A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft via the Internet

Erin Suzanne Davis*

"What are we to do with borders that become meaningless? We're going to have to think of new ways to structure . . . our relationships with other nations so that people know there is no safe place to hide."[1]

I. INTRODUCTION

The Internet is a truly global medium,[2] especially in the realm of electronic commerce.[3] Thus, the Internet has been the source of many new legal and social issues facing the global community.[4] The availability of personal data on the Internet,[5] due considerably to the

---

* J.D. Candidate, 2003, Washington University School of Law.

1. Janet Reno, Speech to the Virginia Journal of International Law (Apr. 1, 2000), *at* http://www.usdoj.gov/archive/ag/speeches/2000/4100aguva.htm.

2. The Internet connects over 159 countries in the world. J.T. Westermeier & Jim Halpert, *E-Commerce Legal Survival Kit*, in 650 SOLVING THE LEGAL ISSUES AFFECTING B2B TRANSACTIONS 421, 426 (2001). In addition, estimates show that 65% of web users will be international by 2003. *Id.*

3. Estimates show "countries other than the United States will account for nearly half of the worldwide e-commerce." *Id*. This is because "websites are available anytime to anyone, anywhere in the world with access to the Internet." *Id.*

4. *See*, *e.g.*, Jim Wolf, *Nations Lack Cyber-Crime Laws; Experts Say Worldwide Investigation, Enforcement Difficult*, HOUSTON CHRONICLE, July 30, 2000, at 5 (discussing the problems involved with global cyber-crime detection and prevention); Reno, *supra* note 1.

5. The availability of personal information is a particular problem "because digital information is easier and less expensive than nondigital data to access, manipulate, and store, especially from disparate, geographically distant locations." Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 178 (1999). For instance, one may obtain a person's home address, phone number, and e-mail address through free services available on the Internet. Stephanie Byers, Note, *The Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS L.J. 141, 143-44 (2001). Further, information brokers, who offer their services for a fee, advertise on the Internet and make personal

rapid increase in commercial activity on the medium,[6] has caused an increase in cases of "identity theft."[7] Identity theft occurs when thieves use personal or financial information about a person (the victim) to create a fake identity for themselves in order to obtain money from either the victim or various other institutions.[8] Identity thieves use the Internet[9] as a weapon against individual consumers by taking personal and financial information,[10] such as credit card

---

information, including social security numbers, available to the general public through the medium. *Id.* at 144 (citing Beth Givens, *Identity Theft: How it Happens, Its Impact on Victims, and Legislative Solutions, at* http://www.privacyrights.org/AR/id_theft.htm (last visited Oct. 1, 2002)). Revenue from this type of product, including revenue from credit reporting agencies, is estimated to be in the "tens of millions" each year. U.S. GOVERNMENT ACCOUNTING OFFICE, REP. NO. GGD-98-100BR, IDENTITY FRAUD: INFORMATION ON LAW ENFORCEMENT EFFORTS, PREVALENCE AND COST, AND INDUSTRY AND INTERNET ISSUES 55 (1998) [hereinafter GAO REPORT], *available at* http://www.gao.gov.

6. Online retail orders increased 200% in 1998 alone. Christopher Paul Boam, *The Internet, Information, and The Culture of Regulatory Change: A Modern Renaissance*, 9 COMM. L. CONSPECTUS 175, 175 (2001).

7. Daniela Ivascanu, *Legal Issues in Electronic Commerce in the Western Hemisphere*, 17 ARIZ. J. INT'L & COMP. L. 219, 239 (2000). *See also* Timothy L. O'Brian, *Officials Worried Over Sharp Rise in Identity Theft*, N.Y. TIMES, Apr. 3, 2000, at A1, *cited in* Michael C. McCrutcheon, Article, *Identity Theft, Computer Fraud and 18 U.S.C. § 1030(g): A Guide To Obtaining Jurisdiction in the United States for a Civil Suit Against a Foreign National Defendant*, 13 LOY. CONSUMER L. REV. 48, n.2 (2001). Identity theft has been described as the "fastest-growing financial crime" in the United States. Byers, *supra* note 5, at 148 (quoting Heather Hayes, *Fighting the Plague of Identity Theft* (Oct. 11, 1999), *at* http://www.cnn.com TECH/computing/9910/11/id.theft.idg/index.html). In fact, Congress considered identity theft so much of a problem that it created the Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028 (Supp. IV 1998). The Act, endorsed and signed by President Clinton, strengthens controls on private identifiable consumer information by "mak[ing] it illegal to (without consent) knowingly transfer or use another person's identification means with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law." Boam, *supra* note 6, at 151.

8. Identity theft has been described as the "gathering [of] enough personal information about a person, such as their name, birthday, and social security number, in order to apply for credit cards in the victim's name." Maria Ramirez-Palafox, *Identity Theft on the Rise: Will the Real John Doe Please Step Forward?*, 29 MCGEORGE L. REV. 483, 483 n.2 (1998) (quoting Neil Munro, *Federal Reserve Board Eyes Online Privacy Rules*, WASH. TECH., Jan. 23, 1997). Cases of this type of theft are growing in the commercial world. *Id.* at n.3.

9. "[T]he Internet has become a breeding ground for cyber-criminals because it . . . is 'where the money is.'" Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON. L. REV. 237, 253 (2000). "Unlawful activity is not unique to the Internet—but the Internet has a way of magnifying both the good and the bad in our society . . . . [Therefore, w]e need to . . . find new answers to old crimes." *Id.* at 237 (quoting former Vice President Gore (Aug. 5, 1999)).

10. *Id.* at 244.

numbers[11] and social security numbers,[12] and then using that information to, among other things,[13] purchase products or launder money.[14] Such a scheme can be devastating for an identity theft victim[15] and can create financial costs for credit card companies and other commercial entities.[16]

The identity theft problem, though not entirely new, has created a host of new issues for the international law community because it can be perpetrated transnationally over the Internet quite easily.[17]

---

11. *Id.* Thefts of bank account numbers and access passwords are also common forms of identity theft. *Id.*

12. *See supra* note 5. Information brokers, such as www.infoseekers.com and www.fastbreakbail.com, sell social security numbers "for as little as $20." Givens, *supra* note 5. "Informational brokers allow identity thieves one-stop shopping in acquiring the personal details of their victims." JOHN Q. NEWMAN, IDENTITY THEFT: THE CYBERCRIME OF THE MILLENIUM 27 (1999), *quoted in* Byers, *supra* note 5, at 145. This problem does not just affect the United States. National identification numbers and systems, similar to social security numbers, are also used in the United Kingdom and South Africa. *See* R. Brian Black, Note, *Legislating U.S. Data Privacy In the Context of National Identification Numbers: Models from South Africa and the United Kingdom*, 34 CORNELL INT'L L.J. 397 (2001).

13. Identity thieves have been known to purchase cars and homes or even create a criminal record under another individual's identity. Givens, *supra* note 5.

14. Ivascanu, *supra* note 7, at 220; O'Neill, *supra* note 9, at 250.

15. *See* Givens, *supra* note 5 (discussing the arduous journey identity theft victims face when attempting to regain their good credit or good criminal records after a fraud has been uncovered).

16. Computer crime in general is becoming a large problem for companies. An FBI study, conducted along with the Computer Security Institute, noted that computer crime caused over 360 million dollars in losses for Fortune 500 companies between 1997 and 1999. Thomas J. Talleur, *The Eavesdropping Society*: *Electronic Surveillance and Information Brokering, in* 632 SECOND ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH AND CHANGING REGULATORY ENVIRONMENT 571, 578 (2001) (citing U.S. Attorney General Janet Reno, Remarks to the National Association of Attorneys General (Jan. 10, 2000), *at* http://www.usdoj.gov/archive/ag/speeches/2000/011000naagfinalspeech.htm). "[I]nternational computer crime is a growth industry, and neither political borders nor language barriers will limit this expansion." John T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. 317, 332-33 (1997). Additionally, U.S. federal law does not hold identity theft victims responsible for the bills that the perpetrators of these frauds incur. Givens, *supra* note 5. Instead, credit card companies as well as banks share the financial losses when identity thieves strike. *Id.*

17. "There are no country or territorial boundaries on the Internet." Westermeier, *supra* note 2, at 425. *See also* O'Neill, *supra* note 9, at 259-60. "[C]omputers may make it possible to reduce the risk of personal harm to the criminal by decreasing the probability of detection, and therefore punishment, while at the same time significantly increasing the expected return." *Id.* at 259. For instance, computer "hackers" who obtain illegal access to a system can use such access to steal personal and financial information from it. Soma et al., *supra* note 16, at 349. These hackers can gain large amounts of data quickly over the Internet, and, thus, they can be much more efficient criminals than if they decided to attempt a bank robbery, which takes

Because of the anonymity between the parties to an e-commerce transaction, it is much easier for a buyer of goods or services to illegally use another individual's personal information or account numbers without the seller detecting the fraud.[18] Anonymity also means that law enforcement authorities do not know the full extent of Internet fraud and identity theft.[19] Thus, the international community has begun to realize the need for international cooperation on this issue[20] and has attempted to address it in a variety of ways.[21]

Uniformity in civil and criminal laws regarding identity theft is needed in order for the international community to function effectively within the Internet medium.[22] No entity currently controls the information that passes over the Internet.[23] In addition, many of

---

extensive planning and creates a high risk of detection. O'Neill, *supra* note 9, at 259. This problem is compounded by the rise in transactions between individuals in one country and businesses in other countries. Prior to this development, the main source of international trade was business-to-business transactions. Peter P. Swire, *Of Elephants, Mice and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991, 1016 (1998). This increase exacerbates the existing problems involving such transactions and makes enforcement of laws even more difficult. *Id.* at 1017.

18. Westermeier, *supra* note 2, at 425-26. Enforcement is further complicated by situations in which an e-consumer and an e-seller do not know one another's nationality, or situations in which there is no physical shipment of goods and, thus, no "ready target" for regulation. Swire, *supra* note 17, at 1017.

19. GAO REPORT, *supra* note 5, at 50-51.

20. Indeed, the United States has been one of the countries proposing such cooperation. "The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national, and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides." President William J. Clinton & Vice President Albert Gore, Jr., A Framework for Global Electronic Commerce (1997), *at* http://www.w3.org/TR/NOTE-framework-970706.html (last visited Oct. 1, 2002), *quoted in* Jurisdiction in Cyberspace Project, American Bar Ass'n, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdictional Issues Created by the Internet*, 55 BUS. LAW. 1801, 1809 (2000) [hereinafter ABA Report].

21. *See infra* Part II.

22. "The lack of uniform national laws on computer crime, combined with discordant attitudes among countries towards this issue, results in varying degrees of enforcement and punishment." Soma, *supra* note 16, at 333. Uniformity is, thus, essential to detecting, investigating, and prosecuting identity thieves. Effective detection, investigation, and prosecution of identity thieves, in turn, will deter criminal activity more effectively and protect consumers by making it clear to the international public that identity thieves will not escape prosecution simply by being in a foreign nation. *See id.* (finding that the lack of uniformity is disadvantageous to extradition of criminals for computer crimes).

23. William Crane, Legislative Update, *The World-Wide Jurisdiction: An Analysis of Over-Inclusive Internet Jurisdictional Law and an Attempt by Congress to Fix It*, 11 DEPAUL-LCA J. ART & ENT. L. 267, 267 (2001).

the issues that the international community must confront when dealing with identity theft hamper international cooperation in prosecuting the crime. These issues include differing ideas on privacy and jurisdiction.[24] Additionally, complications arise from the attempt to achieve an effective balance between encouraging e-commerce[25] transactions while protecting consumers against the theft of their personal information.[26]

Part II of this Note examines both the purposes and the difficulties of maintaining international cooperation to control identity theft via the Internet. Part II also explains the various international conventions and resolutions that have been, or are being, promulgated to combat this problem. Part III analyzes the strengths and weaknesses of current attempts at international cooperation on cyber identity theft issues. Part IV of this Note proposes that the solution to these problems lies in strengthening international regimes to allow for the development of effective laws and law enforcement for identity theft crimes. The international community must create truly global agreements regarding cyber-crime that specifically target identity theft. In addition, the international community should create an international body to enforce laws on cyber identity theft and to work through the kinks of international cooperation. Finally, the international community must also consider creating an international tribunal to ensure a forum for international disputes involving issues such as identity theft.

---

24. *See infra* Part II.

25. There are many definitions of "e-commerce." Tapio Puurunen, Article, *The Legislative Jurisdiction of States over Transactions in International Electronic* Commmerce, 18 MARSHALL J. COMPUTER & INFO. L. 689, 691 (2000). For purposes of this Note, "e-commerce" refers to commercial transactions that occur via the Internet. Chelsea P. Ferrette, *E-Commerce and International Political Economics: The Legal and Political Ramifications of the Internet on World Economies*, 7 ILSA J. INT'L & COMP. L. 15, 21 n.33 (2000) (citing William F. Fox, Jr., *International Electronic Commerce*, GOING INTERNATIONAL: FUNDAMENTALS OF INTERNATIONAL BUSINESS TRANSACTIONS 159, 161 (A.L.I.-A.B.A. Continuing Legal Education Course 1999)).

26. *See infra* Part II.

II. ATTEMPTS AT INTERNATIONAL COOPERATION ON IDENTITY THEFT AND ISSUES SURROUNDING SUCH COOPERATION

A. Purposes Behind and Difficulties of International Cooperation

One important goal of international cooperation is uniformity. Uniformity is especially important in dealing with the Internet because international borders are practically invisible in this medium.[27] Uniformity also aids consumers and e-commerce participants by allowing for a degree of predictability in the kinds of laws and enforcement mechanisms available when an identity theft occurs over the Internet. In addition, uniformity aids law enforcement by making it easier to bring identity thieves to justice.[28] Finally, uniformity aids the e-commerce marketplace by helping to increase consumer confidence in privacy on the Internet.[29]

Another important goal is awakening law enforcement and others, such as the credit reporting industry, to the magnitude of the problem of identity theft in order to give these groups the impetus to deal with the problem.[30] Law enforcement may not be giving identity theft the attention it needs, viewing the crime as less important than more violent thefts such as armed robbery and car-jacking.[31] Many victims of identity theft find the current enforcement system difficult to

---

27. *See supra* note 17.

28. The U.S. Government Accounting Office noted several reasons why law enforcement has not historically tracked identity theft. These include "lack of a standardized definition of identity fraud." GAO REPORT, *supra* note 5, at 20. Thus, organized crime and individuals who would ordinarily perpetrate violent thefts are turning to identity theft as a way to carry out their crimes without the interference of law enforcement. Givens, *supra* note 5. There are other reasons that law enforcement may not be giving identity theft adequate attention. These include the fact that identity theft is really an element of many other crimes and the fact that "mere possession of another person's personal identifying information is not a crime in itself." *Id*.

29. A 1998 *Business Week* Survey noted that consumers who were not at that time using the Internet "ranked concerns about the privacy of their personal information and communications as the top reason they have stayed off the Internet." FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), *available at* http://www.ftc.gov/reports/privacy3/toc.htm. Thus, if uniformity in laws helps to curb instances of identity theft and compromise of consumer information privacy, Internet commerce would be positively affected.

30. Law enforcement officials in the United States have been known to be generally uncooperative in some instances either by not investigating or by not *adequately* investigating such crimes. Givens, *supra* note 5.

31. *Id.*

traverse[32] and are left with no truly viable way to deal with their situation once a thief has perpetrated such a fraud.

International cooperation in combating identity theft is difficult because each state[33] or group of states has a different idea about how to combat the issue, a different view of how much privacy invasion is allowed under a crime-fighting or civil litigation plan,[34] and a different system for regulating and granting jurisdiction. The divergent European and U.S. approaches illustrate this point.[35] The European approach to combating cyber-crime advocates more control to protect consumers and uses strict laws without regard to the effects on e-commerce companies.[36] Europeans consider personal privacy to have the utmost importance, and commercial concerns are addressed as secondary to this primary issue.[37] In the United States, however, the government has taken a more "hands-off" approach because of deeply ingrained laissez-faire economic attitudes.[38] The United States, with the exception of the Federal Trade Commission[39] and several laws proposed to tackle the identity theft problem,[40] generally focuses instead on industry self-regulation.[41] This attitude ignores

32. In many instances, law enforcement has been reluctant to help victims secure the documents needed to clear their credit ratings after such a crime has been committed. *Id.* In addition, credit card companies have been known to treat victims with disbelief, and the steps such companies take to prevent further fraud, such as flagging a victim's credit report, have been ineffective in preventing another fraud from occurring on the same account. *Id.*

33. To clarify, any reference to "state" in this Note is a reference to nation-states and not to states in the context of the United States federal system.

34. Ivascanu, *supra* note 7, at 234.

35. To understand the magnitude of this divergence, one must understand that the United States and the European Union are one another's largest trading partners. Cate, *supra* note 5, at 179. Thus, this problem is an enormous hurdle for cooperative efforts in the international arena.

36. Boam, *supra* note 6, at 185. Several Asian countries also subscribe to this view, including Singapore and India. *Id.* They, too, have instituted "rigorous privacy standards." *Id.*

37. *See id.* at 184; Cate, *supra* note 5, at 179-86.

38. Donna M. Lampert, Fernando Laguarda, & Amy Bushyeager, *Overview of Internet Legal and Regulatory Issues, in* 544 16TH ANNUAL INSTITUTE ON TELECOMMUNICATIONS POLICY AND REGULATION 179, 207 (1998). The United States must also worry about First Amendment principles that prohibit the government from "interfering with the flow of information, except in the most compelling circumstances." Cate, *supra* note 5, at 179-80. Europe's approach is in direct opposition to this constitutional mandate, which creates further problems for cooperation between the regions. *Id.* at 180.

39. Boam, *supra* note 6, at 185.

40. *See* Byers, *supra* note 5, at 149-54.

41. Boam, *supra* note 6, at 185. For example, the United States, along with Japan, issued a statement that "the private sector should lead in the development of electronic commerce and in

both consumers' cries for more protection[42] and a Federal Trade Commission report noting that self-regulation has not provided adequate protection for consumers.[43] This U.S. system opposes the traditional European practice of recognizing privacy as a basic individual right.[44]

International cooperation also faces the complicated task of balancing the competing needs of protecting consumers and encouraging e-commerce growth.[45] This is a difficult balance to strike, due in part to the differing values placed on consumer protection and privacy in various parts of the world.[46] In addition, any laws regulating e-commerce in order to protect consumers will necessarily add costs to e-commerce in a variety of ways.[47] For instance, changes to security measures that enhance personal privacy increase transactional costs for e-businesses and can lead to

---

establishing business practices" and that both countries would "avoid imposing unnecessary regulations or restrictions on electronic commerce." U.S.-Japan Joint Statement on Electronic Commerce (May 15, 1998), *available at* http://www.ta.doc.gov/digeconomy/usjapan.htm (last visited Jan. 14, 2003), *quoted in* Lampert, *supra* note 38, at 208. Although the Supreme Court has found that a "right to privacy" exists for Americans, this right is only effective against government intrusion and not against intrusions by private parties. Byers, *supra* note 5, at 145. This is another reason why self-regulation has been the United States' chosen mechanism for enforcement. Self-regulation mechanisms in the United States include the Better Business Bureau, Direct Marketing Association, and the Online Privacy Alliance, among others. Lampert, *supra* note 38, at 230-31.

42. Consumers "feel that . . . these efforts at self-regulation are not enough since they lack a clear enforcement mechanism and do not provide the level of guarantee that they expect in a commercial transaction." Ivascanu, *supra* note 7, at 240. In addition, some suggest the position of the United States on self-regulation weakens "the U.S. bargaining position for purposes of international negotiation," and thus, "coalition building and development of uniform policy positions with foreign corporate counterparts must be a near-term goal." Boam, *supra* note 6, at 205.

43. Federal Trade Commission, *supra* note 29. This report recognized five core principles in privacy protection: "(1) [Consumer] Notice/Awareness (2) [Consumer] Choice/Consent; (3) [Consumer] Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress." *Id.* Despite the fact that the report states that self-regulation did not adequately serve these principles, the FTC still felt that self-regulation was "desirable." *Id.*

44. Cate, *supra* note 5, at 179. This issue has been so important in Europe that the EU has threatened to suspend the flow of information to the United States. *Id.*

45. Ivascanu, *supra* note 7, at 233.

46. *See supra* notes 35-44 and accompanying text.

47. *See* Ivascanu, *supra* note 7, at 233. This issue "presents policy-makers with new challenges with respect to two seemingly disparate goals—creating an environment where the rights of citizens are protected, while avoiding unnecessary restrictions on transborder flows of personal data that could inhibit potential growth in e-commerce." *Id.*

reductions in productivity.[48] Moreover, especially in the credit reporting industry, there will be a financial cost to any system that makes personal information less readily available to private individuals and companies.[49]

Finally, differences in regulatory and jurisdictional concepts present another major obstacle to creating international cooperation on identity theft issues. Because of the nature of the Internet itself,[50] differing notions of jurisdiction among states make enforcement of laws and extradition of criminals extremely difficult.[51] A country can consider the locus of jurisdiction to be in one of many places, such as the consumer's or victim's state, the perpetrator's state, or the state in which the server is located that was used to commit the crime.[52]

---

48. Cate, *supra* note 5, at 222. There are real concerns that "[a]s e-commerce becomes more widespread, its growth in the long run may be stunted because of the privacy concerns of consumers." Ivascanu, *supra* note 7, at 233.

49. As "personal identifying information has a market value, and such information is widely used for many purposes within both the public and private sectors," any "restriction on [the] sale of personal identifying data could affect business/commerce." GAO REPORT, *supra* note 5, at 57.

50. "A connection between a physical location and an Internet address is both unnecessary and unimportant, in some instances, such a connection is non-existent as many enterprises solely exist digitally." Heaven, *supra* note 50, at 377. Traditional views of jurisdiction focused on the "absoluteness of boundaries and sovereign power within them," but when "changes in the economy and technology made cross-border contact common . . . jurisdictional assumptions changed" to accommodate the needs of a more interdependent world. ABA Report, *supra* note 20, at 1824-25. The Internet is another such change that must be accommodated in the international system.

51. Catherine P. Heaven, Note, *A Proposal for Removing Road Blocks from the Information Superhighway By Using an Integrated International Approach to Internet Jurisdiction*, 10 MINN. J. GLOBAL TRADE 373, 377 (2001). Jurisdictional differences are especially daunting for consumers because of the sometimes small amounts of money that they are seeking to protect in relation to the large transaction costs of pursuing claims in another state's jurisdiction. Ivascanu, *supra* note 7, at 239.

52. *Id.* at 1826-27. With the Internet, it may be that none of these are adequate. For example, consider that in the United States, a state court may have jurisdiction where a tort occurred if "the defendant's conduct and connection with the forum State are such that he should reasonably anticipate being haled into court there." World-Wide Volkswagen, Corp. v. Woodson, 444 U.S. 286, 297 (1980). Imagine how the Internet complicates this rule. In the case of identity theft over the Internet, the victim may be in one state, and the perpetrator in another. Both are working on computers, but they may be dealing with servers and websites located in still other states. Thus, the crime or incident giving rise to a civil action is committed without either party coming into direct contact with the other. An additional problem is determining the location of the information that the thief is stealing. It could be located on the server processing the information or in the hands of the one who possesses it or even in the same place as the owner of the information. Thus, jurisdiction is complicated by the fact that information by its

B. Current Attempts at International Cooperation[53]

1. European Union Data Protection Directive:[54]

The European Union (EU)[55] passed a directive in 1998 designed to restrict data collection, processing,[56] dissemination, and storage in

---

nature does not have a physical location, especially when the Internet is involved.

53. Other organizations (besides those discussed in this note) have also addressed cybercrime and data privacy issues. In 1990 the United Nations issued a resolution that called on member states to: (1) modernize national criminal laws and procedures; (2) improve computer security and crime prevention; (3) adopt measures to sensitize the people, the judiciary, and law enforcement to the problem; (4) adopt adequate training measures for law enforcement and judiciary groups as well to enhance prevention, investigation, prosecution, and adjudication of such crimes; (5) elaborate on rules of ethics in use of computers; and (6) adopt policies for computer-crime victims. Soma, *supra* note 16, at 360 (citing U.N. OFFICE AT VIENNA, CENTRE FOR SOCIAL DEVELOPMENT AND HUMANITARIAN AFFAIRS, INTERNATIONAL REVIEW OF CRIMINAL POLICY, NOS. 43 AND 44: UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME at 16 (1994)). Additionally, the United Nations Centre for International Trade Law (UNCITRAL) adopted a Model Law on Electronic Commerce in 1996 that applied to data messages used in commercial activities on the Internet. Ivascanu, *supra* note 7, at 225, 237.

The Organization for Economic Co-operation and Development (OECD) also joined the fight for protection of personal privacy when it issued a set of guidelines in 1980 on personal data and privacy. *Id.* at 236-37. "The OECD is an intergovernmental organization designed to foster multilateral discussions and co-operation on economic and social policies that have impacts beyond national borders." Stewart A. Baker, *Decoding OECD Guidelines for Cryptography Policy*, 31 INT'L LAW. 729, 732 (1997). The guidelines, promulgated in 1980, represent a voluntary international standard on issues such as collection limitation, purpose specification, use limitation, and security safeguards. Lampert, *supra* note 38, at 230. In 1986 the OECD was also the first international body to address the inadequacies of existing computer crime laws. Soma, *supra* note 16, at 358.

54. Council Directive 95/46/EC, 1995 O.J. (L 281) 31, *available at* http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html (last visited Oct. 1, 2002). Directives are legislation issued by the European Council and the European Commission. Gina Ziccolella, Comment, *Marshall II: Enhancing the Remedy Available to Individuals for Gender Discrimination in the EC*, 18 FORDHAM INT'L L.J. 641, 645 n.20 (1994) (citing Utz P. Toepke, *The European Economic Community—A Profile*, 3 NW. J. INT'L L. & BUS. 640, 645 (1981)).

55. The EU is the body designed to promote political and economic integration among some of the European states. *See* COLIN CAMPBELL ET. AL., POLITICS AND GOVERNMENT IN EUROPE TODAY, 27-29 (2d ed. 1995). The European Commission, a part of the EU, is composed of seventeen members. *Id.* at 30. Its functions include shaping legislation created by the EU. *Id.* The European Council, another part of the EU, coordinates the economic policies of EU member states. *Id.* at 31.

56. "Processing of personal data" means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, blocking, erasure or destruction." Council Directive 95/46/EC, art. 2(b), 1995 O.J.

Europe.[57] The directive encompasses all types of personal data.[58] It includes under its purview all information from European sources and in the rest of the world.[59] Additionally, the directive clearly recognizes an individual right to privacy.[60]

The directive is not self-executing;[61] it requires states to create implementing legislation on their own.[62] Therefore, the laws are different from country to country within Europe, depending on the legislation each adopts.[63] The directive also requires that member

(L 281).

57. *Id.*

58. Swire, *supra* note 17, at 998-99. The directive defines "personal data" as "any information relating to an identified or identifiable natural person." Council Directive 95/46/EC, art. 2(a), 1995 O.J. (L 281).

59. Chapter IV of the directive protects personal data that leaves the EU. *Id.* at Chapter IV. It requires that the non-member country wishing to use such data ensure "an adequate level of protection." *Id.* at art. 25. When such protection is not available in a non-member country, the information will not be transferred unless one of the exceptions in the article applies. Swire, *supra* note 17, at 1000. For a listing of these exceptions, see *infra note* 64. In effect, "multinational businesses [must] conform all of their data processing activities to European law" because it is very difficult to separate data collected in Europe from that collected in other areas of the world. Cate, *supra* note 5, at 184.

60. Byers, *supra* note 5, at 156. The directive states as its objective: "Member states shall protect the fundamental rights and freedoms of natural persons, and in particular their *right to privacy* with respect to the processing of personal data." Council Directive 95/46/EC, art. 1(1), 1995 O.J. (L 281) (emphasis added).

61. A self-executing agreement is "an agreement of which the provisions are automatically and without any formal or specific act of incorporation, part of the domestic law of a state and as such enforceable by the municipal courts." Andre Stemmet, *The Influence of Recent Constitutional Developments in South Africa on the Relationship Between International Law and Municipal Law,* 33 INT'L LAW. 47, 59 (1999).

62. The directive requires that all EU member states adopt "a strict privacy law that provides clear rights" to those whose personal information is being collected. Swire, *supra* note 5, at 999. Those who process such personal data must disclose to the person whose data is being processed, among other things, their identity and the purpose behind the processing. *Id.* Additionally, the directive only allows data collectors to use personal data for the strict purposes the collector has identified to the individual. *Id.* Further, the directive requires that states enact laws whereby data collectors must eliminate all data that is no longer needed. Stephen J. Davidson & Daniel M. Bryant, *The Right of Privacy: International Discord and the Interface with Intellectual Property Law*, 18 COMPUTER & INTERNET LAW. 1, 3 (2001). Finally, each member state must create independent public authorities to oversee personal data protection, and the member states must empower these authorities to hear complaints on data protection matters. Cate, *supra* note 5, at 183. Member states must also provide a way to hold data processors ("controllers") civilly liable for unlawful activities. *Id.* at 184.

63. "[T]he process of transposing the directive into national law introduces significant differences in the legal standards applicable to the processing of personal data in each member state." *Id.* at 195.

states enact laws prohibiting the transfer of data to non-member states that fail to ensure an "adequate" level of protection.[64] Different states, due to differing "traditions and approaches to privacy protection," also view this adequacy requirement in divergent manners.[65] Finally, when necessary for public security, defense, state security[66] and state activities involving criminal law, the directive allows states to forgo certain aspects of the agreement in adopting legislation.[67]

The directive includes some procedures designed to promote uniformity in the laws in Europe and in the treatment of non-member states that process European data.[68] First, the directive allows for its own revision over time. The EU can shape the directive to meet the challenges that will arise in order to ensure that countries in the EU work toward uniformity of data protection laws.[69] Second, the

---

64. *See supra* note 59. There are some exceptions to this "adequacy" rule:

> (1) the data subject has consented "unambiguously" to the transfer; (2) the transfer is necessary to the performance of . . . [certain] contract[s] . . . ; (3) the transfer is legally required or necessary to serve an "important public interest"; (4) the transfer is necessary to protect "the vital interests of the data subject"; or (5) the transfer is from a "register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest . . . ."

Cate, *supra* note 5 at 184 (quoting Council Directive 95/46/EC, art. 26(1), 1995 O.J. (L 281), which further states that these exceptions apply except where a member state chooses not to allow them as "provided by domestic law governing such cases.").

65. Ivascanu, *supra* note 7, at 234.

66. State security includes "the economic well-being of the State when the processing operation is bound up with questions of State security." Council Directive 95/46/EC, art. 3(2), 1995 O.J. (L 281).

67. *Id.*

68. Swire, *supra* note 17, at 1004.

69. *Id.* Article 33 of the directive requires that the commission report on the directive by October 2001, including proposal of possible amendments. *Id.* at 1004-05. "The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32(1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. This report shall be made public." Council Directive 95/46/EC, art. 33, 1995 O.J. (L 281). As of September 2002, the Commission had plans to hold a data protection conference on September 30 and October 1, 2002 in Brussels. Press Release, National Data Protection Commissioners, Commission Organizes Data Protection Conference to Look at Key Privacy Issues (Sept. 26, 2002), *available at http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/02/1373|0|RAPID&lg=EN&display=* (last visited Oct. 1, 2002). This conference was to be the "final part of the Commission's open consultation in preparation for its forthcoming report on how [the Data Protection Directive] is being applied." *Id.* For more information on this conference, see http://europa.eu.int/comm/internal_market/en/dataprot/lawreport/programme

directive creates the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data,"[70] composed of national experts that sit as an advisory panel designed to "render expert advice on matters arising under the Directive."[71] Finally, the directive allows for a committee to hear questions on the "adequacy" of protection in non-member states.[72]

Some representatives of the United States Congress have expressed concern over the directive.[73] They fear that "European data protection laws are on the verge of becoming the world's de facto privacy standard."[74] The United States is concerned that these data protection laws are too strict and "will have a 'potentially regressive impact on international commerce.'"[75]

_en.htm.

70. Swire, *supra* note 17, at 1005. Article 29 of the directive creates the Working Party, and the Party's duties are set out in Article 30. Council Directive 95/46/EC, art. 29-30, 1995 O.J. (L 281). Among other duties, the Working Party must "examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures"; "give the Commission an opinion on the level of protection in the Community and in third countries"; and "advise the Commission on any proposed amendment of this Directive . . . to safeguard the rights and freedoms of natural persons with regard to the processing of personal data . . . ." *Id.* at art. 30.

71. Swire, *supra* note 17, at 1005.

72. *Id.* Article 31 sets forth this process. Council Directive 95/46/EC, art. 31, 1995 O.J. (L 281). The Article 31 Committee aids the European Commission in adopting immediately effective measures to ensure that non-member states comply with the "adequacy" requirement. *Id.*; Swire, *supra* note 17, at 1005.

73. Patrick Thibodeau, *Europe's Privacy Laws May Become Global Standard*, COMPUTERWORLD, Mar. 12, 2001, *at* http://www.computerworld.com/governmenttopics/government/policy/story/ 0,10801,58498,00.html (last visited Oct. 1, 2002).

74. *Id.* Since the Directive's adoption in the EU, other countries such as Argentina, Australia, Canada, and New Zealand have adopted similar legislation. *Id.*

75. *Id.* (quoting Rep. Clifford Stearns (R-Fla) in Congress). Stearns made the statement as the chairman of the House subcommittee on Commerce, Trade and Consumer Protection. *Id.* Another House Republican, Steve Buyer, backed up Stearns's statement, going so far as to say that the EU's data privacy laws explain "the good judgment of [his] ancestors to leave the [European] continent." *Id.* However, Rep. Edward J. Markey (D-Mass) refuted Stearns's statement and the idea that Americans were anti-privacy and pro-business. He noted that surveys show Americans prefer stronger privacy rules like those in Europe. *Id.*

2. Safe Harbor Agreement (under the EU Data Directive)

In May 2000, the United States[76] and the EU entered into a Safe Harbor Agreement.[77] This agreement extended the EU's Data Directive to U.S. companies that use European data information in the United States.[78] The agreement affects only information that these U.S. companies gather as they generate databases in their European operations.[79]

The Safe Harbor Agreement does not require the United States to promulgate any new laws.[80] It simply states that those wishing to be covered under the EU Directive must register and pledge to abide by the directive's rules.[81] The Safe Harbor Agreement uses a "mixed system of enforcement" combining self-regulation with enforcement by EU data protection authorities.[82]

---

76. The U.S. Department of Commerce was responsible for the contribution of the United States to the agreement. Midge M. Hyman and Sandra N.S. Covington, *European Privacy and the Safe Harbor*, N.Y. L.J., Apr. 30, 2001, at § 6.

77. Boam, *supra* note 6, at 184. More information about the agreement is available at http://www.export.gov/safeharbor/ (last visited Jan. 9, 2003), a website operated by the U.S. Department of Commerce for businesses wishing to join. *See also* U.S. Dep't of Commerce, Int'l Trade Admin., Notice, Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45665-45686 (July 24, 2000), *cited in* Hyman, *supra* note 76.

78. Boam, *supra* note 6, at 184.

79. *Id.* In other words, the agreement does not cover situations in which a European accesses an American e-business website and voluntarily leaves his information there. *Id.*

80. *Id.*

81. *Id.* Companies register through the U.S. Department of Commerce, which subjects them to legal action by the Federal Trade Commission for "'deceptive trade practices' if they 'publicly disclose' and then do not follow the rules." *Id.* (citing Commission Decision on the Adequacy of Protection Provided by the Safe Harbor Privacy Principles, Annex I, 2000 O.J. (C 2441)). A company that chooses to sign on to the directive must choose one of three routes to comply with Safe Harbor Principles: "1. Join a self-regulatory program that adheres to the Safe Harbor Principles; 2. Develop [its] own self-regulatory privacy policies that conform with the Safe Harbor Principles; or 3. Comply with statutory, regulatory, administrative, or other laws that effectively protect personal privacy." Davidson, *supra* note 62, at 4.

82. Boam, *supra* note 6, at 184 n.82. The latter of these two types of enforcement occurs when human-resource specific data is transferred and when companies actually *agree* to cooperate with the EU authorities. *Id.* Sanctions under the Safe Harbor Agreement include suspension from the Safe Harbor, awards of damages to those individuals whose privacy was violated, public notice of non-compliance, and injunctive measures. Hyman, *supra* note 76.

The European Parliament[83] has criticized the Safe Harbor Agreement for offering less-than-adequate protection of personal privacy.[84] The Parliament argued that the agreement "neither provide[s] for monetary damages for breach [of the agreement] nor right of appeal in the United States."[85]

Additionally, American businesses have been reluctant to actually put the Safe Harbor Agreement to use.[86] As of the beginning of 2001, only twelve U.S. companies had signed on to the agreement.[87] Many argue that if the Safe Harbor Agreement is not utilized, "the effect of extraterritorial application of the [EU] Directive on U.S. multinational employers, and businesses in general, could be catastrophic."[88] Due to this lack of cooperation by U.S. businesses, the U.S. Department of Commerce began a series of nationwide seminars to encourage U.S. businesses to take advantage of the Safe Harbor Agreement and to make these businesses aware of the agreement's benefits.[89]

---

83. The European Parliament is created by Article 137 of the Treaty of Rome. Campbell, *supra* note 55, at 31. It is part of the institutional framework of the EU. *Id.* at 29-30. It consists of the 567 members elected to represent EU member states and exercises advisory and supervisory powers. *Id.* at 31-32. The Parliament's opinion on the agreement was non-binding. Boam, *supra* note 6, at 185.

84. Boam, *supra* note 6, at 184-85.

85. *Id.* at 185.

86. Brian Krebs, *US Businesses Slow to Adopt EU Safe Harbor Agreement*, NEWSBYTES, Jan. 4, 2001, *available at* http://www.newsbytes.com/news/01/160069.html.

87. *Id.*

88. Barbara Crutchfield George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply With the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 737-38 (2001). "[N]oncompliance with the Directive could mean that in this technological age there would be no transatlantic personal banking or brokerage transactions, no airline or hotel reservations, and no European credit card purchases." *Id.* at 738.

89. Krebs, *supra* note 86. These workshops began in January 2001. *Id.*

3. Council of Europe Convention on Cybercrime

In April 2000 the Council of Europe[90] introduced a draft convention to deal with the problem of cybercrime in Europe.[91] The convention is now complete and open for signatures.[92] In addition to criminalizing certain types of activities, the convention attempts to foster cooperation between countries in *prosecuting* such crimes.[93] The convention aims to define computer crimes to promote uniform national legislation, common criminal procedures, and resources for cooperation on an international level.[94] The convention holds perpetrators of computer crimes responsible for these acts even if their own countries do not consider the acts to be criminal.[95] The convention, however, does not provide for "cross-border investigations" of cybercrimes.[96]

---

90. The Council of Europe was created in 1948. WAYNE C. MCWILLIAMS & HARRY PIOTROWSKI, THE WORLD SINCE 1945: A HISTORY OF INTERNATIONAL RELATIONS 75 (3d ed. 1993). As of June 2001, forty-one member states make up the Council, fifteen of which are also members of the EU. Charles L. Kerr, *Online Privacy: Recent Developments, in* SECOND ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH & CHANGING REGULATORY ENVIRONMENT 51, 139 n.119 (Francoise Gilbert et al. eds., Practicing Law Institute 2001). The purpose behind the Council is to advance European unity and to promote "political pluralism and [protect] citizens' rights." Campbell, *supra* note 55, at 624. All members of the EU are members of the Council as well, and the Council cooperates with, but is not a part of, the EU. *U.S. Supports Two E-Commerce Treaties*, 18 E-COMMMERCE L. & STRATEGY 8 (June 2001).

91. Kerr, *supra* note 90, at 139.

92. Council of Europe Committee of Experts on Crime in Cyber-Space, Convention on Cybercrime, *opened for signature* Nov. 23, 2001, *available at* http://conventions.coe.int/treaty/en/Treaties/Html/185.htm (last visited Jan. 14, 2003).

93. The preamble to the convention states that one purpose of the treaty is to recognize the "need for co-operation between States . . . in combating cyber-crime and the need to protect legitimate interests in the use and development of information technologies." *Id.* The preamble specifically provides that the treaty is designed to foster "the detection, investigation and prosecution of [cyber-crime] offenses at . . . the international level" through greater international cooperation. *Id.*

94. *Cybercrime: Eagerly Awaited But Highly Controversial Convention*, TECH EUROPE, Mar. 15, 2001, *available at* www.lexis.com.

95. Crane, *supra* note 23, at 280 (citing Mark Ward, *Cybercrime Treaty Condemned*, BBC NEWS ONLINE, *at* http://news.bbc.co.uk/2/hi/science/nature/1072580.stm (last visited Oct. 15, 2002)).

96. *Cybercrime: Eagerly Awaited but Highly Controversial Convention*, *supra* note 94. In other words, "one State may conduct an investigation on behalf of another [when there has been an alleged Internet crime committed], but [the Convention] does not provide for . . . cross-border searches." *Id.* The reason such a provision was not added is because "the States negotiat[ing] the draft were unable to agree on that point." *Id.*

The United States, as well as several non-European countries, participated in the drafting of the convention and will have a chance to sign on. These observer nations[97] can thus join the other Council of Europe members in adopting the provisions of the convention.[98] The United States, Canada, Japan, and Australia have signed on to the Council of Europe as associate members in regard to this convention.[99]

The convention has met with opposition from several sources. Civil liberties groups in Europe have expressed concern that the convention would "expand police investigation powers too much" and would interfere with "freedom of expression."[100] In addition, the European Commission has criticized the convention for, among other things, the lack of data protection provisions.[101] Further, other non-governmental organizations and professionals have concerns that the convention will "kill the Internet" because of its "drastic penalties and its failure to respect user privacy."[102]

4. "London Meeting Draft" on Global Jurisdiction Issues Created by the Internet

The London Meeting Draft is a study administered by the American Bar Association and completed in June 2000 that focuses

---

97. For purposes of this Note, 'observer nations' refers to those nations that participated in the drafting of the convention but who are not members of the Council of Europe. *See* Kerr, *supra* note 90, at 140.

98. *Id.*

99. *U.S. Supports Two E-Commerce Treaties*, *supra* note 90.

100. Kerr, *supra* note 90, at 140. These concerns stem from the provisions allowing law enforcement to search and seize computer data as an evidence-gathering technique and to intercept communications during criminal investigations. *Cybercrime: Eagerly Awaited but Highly Controversial Convention*, *supra* note 94. The preamble of the convention attempts to alleviate such concerns by stating that the convention is "[m]indful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights." Convention on Cybercrime, *supra* note 92. The Director General of Legal Affairs for the Council of Europe, Guy de Vel, agrees with this Preamble notion of balance, stating that the convention has no provision for "an Orwellian-type electronic surveillance system." *Cybercrime: Eagerly Awaited but Highly Controversial Convention*, *supra* note 94.

101. Kerr, *supra* note 90, at 140. The Commission also expressed concern that the treaty could infringe on fundamental rights, such as the right to privacy. *Id.* Additionally, the EU was reportedly concerned that the convention "would overrule the EU data privacy protections." *U.S. Supports Two E-Commerce Treaties*, *supra* note 90.

102. *Cybercrime: Eagerly Awaited But Highly Controversial Convention*, *supra* note 94.

on international jurisdictional issues created by the Internet.[103] The London Draft proposes a "multinational 'Global Online Standards Commission,' to study jurisdiction issues and 'develop uniform principles and global protocol standards . . .' working with other international bodies considering similar issues."[104] Additionally, the London Draft suggests that the international community develop online dispute resolution mechanisms to deal with cyber-jurisdiction issues.[105]

There have been no major criticisms of this project because the London Draft is currently just a proposal and is neither legislation nor an agreement as are the EU Directive, the Safe Harbor Agreement, and the Council of Europe Convention.

III. STRENGTHS AND WEAKNESSES OF THE CURRENT ATTEMPTS AT INTERNATIONAL COOPERATION ON IDENTITY THEFT

A. European Union Data Directive

The EU Directive[106] has both positive and negative aspects in terms of international cooperation on identity theft issues. It is an important step in regional international cooperation, as it provides guidelines and principles that aid in uniformity in Europe.[107] In addition, by requiring members to adopt statutes on data protection,[108] the directive harmonizes legislation on identity theft.[109] Furthermore, the directive has been successful in pressuring countries not in the EU to adopt similar legislation.[110] Still, the directive

103. Boam, *supra* note 6, at 200.

104. *Id.* (quoting Press Release, Business Law Section, American Bar Ass'n, ABA Group Releases Study on Cyberspace Jurisdiction (Jul. 10, 2000), *available at* http://www.abanet.org/media/jul00/cyberspace.html (last visited Jan. 14, 2003)).

105. Asaad Siddiqi, *Welcome to the City of Bytes? An Assessment of the Traditional Methods Employed in the International Application of Jurisdiction over Internet Activities—Including a Critique of Suggested Approaches*, 14 N.Y. INT'L L. REV. 43, 103 (2001). The Draft also suggests "employing programmable electronic agents ("bots") [to help] protect [Internet] consumers . . . from Web sites that do not meet their personal standards." *Id*.

106. *See supra* Part II.B.1.

107. *See supra* Part II.B.1.

108. *See supra* note 62 and accompanying text.

109. Swire, *supra* note 17, at 1002.

110. *Id.* This is because many countries, like the United States, that have "extensive trade

remains an ineffective device for the type of uniformity necessary to provide adequate protection to consumers on issues of identity theft over the Internet.

First, the directive suffers because it is not self-executing. Because they allow countries to enact their own laws, agreements that are not self-executing do not lend themselves to uniformity in the law, even when the agreement provides uniform guidelines. Additionally, enforcement levels are bound to vary in such a system based on what types of laws and law enforcement options are available in a state.[111] Finally, because the system is based on individual national laws, the directive lacks some of the enforcement power it seeks.[112]

Second, the member states are not uniform in their response to the "adequacy" requirement for non-member states.[113] The adequacy requirement complicates uniformity for many of the same reasons as self-execution of the regulatory laws. Further complications arise from the fact that member states can opt out of the exceptions allowed under the directive for adequacy in non-member states.[114]

Third, while the directive succeeds in providing protections for consumers, its comprehensive scope, which encompasses all types of personal information and all information from European sources,[115] is so expansive that e-business companies in the rest of the world may find it too restrictive on their activities.[116] This is especially likely in

---

relations with the European Union might be found to lack adequate protection of privacy and thus might encounter limits on the transfers of personal information." *Id. See also supra* note 35 (discussing U.S. and EU trade relations).

111. Levels of enforcement vary from state to state because of "differences in views about proper policy and differing levels of enforcement resources and experience." Swire, *supra* note 17, at 1002.

112. "[N]ational or regional controls are particularly easy to circumvent in the Internet environment, simply by moving data processing activities outside of the territory affected." Cate, *supra* note 5, at 230. This is particularly a problem with identity thieves who can simply obtain personal information in, or move their falsified identification to, another forum. *See infra* note 146 on Sealand, a territory used in just such a fashion.

113. *See supra* note 64 and accompanying text; *see also* Swire, *supra* note 17, at 1002.

114. "The Member States thus retain the discretion to nullify or limit the important exceptions, which [have been] counted on by many organizations to permit transfers," since the directive went into effect in 1998. Swire, *supra* note 17, at 1003.

115. *See supra* note 58 and accompanying text.

116. There is concern that any individual who transfers some small bit of personal information out of the EU will be held personally liable or will make his or her corporation liable. Kevin Bloss, Note, *Raising or Razing the E-Curtain?: The E.U. Directive on the*

the United States where the focus, as discussed above, has been placed on self-regulation.[117] The fact that the directive is not self-executing becomes a part of this problem as well. By allowing individual states to enforce the adequacy requirement against non-member states, non-member states run the risk of having EU states destroy their information, deny them access to the EU market, or instigate legal proceedings against them.[118] This system obviously does not encourage e-commerce.

Finally, the directive fails to deal with the unique issues of the Internet.[119] The direct involvement of individual governments in regulation of data on the Internet is inadequate because of the global nature of the medium.[120]

B. Safe Harbor Agreement

The Safe Harbor Agreement,[121] while fostering international cooperation, also has several problems. The agreement is another important step toward international cooperation and differs from other agreements in that it allows specifically for cooperation between the United States and Europe, despite the differing views Europeans and Americans have on the economy and privacy. However, by allowing American companies to "opt in,"[122] the agreement does not promote uniformity. Further, because many companies are not signing onto the terms of the agreement, it is basically ineffectual.[123]

Protection of Personal Data, 9 MINN. J. GLOBAL TRADE 645, 648 (2000).

117. *See supra* note 41 and accompanying text.

118. Bloss, *supra* note 116, at 649 (citing Council Directive 95/46/EC, 1995 O.J. (L 281)).

119. Cate, *supra* note 5, at 230. For one, the directive was drafted before the World Wide Web was invented, and thus it is "ill-suited to a far-flung, inherently global medium such as the Internet." *Id.* The directive's centralized approach creates problems in a world where data processing takes place in many varied and decentralized locations. *Id.*

120. *Id*. at 231. "The technologies and current structure of the Internet largely frustrate regulation." *Id.*

121. *See supra* Part II.B.2.

122. *See supra* note 81.

123. *See supra* note 86 and accompanying text.

C. Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime[124] is a major step toward international goals of uniformity. Participants in the drafting included the United States, Australia, Canada, and Japan, as well as Europe.[125] The participation of so many states has also aided the treaty in achieving a more global perspective on identity theft issues—one that encompasses at least some non-European notions. Further, the convention does not rely on self-regulation, as the U.S. approach prefers.[126] The convention's emphasis on active enforcement is important because the Internet, by making information so easily accessible, is an environment in which it is much easier to perpetrate an identity theft than in the real world.[127] Additionally, if one goal is to foster e-commerce, then international cooperation must focus on allaying consumer fears about identity theft when they participate in an online business transaction.[128]

However, several important problems plague the treaty. First, if early opposition proves correct,[129] the privacy issue between Europe and the United States will be a daunting hurdle to overcome. The convention, because it is based on European ideals, does not offer the kind of free access to personal information to which U.S. businesses are accustomed.[130]

The United States may also face constitutional constraints, including First and Fourth Amendment issues, if it tries to sign on to the convention.[131] The convention, while a more international effort than the EU directive, will still face issues of free speech and unlawful searches and seizures when U.S. businesses are involved.[132]

---

124. *See supra* Part II.B.3.
125. *See supra* note 90 and accompanying text.
126. *See supra* note 41 and accompanying text.
127. *See supra* note 5 and accompanying text.
128. *See supra* note 29 and accompanying text.
129. *See supra* notes 100-02 and accompanying text.
130. As one writer noted, "[While i]t is clear that strong privacy protection is needed if e-commerce is to flourish . . . this protection must also strive not to restrict the free flow of information, which is one factor that makes e-commerce such a powerful tool." Ivascanu, *supra* note 7, at 235. While Ivascanu was criticizing the EU Directive when he made this comment, the criticism applies equally to the Convention on Cybercrime.
131. *U.S. Supports Two E-Commerce Treaties*, *supra* note 90.
132. *See supra* note 100 and accompanying text.

Finally, the convention lacks data protection laws of the type necessary to curb identity theft and its effects because it does not provide victims of identity theft with civil remedies. It also does not adequately address the types of personal information identity thieves use to perpetrate their crimes, such as social security numbers.

D. "London Meeting Draft" on Global Jurisdiction Issues Created by the Internet

The London Meeting Draft's proposal of creating a Global Online Standards Commission[133] is a good first step in creating a forum for discussion on multinational identity theft issues.[134] Creation of such a task force would prove beneficial because it would supply a group of people that could constantly look for ways to tweak the system and work out the kinks of international cooperation.[135] It is important that the United States, as one of the global leaders in Internet use,[136] be intimately involved in discussions about and promulgation of international rules on the subject. The London Draft's suggestion of developing forms of dispute resolution on cyber-issues[137] is another novel idea that could offer aid for consumers facing an identity theft.

---

133. *See supra* Part II.B.4.

134. This Commission would, of course, also be helpful in dealing with all types of cybercrime issues, not just those involving identity theft.

135. Some commentators have suggested that such an idea is utopian. *See, e.g.,* Siddiqi, *supra* note 105, at 103. However, such a suggestion implies that utopia is not something toward which the world should strive. While it is "hard to believe that sovereigns would work together to form a common bond over the Internet," *id.*, sovereign nations may be forced to do so if jurisdictional and other complicated issues involving the Internet leave consumers unprotected against identity theft in the virtual world. This same commentator, however, offers a good suggestion: A state could "begin to educate its Internet users that they may be subject to the laws of other jurisdictions and therefore be found liable—criminally or civilly." *Id.*

136. Out of the 304 million Internet users in the world, 45% are residents are the United States or Canada. Boam, *supra* note 6, at 175.

137. *See supra* note 105 and accompanying text.

IV. FOSTERING INTERNATIONAL COOPERATION ON IDENTITY THEFT

A. Global Treaty

One major step toward uniformity and prevention of identity theft over the Internet is the creation of a truly global treaty[138] on the subject. In order for a treaty dealing with identity theft to be successful, other non-European and non-American countries must be encouraged to participate. The Council of Europe Draft Convention on Cybercrime[139] is an important step in this direction. It is a workable agreement, assuming that it actually will be expanded to include other parts of the globe as well as crime specific laws and civil remedies dealing with data protection and identity theft.[140] The convention must explicitly contain such protections. In addition, other states must be encouraged to join to make the convention even more global than it already is.[141]

The ideal treaty on identity theft must also create laws that do not focus on industry self-regulation. Its provisions must force credit companies to adhere to policies that both prevent identity theft crimes and allow victims to more easily gain the information and protection they need to restore their credit records and prevent future breaches of their accounts.[142]

B. Formal Body to Coordinate Enforcement

The participating states must make a formal coordinated effort to resolve the enforcement[143] and jurisdictional issues involved in

---

138. Despite the significant shortcomings of treaties as identified by some critics, a treaty is an appropriate starting point for international cooperation because treaties establish "a baseline of agreement between nations." Siddiqi, *supra* note 105, at 101. In addition, state governments may regard treaties more seriously than they would "dramatic and confusing technological 'solutions.'" *Id.*

139. *See supra* Part II.B.3.

140. *See supra* Part II.B.3.

141. *See supra* note 99 and accompanying text.

142. Some have suggested that identity theft will "continue to climb at epidemic proportions" if laws are not promulgated to encourage the credit industry to change their practices. Givens, *supra* note 5.

143. The United States would surely support such an effort as many have recognized the importance of such cooperation on enforcement issues. *See, e.g.*, Wolf, *supra* note 4 (quoting

identity theft over the Internet.[144] The London Draft[145] is an important step in this direction because it provides a forum for discussion and compromise on jurisdictional issues.[146] However, the forum should be extended to deal with issues such as enforcement.[147] This forum could be used not only to coordinate enforcement efforts, but also to educate law enforcement officials in all parts of the Internet-using world about the urgency of the identity theft problem and the importance of identity theft prevention.[148]

C. Formal Body to Try Crimes

Another step that an international coordinated effort may need to explore is the creation a formal body to try major identity theft crimes[149] on an international level. There are, however, many problems with addressing international cooperation in this way. One question that would arise is whether to expand an existing tribunal to try such issues or whether to develop a new tribunal to handle such

---

Edgar Adamson, head of the U.S. National Central Bureau, which is responsible for coordinating with INTERPOL the "global police alliance," as saying, "[T]he border-hopping nature of cyber crime showed the need for international law enforcement cooperation has never been greater." (internal quotations omitted)).

144. One enterprising student note even suggested making the Internet an "international space" similar to space or the law of the sea. *See* Heaven, *supra* note 50, at 374. Under this theory, "nationality, not territory, is the basis for jurisdiction. Thus, the person who created or controls the website or links to websites attaches his or her nationality to the site and creates virtual islands." *Id.* at 390. Another theoretical approach would be to treat the Internet as an independent "territory," which would create "an entirely new landscape for human interaction." Siddiqqi, *supra* note 105, at 94-96.

145. *See supra* Part II.B.4 and Part III.D.

146. For instance, the group could discuss Sealand. Sealand is a "country" of sorts located on an abandoned anti-aircraft platform off the coast of England. Siddiqi, *supra* note 105, at 91-92. Sealand was supposedly formed when a person moved onto the platform and declared it his own country. *Id.* at 92. Sealand declares itself a "data haven." *Id.* at 91. The idea behind this is that companies or individuals can locate their servers on Sealand for the specific purpose of escaping existing jurisdiction laws around the globe. *Id.* at 92. *See also* Simson Garfinkel, *Welcome to Sealand. Now Bugger Off*, WIRED, July 2000, *at* http://www.wired.com/wired/archive/8.07/haven.html. If Sealand has its way and is treated as an area without jurisdiction, criminals will likely flock there to perpetrate mass amounts of identity theft.

147. The forum could be used to discuss any issues dealing with other cybercrimes and to work out any other kinks in the system.

148. *See supra* notes 30-32 and accompanying text.

149. The forum should reach a broader range of issues than just identity theft. It could include other major cybercrimes as well.

cases.[150] If the former is chosen, deciding which existing tribunal to use would be another difficult task. The International Court of Justice[151] (ICJ), for instance, would not be a good choice because only states may be parties to ICJ proceedings.[152] Thus, a state would have to bring its case on behalf of a victim, and the state housing the alleged perpetrator would have to agree to come to the court for such a hearing. Another possibility would be the International Criminal Court (ICC), but there are problems with this idea as well. First, the United States has not ratified the treaty creating the ICC.[153] Second, the ICC, like the ICJ, has limited jurisdiction.[154] Either way, the creation of a new tribunal or the expansion of an existing one will cost the international community a great deal of time and money. One possible solution is that those countries who agree to use the new or updated tribunal as the forum for international e-commerce disputes could bear the burden[155] of funding such a venture.

---

150. Many have suggested that there are already too many smaller specialized or regional courts and tribunals in the world. H.E. Judge Gilbert Guillaume, President of the International Court of Justice, Address to the General Assembly of the United Nations (Oct. 30, 2001), *available at* http://www.icj-cij.org/icjwww/ipresscom/SPEECHES/iSpeechPresident_Guillaume_GA56_20011030.htm (last visited Jan. 14, 2003).

151. The International Court of Justice was established, along with the United Nations, after World War II. MARK W. JANIS & JOHN E. NOYES, INTERNATIONAL LAW: CASES AND COMMENTARY 260 (2d ed. 2001). The ICJ works within the framework of the United Nations, as its contentious jurisdiction is part of the U.N. Charter. *Id.* In addition, the ICJ can "render advisory opinions pursuant to Article 65 of its Statute and Article 96 of the U.N. Charter itself." *Id. See also* Statute of the International Court of Justice art. 65, *found in* Janis, *supra* at 866; U.N. CHARTER art. 96, *found in* Janis, *supra* at 850.

152. Statute of the International Court of Justice art. 34(1), *found in* JORDAN PAUST et al., INTERNATIONAL CRIMINAL LAW DOCUMENTS 15 (Supp. 2000). In addition the ICJ is currently at its caseload capacity. H.E. Guillaume, *supra* note 150. Thus, expanded use of the court for such purposes would be costly to the United Nations.

153. The ratification process will not be easy in the United States due to strong objections by many to the ICC. International Criminal Court Overview, *available at* http://www.unausa.org/programs/icc.htm#overview (last visited Jan. 12, 2002).

154. "The jurisdiction of the Court shall be limited to the most serious crimes of concern to the international community as a whole. The Court has jurisdiction with this Statute with respect to the following crimes: (a) The crime of genocide; (b) Crimes against humanity; (c) War crimes; (d) The crime of aggression." Rome Statute of the International Criminal Court, PAUST, *supra* note 152, at 207-08. It is doubtful that the international community would consider cybercrimes, such as identity theft, as serious enough to warrant ICC jurisdiction alongside crimes such as genocide and crimes against humanity.

155. The countries agreeing should bear this burden proportionally to the amount of Internet use that occurs in the country. Thus, the United States would pay a large amount for these changes, while a developing country with no Internet usage would pay nothing.

D. Cooperation and Compromise

In dealing with the privacy issue,[156] both sides will have to compromise before uniformity is possible. Europeans will have to learn to live with a somewhat diminished protection on their personal information.[157] U.S. businesses will bear the brunt of the changes, however.

U.S. businesses must accept more restraints on their freedom when they transact internationally than they are used to in their domestic transactions.[158] The United States must allow heightened protection of consumer privacy if it is to protect consumers adequately against identity theft over the Internet. Privacy has been considered an important concept in American society, and the Supreme Court has protected privacy on many occasions as a constitutional right.[159] However, the Constitution is considered to protect privacy only against *government* intrusions. Therefore, the United States will have to pass legislation allowing for the protection of privacy from intrusion by private entities. This burden on business seems fair, however, because heightened security measures designed to protect consumer information will also likely improve consumer confidence in the Internet as a commercial medium.[160] This consumer confidence, in turn, can be expected to bolster e-commerce in the long run by helping to increase sales of goods and services over the Internet.

States must also to reexamine the concept of sovereignty before full international cooperation over Internet issues is possible.[161] No state should be required to forgo the idea of itself as a separate entity from other states with full power over its own territory and destiny.

---

156. *See supra* notes 35-44 and accompanying text.

157. To some extent the Convention on Cybercrime already takes some privacy away from Europeans by allowing law enforcement to search and seize some computer information. *See supra* note 100 and accompanying text.

158. *See supra* note 41 and accompanying text.

159. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (holding that the right to privacy protects a individual's decision to use birth control measures).

160. *See supra* note 29 and accompanying text.

161. This is what former Attorney General Janet Reno terms getting "away from the buttheaded notion of sovereignty." Reno, *supra* note 1.

The scope of this sovereignty must be redefined, however.[162] Trust is an essential element of this redefined sovereignty. States must earn the trust of others and learn to trust the judgments of others for international cooperation to truly become a reality.[163] This task will be especially daunting in the post-September 11 world.

V. CONCLUSION

It will be a long and arduous process before major progress in global cooperation on cyber-identity theft can be realized. In fact, a "perfect cyber-world" is likely an impossibility. Attempts to work toward this utopian ideal should continue, however, if we are ever to see a world in which individuals can safely use the Internet to its full potential.

The steps suggested above[164] all entail lofty goals. The hurdles cooperating states face, such as the surrendering of some sovereignty and the compromising of strategies, will likely prove difficult enough that a high degree of cooperation on identity theft is, for now a distant, though exciting prospect.

---

162. Some have noted that this redefinition of sovereignty should instead be directed against the Internet medium itself. Some commentators recommend viewing the Internet as its own territory. *See* Siddiqqi, *supra* note 105, at 94-96.

163. Janet Reno tells the story of a Minister of Justice who told her how much his country trusts the U.S., but then refused to extradite one of his country's nationals to the U.S. for prosecution in a murder case. Reno, *supra* note 1. Reno decrees that "if we're going to trust each other he should trust us enough to know that we can prosecute his national in a fair way according to principles of due process." *Id.* While this is a good illustration, Reno's account is an understandably America-centric view that must be countered with the notion that states have to *earn* each other's trust in such areas by prosecuting and regulating their own Internet criminals in a manner that comports with the ideals put forth by the international community.

164. *See supra* Part IV.