating nations without Letters Rogatory.[145]

Additionally, those international organizations, such as the Organization of American States ("OAS"), which do provide protocols for Letters Rogatory, have taken steps to encourage participating OAS nations to incorporate the CoE Convention into existing protocols. Specifically, the Ministers of Justice of the OAS in April 2004 called upon OAS members to accede to the CoE Convention and incorporate its principles into their national legislation.[146] In short, the defense is relegated in a very real sense to relying upon the limited discovery obligations of the prosecutor.[147] The limitations are obvious. The defendant's desire for specific information in the possession of the host country may materially differ from the information sought by the prosecution.

IV. PRINCIPLES OF HARMONIZATION: AN ONGOING DILEMMA

A. THE CONVENTION AS A HARMONIZATION MODEL

There are differing models for harmonization of penal enforcement in the European Community. The classical instrument of international cooperation is the convention.[148] The convention model has its genesis in the Treaty on European Union, TEU.[149] Specifically, the so-called

144. International Narcotics Control Board, United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 http://www.incb.org/e/conv/1988/index.htm (accessed Nov. 16, 2004).

145. *See MLAT*, *supra* n. 128. This convention entered into force on November 11, 1990.

146. *See* Guy De Vel, Dir. Gen. of the Legal Affairs of the Council of Europe, Remarks, *The Challenge of Cybercrime* (Council of Europe, Conference on the Challenge of Cybercrime Sept. 15-17, 2004) (*available at* http://www.coe.int/T/E/Com/Files/Events/2004-09-cybercrime/disc_deVel.asp) (accessed May 21, 2005) (also recognizing the decision of APEC leaders in 2002 to recommend to their members to adopt laws against cybercrime in conformity with the CoE Convention).

147. Fed. R. Crim. P. 16(a)(1)(E)(i)-(iii).

148. *See See* Mareike Braeunlich, *European Criminal Law* 31 (unpublished Master Thesis, Lund University Spring, 2002) (on file with author) (available at www.jur.lu.se/. . ./english/essay/Masterth.nsf/0/94E4D9B5A0990798C1256BC900560788/$File/xsmall.pdf?, at 13. (Another model is the "directive." A directive leaves the choice of forms and method for achieving the desired results to the Member states. (Treaty of the European Community, ECT, Art. 249). Penal sanctions are never included in a directive. For example, a convention was used as the model to criminalize fraud against EC financial interests, whereas, in the case of money laundering, the EC utilized a directive. A third method, the "intergovernmental method" provides for a structure of cooperation and common decision making between nation states resting primarily on a network of multi-lateral agreements that allow nation states to retain sovereignty).

149. The TEU, also referred to as the Maastricht Treaty, entered into force in 1993. Cooperation on justice and home affairs was institutionalized under Title VI of the treaty, Article K. *See* Europa, *Title VI: Provisions of Cooperation in the Fields of Justice and Home Affairs, Article K*, http://europa.eu.int/en/record/mt/title6.html (accessed May 21, 2005).

"third pillar area" of the TEU, Title V, Articles 29-45, provides for police and judicial cooperation in criminal matters.[150] Simply, a convention is a treaty signed by participating nations which is then adopted nationally in accordance with the constitutional requirements of each Member State.[151] Conventions take the form of traditional international law agreements, enforceable as international treaties but not through any central organizational mechanism.[152] Procedural criminal rule making is addressed in the TEU, Title VI, Article K.2 as follows: judicial cooperation in criminal matters, rules combating fraud on an international scale and police cooperation for purposes of combating serious forms of international crime "shall be dealt with in compliance with the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 [ECHR] . . . ." The impact of the ECHR on penal matters in Europe is recognized as the most elementary guarantee of procedural due process rights in the criminal law context.[153] The ECHR is typically incorporated into crime control instruments that take the form of treaties to which the member state may agree.[154] Section II, Article 15 of the CoE Convention incorporates the ECHR as the principal safeguard of procedural due process.[155]

---

150. The European Convention, Brussels, 31 May 2002 (03.06), CONV. 69/02, *Subject:Justice and Home Affairs-Progress Report and General Problems*, at 4.

151. *Id.* The sole difference between conventions and agreements, both under the rubric of a treaty, is the form in which a State may express its consent to be bound. Agreements may be signed with or without reservations as to ratification, acceptance or approvals. Conventions require ratification. Council of Europe, *Glossary*, *supra* n. 6.

152. *See,* Braeunlich, *supra* n. 148, at 10.

153. *See id.* at 9.

154. The continuous development of fundamental rights in the European Union Treaties has been an evolving process, recently culminating with the Treaty Establishing A Constitution For Europe. Beginning in 1986, the preamble to the Single European Act, 2/28/1986, provides for the development of international law on the basis of "the fundamental rights recognized in the constitutions and laws of the member states." Article 6.2 of the Maastricht Treaty, TEU, 2/7/1992, requires the Union to "respect fundamental rights, as guaranteed by the [ECHR]. . ." The Nice Treaty, 2/26/2001,(Official Journal C80 of 10 March 2001) may determine if there is a serious breach of Article 6 by a member state. The Treaty on the European Union, the Amsterdam Treaty, 10/2/1997, confirms "their attachment to fundamental social rights. . .and respect for human rights and fundamental freedoms and the rule of law . . . ." The Official Journal of the European Union recently released the Treaty Establishing A Constitution for Europe, intended to replace all existing treaties and agreements relative to the formation of the EU, including The Treaty Establishing the European Community (Official Journal C325 of 24 December 2002) and the Treaty on the European Union, (Official Journal C325 of 24 December 2002).Constitution, Article IV-437. Further, Title VI, Article II, for the first time, formulates specific constitutional due process rights in the field of criminal prosecution that shall be binding on all member states. Official Journal, C310 (Dec. 16, 2004) (*available at* http://europa.eu.int/eur-lex/lex/JOHtml).

155. *See supra* Discussion, § II, B (2).

Conventions, as a harmonization model for international criminal enforcement, are criticized for several reasons. Several of these criticisms also underscore the flawed approach to procedural harmonization in the CoE Convention.

First, conventions may not come into force within a reasonable period of time for lack of ratification.[156] It is usual for countries to sign but never follow up with ratification. The United States is a case in point.[157] The United States signed the Criminal Law Convention on Corruption on October 10, 2000, but has never ratified it. The Convention on Cybercrime was signed on December 11, 2001, but is not ratified. While the United States ratified the Convention on Mutual Administrative Assistance in Tax Matters on February 13, 1991, an insufficient number of member states ratified until four years later when the convention finally entered into force on January 4, 1995.[158] The European Convention on Extradition, CETS No. 024, was open for signature and accession by non-member states on December 13, 1957. The United States has never signed that convention.[159]

Second, conventions do not include any follow-up measures to ensure that ratification is followed by compliance. Member States may express "reservations" that allow them to be exempted from certain operative provisions of the convention. In fact, the United States signed the CoE Convention subject to several reservations.[160]

Another problem is the failure of uniform interpretation based on linguistic and cultural differences. These differences translate into a serious concern about the prosecution of foreign nationals.[161] Specifically, there is no guarantee that an accused will understand the language or culture in the prosecution venue. Nor is there any guarantee that an

156. Ratification is an act by which the State expresses its definitive consent to be bound by the treaty. Then the state must respect the provisions of the treaty and implement it. Council of Europe, *Glossary*, *supra* n. 6.

157. The United States, a non-member country of the Council of Europe was given "observer Status" on December 7, 1995. Observer status was enacted on May 14, 1993 by the Committee of Ministers and extended to any nation wishing to cooperate with the CoE and "willing to accept the principles of democracy, the rule of law and respect for human rights and fundamental freedoms of all persons within its jurisdiction." Res(95)37 on observer status for the United States of America with the Council of Europe (*available at* http://www.coe.int?t?E?com/About_Coe/Member_states/eUSA.asp) (accessed Jan. 17, 2005).

158. Statistics *available at* http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?PO=U, (accessed Jan. 17, 2005).

159. *Id.*

160. *See e.g.*, Powell, *supra* n. 2, at vii, x, xi, xii, xvi, xxi. "Federal Clause" reservations allow for variations between domestic law and Convention obligations permitting parties to "modify or derogate from specified Convention obligations."

161. International Law Association, London Conference, *The Final Report On The Exercise of Universal Jurisdiction in Respect of Gross Human Rights Offenses*, www.ila-hq.org/pdf/Human%20Rights%20Law/HumanRig.pdf (accessed May 25, 2005).

accused will be afforded the right to counsel or an interpreter, or even have the right to call or examine witnesses. The CoE Convention resolves none of the foregoing criticisms.

B. The Fallback of "Cultural Diversity"

The recognition of cultural differences among nations appears to be the greatest stumbling block to achieving harmonization in the area of procedural due process. Each nation has its own notion about what constitutes criminality, the appropriateness of punishment, proportionality of punishments, and the rights accorded to the accused. Often, the rubric of cultural differences, ostensibly used to oppose harmonization, is merely a cover for opposition based upon "irrational historical reminiscences" and political opposition.[162] In an effort to reach a baseline consensus among nations, the CoE Convention employs "flexible harmonization,"[163] a model of uniform rule making confined to establishing parameters for acceptable substantive rules, leaving the formulation of procedural due process rules to the cultural peculiarities of each nation.[164] This paradigm of flexible harmonization facilitates diplomatic appeasement to national sovereignty enabling the CoE to accomplish law enforcement goals. However, the legitimacy of reaching law enforcement goals at the expense of fundamental fairness to the accused is contrary to the long term interests of international governance.

Added to the need for political appeasement is the perplexing phenomenon that often follows accommodation. Nations frequently enter into treaties and then fail to act in conformity with treaty obligations. The reasons that nations enter into treaties, only to later ignore them, remain sketchy.[165] Typically, successful implementation rests on the degree of one nation's willingness to voluntarily diminish its sovereignty over criminal enforcement for the common good of the international community. Not unexpectedly, compliance can be predicted where it is in the material interest of the participating nation to do so.

It bears repeating that the issue here is not whether international legal conventions work but rather, whether the CoE Convention, despite the aforementioned legal, cultural and political complications, provides a reliable guarantee of procedural due process of law. The watered down compromise of flexible harmonization offers little to motivate nations to voluntarily relinquish sovereignty in favor of international regulation.

---

162. *See* Sieber, *supra* n. 1, at 11, 16.

163. *Id.*

164. *Id.*

165. For an interesting discussion on this topic, *See,* Oona A. Hathaway, *The Promise and Limits of the International Law of Torture*, in *Foundations of International Law and Politics*, 228-238 (Oona A. Hathaway and Harold Hongju Koh eds., Foundation Press 2005).

Instead, the absence of procedural harmonization undermines predictable implementation and is contrary to a party's national interest to protect its own citizens abroad.

V. THE COE CONVENTION DOES NOT ADEQUATELY SAFEGUARD PROCEDURAL DUE PROCESS RIGHTS

A. WHAT IS PROCEDURAL DUE PROCESS?

The Fifth Amendment to the United States Constitution provides that "No person shall be . . . deprived of life, liberty or property, without due process of law . . . ." The Fourteenth Amendment contains the same language as expressly applied to the States.[166] The United States Supreme Court recognizes both procedural and substantive due process components.[167]

Substantive due process provides the contours of what laws may proscribe or prohibit. Procedural due process focuses on the concept of fundamental fairness and the rules that provide fair procedures to ensure that an accused is not unfairly or unjustly convicted. Explicit procedural guarantees of due process are found in the Constitution and the Bill of Rights.[168] However, as discussed below, domestic juridical limitation on the application of procedural due process to aliens necessarily diminishes the United States' commitment to the general admonitions in the treaty.

B. WHAT IS THE MODEL FOR PROCEDURAL DUE PROCESS IN THE COE CONVENTION?

Section II, Article 15, entitled "Conditions and Safeguards" of the CoE Convention, leaves the responsibility for enactment of procedural due process rules to each party as "provided for under its domestic law. . . which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms [ECHR], the 1966 United

166. The due process clause finds its roots in a similar clause of the Magna Carta in which the King of England agreed in 1215 A.D. that "[n]o free man shall be taken, or imprisoned, or be disseised of his Freehold, or liberties, or free Customs, or be outlawed, or exiled, or any otherwise destroyed; nor will we pass upon him, nor condemn him, but by lawful Judgment of his peers, or by the Law of the Land." (*available at* http://www.bl.uk/collections/treasures/magnatranslation.html).

167. *Schriro v. Summerlin*, 124 S. Ct. 2519, 2523 (2004).

168. *See e.g.*, U.S. Const., art. III: right to a jury trial; amend. V: right to a grand jury indictment, prohibitions against double jeopardy and self-incrimination, right to due process of law; amend. VI: rights to a speedy and public trial, jury of one's peers, to confront and cross-examine witnesses, right to counsel; and amend. XIV right to due process as applied to the states.

Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality."[169]

Specifically, these rules do not require judicial supervision, but may include "other independent supervision."[170] The parties are also admonished to "consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties."[171] The tone is limited to aspirational guidance.

The Explanatory Report underscores the point that there are no unified or minimal standards for procedural due process: "As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure."[172] Significantly, the Explanatory Report acknowledges that the ECHR is only applicable "in respect of the European States that are Parties to them."[173] The United States is not a party to the ECHR and thus, is not bound by its minimal standards. Indeed, any CoE Convention signatory, not a member state of the Council of Europe, is not a party to the ECHR because the ECHR is not open for signature to non-member states of the Council of Europe.[174]

The safeguard of "proportionality" is also left to the discretion of the parties. "States will apply related principles of their law such as limitations on overbreadth of production orders and reasonableness for searches and seizures."[175] In very sketchy fashion, the Explanatory Report homogenizes aspirational recommendations for protections against self-incrimination and possible invasions of privacy rights through intrusive means of search and seizure:

> National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards. As stated in Paragraph 215, Parties should clearly apply conditions and safeguards such as these with respect to interception [of data communications], given its intrusiveness. At the same time, for example, such safeguards need not apply equally to preservation [of seized data communication]. Other safeguards that should be addressed under domestic law include the right against self incrimination, and legal privileges and specificity

169. Council of Europe, *Treaty*, *supra* n. 4, at art.15, ¶ 1.

170. *Id.* at ¶ 2.

171. *Id.*

172. CoE Explanatory Report, *supra* n. 46, at ¶ 145.

173. *Id.*

174. Council of Europe, http://www.conventions.coe.int/Treaty/Commun/ListeTraites.asp (accessed Jan. 17, 2005) (listing treaties open to the member states of the Council of Europe).

175. CoE Explanatory Report, *supra* n. 46, at ¶ 146.

> of individuals or places which are the object of the application of the measure.[176]

Using a legally non-binding treaty as the primary source of procedural due process, in lieu of specific minimal guidelines to protect an accused, results in a structural weakness in the treaty. More than mere advice is required where penal sanctions stand to deprive an accused of liberty.

C. The Dynamic of Self-Enforcement

Whether a particular party has enacted sufficient due process protections, or even extends existing domestic due process protections to aliens prosecuted within its borders, must necessarily remain untested until cases are actually prosecuted. The dynamic of self-enforcement of the treaty objectives remains within the domain of each respective national legislature. What are the prospects for extending procedural due process to aliens prosecuted for cybercrime in the United States?

Central to the model of procedural due process in the CoE Convention is the mandate that each nation recognize "rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms [ECHR], the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality."[177] The Supreme Court of the United States, in rejecting an alien's claim for damages under the Aliens Tort statute arising out of an alleged arbitrary arrest and unlawful seizure,[178] concluded that neither the ECHR nor the other international treaties imposed any legal obligation on the United States. Therefore, federal courts had no power to enforce individual rights violations under these treaties, even where the United States was a signatory.

> Petitioner says that his abduction by [DEA operatives] was an 'arbitrary arrest' within the meaning of the Universal Declaration of Human Rights (Declaration), G.A. Res. 217A(III), U.N. Doc. A/810 (1948). And

176. *See id.* at ¶ 147.

177. Council of Europe, *Treaty*, *supra* n. 4, art.15, ¶ 1.

178. The petitioner was acquitted on charges arising out of the torture and murder of a DEA agent by Mexican nationals. In a related lower court decision, the Ninth Circuit found that DEA agents had no authority under federal law to execute an extra-territorial arrest of the petitioner indicted in a federal court in Los Angeles. *Alvarez-Machain v. U.S.*, 331 F.3d 604, 609 (9th Cir. 2003). In fact, the agents unlawfully kidnapped petitioner to bring him to the United States to stand trial. *Id.* Petitioner moved to dismiss his indictment based upon "outrageous government conduct" and a violation of the extradition treaty with Mexico. *Id.* The district court agreed, the Ninth Circuit affirmed and the Supreme Court reversed holding that the forcible seizure did not divest the federal court of jurisdiction. *United States v. Alavrez*, 504 U.S. 655 (1992).

> he traces the rule against arbitrary arrest not only to the Declaration, but also to article nine of the International Covenant on Civil and Political Rights (Covenant), Dec. 19, 1996, 999 U.N.T.S. 171, to which the United States is a party, and to various other conventions to which it is not. But the Declaration does not of its own force impose obligations as a matter of international law . . . . And, although the Covenant does not bind the United States as a matter of international law, the United States ratified the Covenant on the express understanding that it was not self-executing and so did not itself create obligations enforceable in the federal courts.[179]

Thus, the ECHR, along with the other human rights treaties, incorporated into Section II, Art. 15, creates no enforceable procedural due process rights in United States federal courts.

Moreover, the decision to extend the protections of the Bill of Rights to aliens is not an automatic one or implicit in the concept of ordered liberty, and so the courts have held. Specifically, the Supreme Court declined to extend the protection of the Fourth Amendment to an alien extradited to the United States for trial on criminal charges. The Court reasoned that:

> [A]liens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country. . .but this sort of presence-lawful but involuntary [extradition]- is not the sort to indicate any substantial connection with our country.[180]

Further rejecting the alien's equal protection argument, to wit: that aliens should be afforded the same constitutional rights afforded U.S. citizens in criminal cases, the Court concluded: "They are constitutional decisions of this Court expressly according different protections to aliens than to citizens, based on our conclusion that the particular provisions in question were not intended to extend to aliens in the same degree as to citizens." Justice Kennedy, in his concurring opinion, concluded that:

> The distinction between citizens and aliens follows from the undoubted proposition that the Constitution does not create, nor do general principles of law create, any judicial relation between our country and some undefined, limitless class of non-citizens who are beyond our territory.[181]

These decisions leave little doubt that the Bill of Rights does not operate extraterritorially in relation to searches and seizures authorized under the CoE Convention or in relation to constitutional infringements of the right to privacy in seizing data communications used to prosecute aliens for cybercrime. Instead, the extension of existing procedural due

179. *Sosa v. Alavrez-Machain, et.al.*, 124 S.Ct. 2739, 2767 (2004).

180. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990).

181. *Id.* at 275.

process guarantees to aliens turns on the two-prong voluntariness and substantial connection analysis. That ad hoc determination leaves little room for predictability in the application of the treaty in the United States.

Accordingly, the procedural due process rhetoric of the CoE Convention has no demonstrable influence on American jurisprudence. As noted previously, the Secretary of State indicated that no implementing legislation was required to ratify the treaty, necessarily excluding any additional legislation to effectuate the rights of aliens in the United States consistent with Section II, Art. 15 of the treaty. The United States should expect no more protection with respect to its citizens similarly situated in other participating nations. The cycle of mistrust is inevitably self-perpetuating under these circumstances.

D. Rejecting the Messy Compromise in Favor of a Structural Fix

The CoE Convention abdicates all responsibility for providing procedural due process of law to an accused charged with crimes arising under offense categories. The sole justification provided is that it is "impossible" to draft even minimal obligatory guidelines for due process based on "cultural differences." Is this reason justified?

The logic simply does not follow that culturally diverse parties can agree on offense conduct but not upon internationally recognized standards that preserve basic human freedoms. The treaty's use of flexible harmonization strikes an ostensibly workable compromise among sovereign nations, particularly where the imposition of procedural due process standards may be superior to those offered by a party's own domestic legislation.

Indeed, this glaring legal ambiguity in the CoE Convention underscores a core weakness in international law, namely, the deference to territoriality principles of regulation and enforcement based on national sovereignty. The decentralized nature of international law, relegating enforcement to domestic legislation, results from the decentralized structure of international society and the inability to enforce violations of binding legal rules.[182] Left to the questionable dynamic of self-enforcement by participating nations, the CoE Convention surrenders any attempt to navigate the problem.

However, the counter-argument is persuasive. It may be unreasonable to expect the CoE Convention, a discreet body of international crimi-

182. For a more in-depth discussion of the problems with decentralization in international law, *see* H.J. Morgenthal, *Politics Among Nations*, in *Foundations of International Law and Politics*, 31-42, (Oona A. Hathaway and Harold Hongju Koh eds., Foundation Press 2005).

nal law, to resolve the bigger issue of decentralization that characterizes the entire body of international law.

Yet, the CoE Convention recognizes that criminal enforcement typically requires serious privacy intrusions[183] to facilitate individual prosecution. The equation presented by the CoE Convention, allowing for enforcement without ascertainable measures of procedural due process, results in an imbalance disfavoring individual liberties implicated by the very nature of a criminal prosecution. Thus, the need to eradicate cybercrime cannot outweigh the equally important need to achieve a consensus on minimal standards for securing fundamental procedural due process guarantees.

Additionally, mutual cooperation, a centerpiece of the treaty,[184] will be less forthcoming where one participant cannot rely on another to guarantee fair treatment of its own citizens subject to prosecution. This may be a reason that the CoE Convention does not supercede, but merely supplements pre-existing MLATs. The dynamic of national self-enforcement may be easier to predict "one on one" than on a broader international scale where countries frequently fail to honor treaty obligations, or fail to ratify them at all.

One solution may be the addition of a Protocol[185] to the treaty, modeled after the proposed Treaty Establishing a Constitution for Europe,[186] [hereinafter "Constitution"], which does include specific minimal procedural due process formulations, extended to citizens of all participating nations. The Constitution is expected to come into force in 2006, replacing all international agreements that provide for European unification.[187] Specifically, the Constitution provides for the right to an effective remedy and to a fair trial,[188] presumption of innocence and right of defense,[189] principles of legality and proportionality of criminal offenses

183. Global Internet Liberty Campaign, *Member Letter on Council of Europe Convention on Cybercrime*, http://www.gilc.org/privacy/coe-letter-1000.html (accessed May 21, 2005) (The Global Internet Liberty Campaign, comprised of national and international organizations such as the American Civil Liberties Union, the Human Rights Network, Privacy International, and others, presented detailed objections to the CoE about the CoE Convention with respect to Data Protection, and privacy concerns. "We believe that the draft treaty is contrary to well established norms for the protection of the individual, that it improperly extends the police authority of national governments, that it will undermine the development of network security techniques, and that it will reduce government accountability in future law enforcement conduct").

184. Council of Europe, *Treaty*, *supra* n. 4, art. 23.

185. *See* Council of Europe, *Glossary*, *supra* n. 6 (explaining that a protocol is a legal instrument that compliments, amend or modifies the main treaty).

186. Constitution, *supra* n. 154.

187. *See id.* at Part IV, Art. IV-437(1).

188. *See id.* at Title IV, Art. II-107.

189. *See id.* at Title IV, Art. II-108.

and penalties,[190] and the prohibition against double jeopardy.[191] Additionally, the Constitution expressly prohibits any abuse of rights set forth in its other provisions.[192] This structural fix is, therefore, consistent with the prevailing international movement toward true harmonization.

VI. CONCLUSION

The decentralized nature of international law, particularly in the sphere of criminal law enforcement, may explain the CoE Convention's accommodation of flexible harmonization to achieve law enforcement goals aimed at the timely eradication of cybercrime. Having a sense for "what will fly" in the international body politic, heavily dependent upon cultural understandings and differences, must always be a practical and necessary concern.

However, cybercrime prosecutions will most certainly raise issues relating to concurrent jurisdiction and/or the application of domestic law to foreign nationals. While the particular offense conduct may be properly circumscribed, the means of investigating and prosecuting the conduct will not be predictable. The rights of an accused suffer where true procedural harmonization is excised from the convention model. Nowhere is this legal defect more apparent than in the disconnect between the treaty's incorporation of human rights treaties as the due process model, and the American constitutional legal precedent rejecting the same treaties as a source of rights protections for aliens.

In its present form, the CoE Convention allows state intrusions into the sphere of individual privacy rights to gather evidence for use in subsequent criminal prosecutions without adequate guarantees of procedural due process. One solution may be the addition of a Protocol to the treaty, modeled after the proposed CoE Constitution providing minimal guidelines for procedural due process, extended to citizens of all participating nations. In this way, the CoE Convention on Cybercrime could become a blueprint for future international endeavors to harmonize penal law enforcement.

---

190. *See id.* at Title IV, Art. II-109.

191. *See id.* at Title IV, Art. II-110.

192. *See id.* at Title VII, Art. II-114.