International Computer Fraud: A Paradigm for Limiting National Jurisdiction

*Ellen S. Podgor**

TABLE OF CONTENTS

INTRODUCTION 268
I. CRIMINAL COMPUTER FRAUD 272
A. *Computer Crime* 272
B. *Fraud* 278
C. *Criminal Computer Fraud* 279
II. EXTRATERRITORIAL JURISDICTION 281
A. *Statutory Recognition of Extraterritoriality* 284
B. *International Bases* 287
1. Jurisdictional Bases 288
2. A Limit on Jurisdictional Bases 291
3. Criminal Jurisdiction in Cyberspace 293
4. Jurisdiction for Computer Fraud Prosecutions 294
C. *A Proposed Federal Approach* 297
III. INTERNATIONAL INITIATIVES AND PERSPECTIVES 299

---

* Professor of Law, Georgia State University College of Law. John S. Stone Visiting Endowed Chairholder, University of Alabama School of Law, Fall 2001. Visiting Professor of Law, University of Georgia School of Law, Fall 2000. Visiting Scholar, Yale Law School, Fall 1998. B.S., 1973, Syracuse University; J.D., 1976, Indiana University School of Law at Indianapolis; M.B.A., 1987, University of Chicago; L.L.M., 1989, Temple University School of Law. The author wishes to thank Professors Jonathan S. Berck and Eli Lederman for their helpful comments on drafts of this paper and the participants in the Southeastern Association of American Law Schools (S.E.A.A.L.S.) and University of Alabama School of Law, where drafts of this paper were presented. The author also thanks Georgia State University College of Law for its financial assistance during the writing of this article.

A. Council of Europe Draft Convention on Cybercrime 299
B. The Stanford Conference 301
C. International Space Jurisdiction 303
IV. RAMIFICATIONS OF EXTRATERRITORIAL PROSECUTION OF CRIMINAL COMPUTER FRAUD 304
A. Punishment 305
B. The Merging of Civil and Criminal Fraud 307
C. Imposing United States Law on Other Nations 308
D. Constitutional Considerations 309
E. Identity 310
F. Kidnapping and Luring the Perpetrator to the United States 311
V. LIMITING EXTRATERRITORIAL PROSECUTION OF COMPUTER FRAUD 313
A. Specific Congressional Language 313
B. Reconfiguring Objective Territoriality 314
C. Enforcing the Reasonableness Doctrine 315
CONCLUSION 316

INTRODUCTION

Historically, most penal laws in the United States were not afforded extraterritorial application.[1] For the most part, the locus of the criminal activity determined the place of prosecution.[2] This premise, however, has become like the hearsay rule, with more and more exceptions diluting the initial rule.[3] Today, globalization has taken U.S. law enforcement to a point where many prosecutions are premised upon conduct occurring outside the United States.[4] It is common for federal prosecutors to proceed against individuals who are located outside the United States and who have perpetrated crimes beyond the borders of

---

[1] LEA BRILMAYER, AN INTRODUCTION TO JURISDICTION IN THE AMERICAN FEDERAL SYSTEM 336 (1986).

[2] The United States, however, did have consular courts in some countries with the purpose of prosecuting U.S. citizens who committed crimes in those countries. Consular courts no longer exist. *See* EDWARD M. WISE & ELLEN S. PODGOR, INTERNATIONAL CRIMINAL LAW: CASES AND MATERIALS 241 (2000) (discussing history of consular courts).

[3] *See* United States v. Bowman, 260 U.S. 94, 98-100 (1922) (discussing circumstances when criminal statutes can have extraterritorial application). *Since Bowman*, courts have expanded the extraterritorial application of U.S. laws. *See*, e.g., United States v. Parness, 503 F.2d 430, 439 (2d Cir. 1974) (finding extraterritorial application of enterprise element of RICO statute); United States v. Cotton, 471 F.2d 744, 750 (9th Cir. 1973) (permitting prosecution for theft of government property that occurs outside United States).

[4] *See infra* notes 68-70 and accompanying text.

this country.[5] Computers present a new issue for consideration in determining the extraterritorial application of United States criminal laws. At first blush, the universal speed and accessibility of computers would seem to make computer-related crimes appropriate for broad extraterritorial jurisdiction. After all, a touch of a mouse by a person in one country can be destructive and criminal in another country. As stated by former Attorney General Janet Reno, "[a] hacker needs no passport and passes no checkpoints."[6] Criminal computer conduct that occurs outside the United States can easily affect those within the United States. When this happens, some might argue that the United States should be able to exercise extraterritorial jurisdiction over the perpetrator.

Further reflection, however, reveals problems with having such a broad exercise of extraterritorial jurisdiction. Should the United States acquire jurisdiction of all criminal activity when the medium for the crime involves the use of a computer, and the activity has an effect in this country? Should every "I Love You"[7] type worm or virus that invades the United States be the source of a criminal prosecution within this country? When computers are involved in the criminal activity, the issue of extraterritorial application is not simplistic. Whether one standard should apply to all computer crimes, whether the focus should be on the

---

[5] *See generally* WISE & PODGOR, *supra* note 2, at 28-178 (describing array of different federal offenses that prosecutors have used for conduct occurring outside United States).

[6] Former U.S. Attorney General Janet Reno, Keynote Address at the Meeting of the P-8 Senior Experts' Group on Transnational Organized Crime (Jan. 21, 1997), *available at* http://www.usdoj.gov/criminal/cybercrime/agfranc.htm. One of the President's working groups repeated this metaphor in its report on cybercrime. PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, 21 (Mar. 2000) [hereinafter ELECTRONIC FRONTIER], *at* http://www/usdoj.gov/criminal/cybercrime /unlawful.pdf.

[7] The estimated cost of damages to businesses worldwide resulting from the "I Love You" virus was $6.7 billion dollars. Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice, Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime, A.4. (Dec. 1, 2000), *at* http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm; *see also* Lev Grossman, *Attack of the Love Bug*, TIME, May 15, 2000, at 49 (stating that "I Love You" virus caused estimated $10 billion in damages). The "I Love You" worm is just one email virus that has been internationally followed. *CHIPS to Fight Cybercrime*, TIMES UNION, July 31, 2001, at B3, *available at* 2001WL 24802478 (stating that "Melissa" virus caused more than $80 million in repairs). *See* Kevin Johnson, *'Mafiaboy' Trying to Stare Down Prosecutors*, USA TODAY, Dec. 5, 2000, at 10A (discussing sixteen-year-old Canadian who hacked into websites and caused estimated $1.3 billion in lost business); Nancy Parello, *'Melissa' Created By N.J. Man, Officers Say*, ATLANTA J. & CONST., Apr. 3, 1999, at 1F.

criminal act as opposed to the medium used to commit the act,[8] and whether the location of the alleged perpetrator or victims should control, are just some of the many issues for consideration.

This Article undertakes a re-evaluation of the basic principles of international criminal jurisdiction to assess whether United States extraterritorial application is warranted in cases involving computer fraud.[9] The Article is limited to one segment of computer criminality, namely, fraud, but offers considerations that may likewise serve as a starting point for resolving the many jurisdiction issues that accompany computerization.[10] It is important to note, however, that issues of cyberterrorism and issues that directly affect the self-defense of the United States raise a host of other considerations that are not the focus of this Article.[11] Although this Article discusses some of the ongoing international discussions related to jurisdiction with respect to computer issues,[12] it focuses on national law issues that can remain irrespective of

---

[8] *See* Robert J. Sciglimpaglia, Jr., Comment, *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199, 213 (1991) (discussing "ends" and "means" approaches to hacking).

[9] This Article does not explore issues of cyberterrorism or the cooperative efforts that the United States has instituted to protect its "critical infrastructure." *See National Security Advisor Rice Says It's Time to Prepare for Cyber-Terrorism*, 1 Cybercrime L. Rep. (P & F) No 1, at 6 (Apr. 9, 2001).

[10] This Article limits its scope to federal jurisdiction, although it recognizes that many of the questions regarding extraterritoriality can arise in state prosecutions that involve conduct occurring outside the United States. *See* Terrence Berg, *www.wildwest.gov: The Impact of the Internet on State Power to Enforce the Law*, 2000 B.Y.U. L. REV. 1305, 1327-36 (2000) (discussing extraterritorial state jurisdiction of Internet crimes). Nor is limiting this Article to federal actions meant to diminish the importance of state prosecutions that might involve extraterritorial conduct falling within the United States' borders. *See* Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117 (1997) (discussing regulation of cyberspace by states). This Article *also* excludes from its discussion computer-related conduct of foreigners within the United States. Jurisdiction of these offenses is presumed since the locus of the crime is within this country. *See Day Trader Convicted of Charges of Stock Manipulation by Internet*, 1 Cybercrime L. Rep. (P & F) No. 1, at 5 (Apr. 9, 2001) (discussing Internet securities fraud case of Canadian citizen who resided in Houston).

[11] Principles of necessity and proportionality, as opposed to questions of jurisdiction, may guide military responses in self-defense to terrorist acts. *See, e.g.*, Robert J. Beck & Anthony Clark Arend, *"Don't Tread on Us": International Law and Forcible State Responses to Terrorism*, 12 WIS. INT'L L.J. 153 (1994) (discussing United States' response to Iraqi government's attempt to assassinate Former President Bush); *Military Responses to Terrorism*, 81 AM. SOC'Y INT'L. L. PROC. 287 (1987) (discussing proposed responses to recent increases in terrorism directed against Americans). The question of whether cyberterrorism warrants a military response is beyond the scope of this article.

[12] International initiatives offer strong possibilities for future cooperation. Ad hoc tribunals and the Rome Statute of the International Criminal Court offer an increased progression toward an international recognition of the need to control crime from a global perspective. U.N. GAOR Int'l L. Comm., Rome Statute of the International Criminal Court,

the adoption of international treaties.[13]

This Article commences by providing an understanding of what will be encompassed within the term "computer fraud." The discussion turns next to United States federal extraterritorial jurisdiction in the prosecution of computer fraud acts that occur outside the borders of this country. Two avenues warrant consideration here. One examination focuses on the appropriateness of extraterritorial application under the explicit language of the pertinent criminal statute and congressional intent. A second examination looks at the appropriateness of extraterritorial application under international bases of jurisdiction.

U.N. Doc. A/CONF.183/9 (July 17, 1998), *available at* http://www.un.org/law/icc/index.html. These international tribunals, however, usually include only a limited number of crimes. Although a computer crime may in fact be a crime against humanity or war crime, and therefore encompassed within the tribunal, classic computer fraud acts are beyond the existing language found in these tribunals. *See, e.g., id.* Treaties, meetings, and conferences that consider computer crime from a global perspective are also emerging. *See* JEREMY BRANSTEN, *World: G-8 Countries Tackle Cybercrime*, RADIO FREE EUROPE, WEEKDAY MAGAZINE, (May 19, 2000) (discussing meeting of G-8 countries to discuss cybercrime), *available at* http://www.rferl.org/nca/features/2000/05/f.ru.000519122559.html; UNITED STATES-CANADA COOPERATION AGAINST CROSS-BORDER TELEMARKETING FRAUD, REPORT OF THE UNITED STATES-CANADA WORKING GROUP TO PRESIDENT BILL CLINTON AND PRIME MINISTER JEAN CHRÉTIEN,(Nov. 1997) [hereinafter U.S.-CAN. WORKING GROUP] (examining incidence of telemarketing fraud between United States and Canada and suggesting ways to address it), *available at* http://www.usdoj.gov/criminal/uscwgrtf/index.html. Recently, the Council of Europe produced a convention on cybercrime that may offer significant advancement toward global cooperation. Comm. of Experts on Crime in Cyber-Space, Council of Europe, Draft Convention on Cybercrime, *approved by* Eur. Comm. on Crime Problems, 50th Sess., June 18-22, 2001, Doc. No. CDPC(2001)17 [hereinafter Draft Convention], *available at* http://conventions.coe.int/Treaty/EN/cadreprojets.htm. This convention would require signatory countries to establish specific substantive and procedural laws for computer related offenses. *Id.* at ch. II, §§ 1-2. The Convention *also* provides for international cooperation. *Id.* at ch. III. United States businesses have expressed opposition to this convention. U.S. Business Interests, Rights Groups Still Dislike Internet Crime Treaty Draft, 1 Cybercrime L. Rep. (P & F) No. 6, at 14 (June 4, 2001) (quoting Jeffrey Pryce, international lawyer with Steptoe & Johnson, who stated "that businesses have three major concerns with the proposed treaty — the apparent criminalization of ordinary activities, third-party liability, and burdensome and invasive interception requirements"). *Id.* In the process of waiting for international solutions, courts should not leave decisions on how to regulate this conduct to prosecutorial discretion. Permitting individual prosecutors to make decisions regarding when an extraterritorial crime will be prosecuted would allow for inconsistency and inaccuracy within the law. *See* Ellen S. Podgor, *The Ethics and Professionalism of Prosecutors in Discretionary Decisions*, 68 FORDHAM L. REV. 1511 (2000).

[13] Treaties do not always resolve issues regarding the boundaries of national law. *See, e.g.*, United States v. Alvarez-Machain, 504 U.S. 655, 663-66 (1992) (holding that United States-Mexico Extradition Treaty did not preclude abducting individual from Mexico to stand trial in United States).

Irrespective of the criminal statute that is the source for the prosecution, the international bases of jurisdiction can easily be satisfied when the medium for the criminal act is a computer and the victims of the crime reside in the United States. But should traditional considerations in determining extraterritorial application permit the United States to prosecute computer fraud crimes that occur outside this country? The ease of use and worldwide accessibility of computers raise questions as to whether the traditional methodology for determining extraterritorial jurisdiction should apply. Noting the ramifications of an expansive reading of extraterritorial jurisdiction, this Article stresses the importance of tempering prosecution of extraterritorial computer fraud acts.

I. CRIMINAL COMPUTER FRAUD

Globalization has made the topic of extraterritoriality a significant area of interest. Prior to examining extraterritorial application, however, it is necessary to note the context in which this discussion will take place. The discussion of extraterritoriality can take on a different complexion, oftentimes dependent upon the crime committed. As the following section will show, the importance of precision in discussing extraterritoriality is particularly pronounced with respect to cybercrimes.

A. Computer Crime

There is no generally accepted definition of the term "computer crime."[14] Internationally, there is a continuing debate "on just what constitutes a computer crime."[19] The most recent draft of the Convention on Cyber-Crime includes an array of different computer related offenses in its substantive criminal law provisions.[16] For example, one section

---

[14] *See* RICHARD W. ALDRICH, CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME 11-30 (USAF Inst. For Nat'l Sec. Studies, Information Operations Series, INSS Occasional Paper 32, Apr. 2000) (discussing various international definitions of computer crimes), available at http://www.usaafa.af.mil/inss/ocp32.doc.

[15] INTERNATIONAL REVIEW OF CRIMINAL POLICY — UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, UNCJIN, 8th U.N. Congress, Nos. 43 & 44,at 4, *available at* http://www.uncjin.org/Documents/irpc4344.pdf.

[16] The Draft Convention on Cybercrime includes sections on "Offenses against the confidentiality, integrity and availability of computer data and systems," "Computer-related offenses," "Content-related offenses," and "Offenses related to infringements of copyright and related rights." Each of these categories also may include subsections. Draft Convention, *supra* note 12, at ch. II, § 1, tits. 1-4.

that relates to "computer-related offenses" is subdivided into articles on computer-related fraud and computer-related forgery.[17]

The difficulty of defining "computer crime" arises partly because computers can serve many different roles in criminal activities.[18] They can be the "object" used to commit the crime,[19] the "target" of the criminal activity,[20] or tangential to the crime.[21] Further, the enormity of different criminal conduct associated with computer crimes provides an endless list of activities that can be encompassed within the term "computer crime." For example, computer crimes can include crimes involving pornography,[22] auction fraud,[23] telecommunication fraud,[24] copyright and piracy offenses,[25] online extortion plots,[26] identity fraud,[27]

---

[17] Article 7 is "Computer-related Forgery" and Article 8 is "Computer-related Fraud." Draft Convention, *supra* note 12, at ch. II, § 1, arts. 7-8.

[18] Ellen S. Podgor, *Computer Crime*, in ENCYCLOPEDIA OF CRIME & JUSTICE 221-28 (Joshua Dressler, ed., 2nd ed. forthcoming 2002); *see also* Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 934 (1996) (discussing how computer can be "target of the offense," "tool of the offense," or "incidental to the offense"); Joe D. Whitley & William H. Jordan, *Computer Crime*, E-1 ABA WHITE COLLAR CRIME INST. § 21.01[1], at 21-3 to 21-6 (1999) (describing how computer can be "object, subject, or instrument of a crime").

[19] Computers are often used as "communications tools" to commit online a traditional, "off-line" crime such as fraud or pornography. *See* ELECTRONIC FRONTIER, *supra* note 6, at 9-11.

[20] *Id.* at 7-9 ("This form of crime targets a computer system, *generally* to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server."). *Id.*

[21] Often the computer is merely the storage device used to keep information for criminal acts. *See id.* at 9.

[22] *See* George Ivezaj, *Child Pornography on the Internet: An Examination of the International Communities Proposed Solutions for a Global Problem*, 8 MSU-DCL J. INT'L L. 819 (1999) (discussing international initiatives that can be used for deterring child pornography); *see also N.C. Man Convicted in Internet Sex Case*, ATLANTA J. & CONST., May 2, 2001, at 6B. (discussing individual's alleged entry into chat room to carry on sexually explicit conversations with 13-year-old).

[23] *See Three in Texas Indicted for Mail Fraud in Connection with Internet Auctions*, 1 Cybercrime L. Rep. (P & F) No. 6A at 7 (June 18, 2001) (discussing defendants' use of Internet to sell items they did not possess); Karen Dean, *It's a Crime*, ATLANTA J. & CONST., Mar. 5, 2000, at 1H (noting how auction fraud is primary type of Internet fraud).

[24] *See* SECT. OF SCIENCE & TECH., ABA, GUIDE TO THE PROSECUTION OF TELECOMMUNICATION FRAUD BY THE USE OF COMPUTER CRIME STATUTES (1989).

[25] *See* Christopher P. Bussert, *Software Piracy, Napster and MP3s - Is Intellectual Property Safe?*, C-1 1ST ANNUAL CYBERCRIME INST., PROGRAM MATERIALS, INST. OF CONTINUING LEGAL EDUC. IN GA. (2000).

[26] *See* John Markoff, *Thief Reveals Credit Card Data When Web Extortion Plot Fails*, N.Y. TIMES, Jan. 10, 2000, at A1 (discussing alleged online extortion plot).

[27] *See Tycoons Targeted in Alleged Identity Fraud Scheme*, ATLANTA J. & CONST., Mar. 21, 2001, at 3E.

hacking,[28] cyberterrorism,[29] and cyberstalking.[30] Many of these crimes are traditional offenses that are now being committed through the use of a computer.[31]

The perpetrators, victims, and motives can also vary greatly in computer crimes. For example, one offender may be a juvenile hacker intent upon showing off his or her abilities to break into a government security system. Then again, the offender may be a terrorist breaking into the same system for the purpose of destroying the government entity.[32]

The vast array of activities that can be associated with computer crimes makes it simple to argue that one should focus on the act of the perpetrator and merely consider the computer the medium used.[33] The U.S. Department of Justice appears to endorse this approach.[34] In contrast, other commentators provide strong arguments that computers

---

[28] *California Man Gets 18 Months for Unauthorized Access and Causing Damage to Hundreds of Computer Systems*, 1 Cybercrime L. Rep. (P & F) No. 6A, at 8 (June 18, 2001) (discussing how computer intrusions compromised many computer systems); *see also* Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171 (2000); Matt Richtel, *Federal Cybercrime Unit Hunts for Hackers*, N.Y. TIMES, June 2, 1999, at A16.

[29] *See Cybercrimes: Infrastructure Threats From Cyber-Terrorists*, 4 CYBERSPACE LAW, 23 (Apr. 1999).

[30] *See* 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY, A REPORT FROM THE ATTORNEY GENERAL TO THE VICE PRESIDENT (Aug. 1999), *available at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

[31] *See, e.g.*, United States v. Champion, 248 F.3d 502 (6th Cir. 2001) (using Internet to coerce and entice minor to engage in sexual act). In some cases the crime may be dependant upon whether the conduct meets traditional elements of an offense, such as theft. Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921, 934-36, 940 (1989). Laws governing trade secrets and confidential computer information may focus on the exclusiveness of the protected item. *See generally id.* (explaining how these laws overlap to form "shared domain" beyond their "exclusive realms").

[32] The "hacker" who engages in the computer activity with a criminal intent to cause damage is often described as a "cracker." *See* Eric J. Sinrod & William P. Reilly, *Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 181-83 (2000).

[33] *See, e.g.*, Bruce P. Keller, *The Game's the Same: Why Gambling in Cyberspace Violates Federal Law*, 108 YALE L.J. 1569, 1575 (1999) ("[T]here is nothing unique about Internet gambling that should lead the federal government to abandon its traditional protective role in this area . . . .").

[34] "The Department of Justice ('DOJ') broadly defines computer crimes as 'any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution.'" Laura J. Nicholson et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207, 208-09 (2000) (citing NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989)).

need to be treated differently.[35] For example, Professor Neal Kumar Katyal presents the economic rationales for finding that "cyberspace is a unique medium" that demands a distinct set of rules.[36]

The federal statutory approach in the United States to computer crime offers little in resolving the differing approaches to this subject. On one hand, there exists a computer fraud statute, 18 U.S.C. § 1030, that examines seven different types of computer related conduct.[37] Based on

---

[35] *See* David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) ("Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility — and legitimacy — of laws based on geographic boundaries."); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1004 (2001).

[36] *Id.* Johnson & Post, *supra* note 35, at 1367.

[37] 18 U.S.C. § 1030(a), as amended by the USA Patriot Act of 2001, provides:

> (a) Whoever —
>
> (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y or section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
>
> (2) intentionally access a computer without authorization or exceeds authorized access, and thereby obtains —
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer if the conduct involved an interstate or foreign communication
>
> (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) —

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if —

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

Id. 18 U.S.C. § 1030(a) (1994 & Supp. V 1999), *amended by* USA Patriot Act of 2001, Pub. L. No. 107-56, tit. V, sec. 814(a)-(b), § 1030(a)(5), (7), 115 Stat. 272; *see* H.R. 3162, 107th Cong. § 814 (2001).

this statute, one might conclude that Congress recognizes a need to treat computer crimes separately. The statute includes different types of computer-specific conduct, such as acts involving the use of a computer for espionage,[38] browsing in a government computer,[39] interstate trafficking of passwords,[40] and extortion activity resulting from the use of a computer.[41]

When, however, one examines the sentencing guidelines used to formulate the prison sentences of those convicted under § 1030, one sees that the use of the computer reflects merely the means for committing a traditional form of crime. At present, the sentencing guidelines applicable to 18 U.S.C. § 1030 do not contain guidelines exclusive to computer fraud offenses. In some cases, the court might use a fraud guideline,[42] while other cases might warrant a theft[43] or espionage guideline.[44] Sentencing guidelines for technology offenses, however, have been a subject of recent examination by the United States Sentencing Commission. It remains to be seen whether this examination will result in changes to the existing sentencing structure used for computer crimes.[45]

Besides the computer fraud statute, prosecutors also use generic statutes to prosecute computer crimes.[46] One finds computer-related prosecutions using statutes such as wire fraud,[47] copyright infringement,[48] illegal transportation of stolen property,[49] and

---

[38] § 1030(a)(1).

[39] § 1030(a)(3).

[40] § 1030(a)(3).

[41] § 1030(a)(7).

[42] *See* U.S. SENTENCING GUIDELINES MANUAL § 2F1.1 (2000).

[43] *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 (2000).

[44] *See* U.S. SENTENCING GUIDELINES MANUAL § 2M3.2 (2000).

[45] *See* U.S. Sentencing Comm'n, Symposium, *Federal Sentencing Policy for Economic Crimes and New Technology Offenses* (2000) [hereinafter *Federal Sentencing Symposium*], *available at* http://www.ussc.gov/2000sympo/2000sympo.htm.

[46] Glen D. Baker, *Trespassers will be Prosecuted: Computer Crimes in the 1990s*, 12 COMPUTER L.J. 61, 79-91 (1993) (discussing 18 U.S.C. § 1030 and other statutes that have been used to prosecute alleged computer crimes).

[47] 18 U.S.C. § 1343 (1994). *See, e.g.*, United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994) (dismissing alleged computer prosecution that was brought under wire fraud statute); *see also* Michael P. Dierks, *Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 325-27 (1993) (discussing how wire fraud statute has been used to prosecute computer crimes); Aaron D. Hoag, Note, *Defrauding the Wire Fraud Statute:* United States v. LaMacchia, 8 HARV. J.L. TECH. 509 (1995) (discussing how MIT student was indicted under federal wire fraud statute for operating website that allowed users to download copyrighted software free of charge).

[48] 17 U.S.C. § 506 (1994 & Supp. V 1999).

conspiracy.[50] In this regard, one might conclude that the federal approach is premised upon the computer being used as the medium for the commission of a crime.[51]

B. Fraud

Equally perplexing is the definition of fraud. Fraud is a "concept"[52] bereft with breadth. It can be conduct that is subject to punishment, the mens rea in a statute, or it can also be used in conjunction with other terms to describe conduct or activity, such as "obtains by fraud" or a "scheme or artifice to defraud." Moreover, fraud is a term that crosses into both the civil and criminal arenas.

Although the concept of fraud was initially limited to acts against the public, today the term encompasses a wide array of conduct, including conduct exclusively between two private individuals. The term fraud is interpreted differently if examined from the perspective of the Model Penal Code,[53] statistical reporting of crimes,[54] and the sentencing guidelines.[55] Although numerous substantive offenses in Title 18 use terms related to "fraud," a more limited application will be used in this Article.

For purposes of this Article, fraud will not include crimes related to espionage or terrorist activity. Despite the fact that 18 U.S.C. § 1030, the federal computer fraud statute, includes these types of activities, this Article is limited to the classic understanding of what constitutes fraud. The reason for limiting fraud will become apparent when discussing aspects of extraterritoriality.

---

[49] 18 U.S.C. § 2314 (1994 & Supp. V 1999).

[50] 18 U.S.C. § 371 (1994 & Supp. V 1999).

[51] Legislation is also pending to enlarge the existing mail fraud statute to add a misdemeanor criminalizing the "intentional sending of spam with a false or misleading return address." *Lawmakers Introduce Bill in Senate Criminalizing Sending of Unwanted Spam*, 1 Cybercrime L. Rep. (P & F) No. 1, at 7 (Apr. 9, 2001).

[52] Ellen S. Podgor, *Criminal Fraud*, 48 AM. U. L. REV. 729, 730 n.3 (1999).

[53] *Id.* at 746-47.

[54] *Id.* at 742-43.

[55] *Id.* at 743-46.

C. Criminal Computer Fraud

For purposes of this Article, computer fraud is defined similar to the definition accorded it by the Council of Europe Cyber-Crime Convention. This definition focuses on intentionally causing a loss of property in order to improperly secure economic benefits and advantages by "any input, alteration, deletion or suppression of computer data" or "any interference with the functioning of a computer or system."[56] Included within the definition is fraud related to Internet auctions,[57] telemarketing fraud,[58] intentional illegal entry into sites for economic gain, and misuse of a computer for the purpose of achieving an illegal economic advantage.[59] Excluded will be espionage that is geared toward securing a political advantage. Computer fraud can have government victims, such as when the illegal computer act involves bidding for government contracts. Computer fraud can, likewise, have victims that are private individuals and businesses.

Although computer fraud actions can be subject to both civil and criminal action, this Article is limited to the criminal sphere. With respect to civil actions, the American Bar Association (ABA) Report on

---

[56] According to Article 8 — Computer-related Fraud:

> Each Party shall adopt such legislative and other measures as criminal offenses under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:
>
> a. any input, alteration, deletion or suppression of computer data,
>
> b. any inference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Draft Convention, *supra* note 12, at Ch. II, § 1, Tit. 2, Art. 8 — Computer-related fraud.

[57] In 1988, auction fraud constituted the highest number of Internet fraud complaints. Karen Dean, *It's a Crime*, ATLANTA J. & CONST., Mar. 5, 2000, at 1H (listing top ten sources of Internet fraud complaints in 1998, as provided by National Fraud Information Center: (1) Auctions, (2) General merchandise, (3) Computer hardware/software, (4) Internet-related services, (5) Work-at-home opportunities, (6) Business opportunities/franchises, (7) Multilevel marketing, (8) Credit card issuing, (9) Advance-fee loans, (10) Job offers/overseas work).

[58] *See* U.S.-CAN. WORKING GROUP, *supra* note 12, at *Executive Summary* ("Telemarketing fraud has become one of the most pervasive forms of white-collar crime in the United States and Canada, with annual losses in both countries in the billions of dollars.").

[59] The types of fraud that are increasing in number include: "auction or retail fraud," securities fraud, "pyramid or Ponzi schemes," credit card fraud, identity theft, "business opportunity schemes." *See* Jonathan Rusch, Remarks at Breakout Session Four, Day Two, *Consumer Fraud Via the Internet*, Symposium on Federal Sentencing Policy for Economic Crimes and New Technology Offenses 290-94 (Oct. 13, 2000), *available at* http://www.ussc.gov/2000sympo/vGroupFourDayTwo.pdf.

Jurisdiction in Cyberspace Project, titled *Achieving Legal and Business Order in Cyberspace*, presents a thorough catalogue for answering jurisdiction questions that arise in the electronic commerce area.[60] The continuing project of the American Bar Association covers a multitude of jurisdiction issues that can arise in areas such as tax, intellectual property, and securities law.[61] Internet commerce, however, is not equivalent to "Internet crime."[62] The ABA Report does not speak to these criminal law issues; questions that present unique qualities in part because of the possible punishment of imprisonment, procedural issues such as extradition, and constitutional rights that are provided to defendants in criminal cases.[63] Likewise, criminal law cases do not use the traditional principles that assist in resolving jurisdiction questions that arise in civil matters.[64]

The true extent of computer fraud is hard to determine, in that some businesses may be reluctant to report the crime for fear of possible repercussions to their companies.[65] Nonetheless, it is apparent that the number of Internet related fraud offenses is not a nominal figure, and the

---

[60] A.B.A. JURISDICTION IN CYBERSPACE PROJECT, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet*, TRANSNATIONAL ISSUES IN CYBERSPACE: A PROJECT ON THE LAW RELATING TO JURISDICTION, LONDON MEETING DRAFT REPORT, *available at* http://www.abanet.org/buslaw/cyber/initiatives/draft.rtf.

[61] *See id.* (outlining ongoing issues related to Jurisdiction in Cyberspace Project).

[62] *Id.* at 9.

[63] Defendants in criminal cases have no right to choose their jurisdiction through a contract with the prosecutor. Although plea bargains may encompass an agreement on jurisdiction, the agreement comes after the activity occurs, as opposed to an agreement reached between parties prior to a particular incident, as can be secured in some civil matters. Additionally, the ABA Report predominantly speaks to enforcement of judgments, but does not speak of imprisonment. *Id.* at 90-93. The section on Data Protection, however, does refer to criminal enforcement. *Id.* at 111.

[64] *See, e.g.*, Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945); Pennoyer v. Neff, 95 U.S. 714 (1877); *see also Symposium, Jurisdiction and the Internet*, 32 INT'L LAW. 959 (1998) (discussing various issues concerning jurisdiction in cyberspace).

[65] BRANSTEN, *supra* note 12. More private-sector companies are reporting to and cooperating with the government when computer security breaches occur in their businesses. *See Cybercrime: Special Field Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Committee on the Judiciary*, 106th Cong. (Apr. 21, 2000) (statement of Guadalupe Gonzalez, Special Agent in Charge, Phoenix Field Division, Federal Bureau of Investigation) (discussing improvement in reporting by private businesses) [hereinafter Gonzalez Statement], *available at* http://www.fbi.gov/congress/congress00/gonza042100.htm; *see also Government, Private Industry Combine to Fight Internet Fraud, CLA Conference Told*, 1 Cybercrime L. Rep. (F & P) No. 4, at 3 (May 21, 2001) (reporting steps taken by DOJ, Federal Trade Commission (FTC), and eBay Inc. to identify and combat online fraud).

number appears to be increasing.[66] Recently, the Federal Bureau of Investigation targeted fraudulent schemes involving computers including, "online auction fraud, credit card fraud, bank fraud, investment fraud, multilevel marketing, and pyramid schemes."[67]

II. EXTRATERRITORIAL JURISDICTION

International crime[68] has become a growing concern in the United States.[69] Fraud is a part of the increasing amount of crime that is occurring on the international level.[70] When fraud operates internationally without computers, it is fairly easy to determine a locus for the offense. Typically, the location of the perpetrators' scheme to defraud, the location of the mailing, or the location of the telephone call becomes the venue for the prosecution. Of course, this approach does

---

[66] "[A representative of the Federal Trade Commission (FTC)] reported that in 1997 'the Commission received fewer than 1,000 Internet fraud complaints'. . . . in 2000, the FTC received 25,000 complaints related to online fraud." *New Anti-Fraud Laws Called Unnecessary*, 1 Cybercrime L. Rep. (P & F) No. 6, at 3 (June 4, 2001). This increase is mirrored in other countries. For example, Russia Interior Ministry reported that "the number of Internet -related crimes in Russia jumped to 200 for the first three months of this year 'more than all of those recorded for 1999.'" BRANSTEN, *supra* note 12; *see also* Press Release, Computer Security Institute, Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar (May 12, 2001) (reporting on Computer Security Institute's announcement of results of its 2001 Computer Crime and Security Survey, which "confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting"). Identity fraud has also significantly increased. "[T]he Federal Trade Commission currently records about 1,700 complaints and inquiries per week on identity fraud compared with 400 in March of 2000." *Treasury Department's Suspicious Activity Review Indicates Dramatic Increase in Identity Theft*, 1 Cybercrime L. Rep. (P & F) No. 7, at 3 (July 2, 2001).

[67] *FBI Cracks Down on Internet Fraud, National Investigation Nets Series of Charges*, 1 Cybercrime L. Rep. (P & F) No. 6, at 3 (June 4, 2001).

[68] "International crime" is used here in a generic sense to mean individual criminal responsibility, despite the fact that some consider that the term is limited to crimes for a state's breach of an international obligation. *See* Edward M. Wise, *International Crimes and Domestic Criminal Law*, 38 DEPAUL L. REV. 923, 928-29 (1989).

[69] International crimes involving computers have also been increasing. *See Chinese Hackers Invade 2 Official U.S. Web Sites*, N.Y. TIMES, Apr. 29, 2001, at 6; *Adobe, DMCA Foes Say Free Accused Russian eBook Hacker; U.S. Declines*, 1 Cybercrime L. Rep. (P & F) No. 9, at 3 (July 30, 2001) (discussing arrest of Russian programmer for acts occurring outside of United States); Markoff, *supra* note 26, at A1 (reporting that computer intruder believed to be from Eastern Europe); *Hackers From Abroad Obtain Data on Washington Patients*, N.Y. TIMES, Dec. 6, 2000, at A21 (reporting how Dutch man stole confidential medical records from University of Washington's medical center Web site).

[70] Press Release, Office of the Press Secretary, The White House, International Crime Control Strategy (May 12, 1998), *available at* http://www.usinfo.state.gov/topical/pol/terror/crimestr.htm.

not presume that the prosecution is limited to one specific jurisdiction. Several jurisdictions may be entitled to prosecute when the perpetrator acts in more than one place, or when the conduct involves a conspiracy with the agreement or overt acts in several different locations.

In contrast, the venue for prosecuting computer fraud may not focus exclusively on the physical location of the perpetrator. The Internet may offer a multitude of different jurisdictions as a venue for a criminal prosecution. With the Internet, there is the initial site where the activity commences. The Internet message may then pass through an array of different sites. It may proceed into a multitude of different locations, some of which may not depend upon what the initial perpetrator intended. Multiple individuals may access a page on the World Wide Web that may bring them into the realm of the criminal activity.[71] Moreover, unlike the classic criminal conduct engaged in by an individual, the victims of the fraud may be totally unknown individuals to the actual perpetrator.

Under what circumstances does the United States have jurisdiction to prosecute a perpetrator of computer crime? When the perpetrator acts within the United States and commits the initial criminal computer conduct in the United States, and the victims are likewise in the same country, there is no question that there is jurisdiction to prosecute in the United States. When the perpetrator acts within the United States, although the victims may be outside the borders, jurisdiction is also readily apparent as being in the United States. Jurisdiction, however, becomes problematic when the activity by the perpetrator occurs outside this country but substantially affects individuals within this country.

Presently, two considerations determine whether there is extraterritorial jurisdiction that permits the prosecution to occur in the United States. Courts look at the pertinent criminal statute to determine legislative intent in providing for extraterritorial application. Courts also examine the international bases of jurisdiction; here, the court focuses on whether extraterritoriality is justified under principles of territoriality, nationality, passive personality, universality, or the protective principle.[72] Note, however, that courts vary on the ordering of these two

---

[71] When the perpetrator initially acts within the United States, jurisdiction is not controversial, even if the criminal activities exceed the borders of the United States. *See* David Kocieniewski, *Man is Charged in the Creation of E-Mail Virus*, N.Y. TIMES, Apr. 3, 1999, at A1 (discussing prosecution of New Jersey individual for creation of "Melissa Virus").

[72] These five principles originate from a Harvard study. *See* RESEARCH IN INT'L LAW, FACULTY OF HARVARD LAW SCH., *introductory comment* to *Part II: Jurisdiction With Respect to Crime*, *in* CODIFICATION OF INTERNATIONAL LAW, 29 AM. J. INT'L L. 435, 445 (Supp. 1935).

considerations, with some courts looking first at the statute and congressional intent and other courts initially examining whether the conduct falls within the international bases of jurisdiction.[73]

When one examines the extraterritorial application of computer fraud crimes using this traditional approach, it is easy to secure jurisdiction in the United States. Approaching computer crimes in a technologically neutral way[74] means that any substantial effect upon the United States may provide a sufficient basis under international law for the United States to obtain jurisdiction for a prosecution. Drawing jurisdiction lines premised upon the specific conduct involved, however, can prove problematic and give rise to many questions. For example, should the United States limit extraterritorial computer prosecutions to acts involving cyberterrorism? Should juvenile hacking, auction fraud, and economic espionage be the subject of United States prosecution, even when the initial act occurs outside the borders of this country? Should it make a difference if the prosecution proceeds under the computer-fraud statute or the federal wire-fraud statute? Should it make a difference whether the computer is used as a *storage device* or as the *object* or *target* of the crime? Should it make a difference if the individual specifically targets individuals in the United States?[75] Despite the fact that many questions remain unanswered, the United States has proceeded with extraterritorial application in prosecuting computer related crimes. For example, individuals outside the United States have been indicted for crimes such as child pornography,[76] gambling,[77] copyright crimes,[78] and

---

Some scholars add additional bases in discussing prescriptive jurisdiction. *See* ALDRICH, *supra* note 14, at 31, 41-42. (adding consensual jurisdiction "based on consent of the accused's state").

[73] *See e.g.*, United States v. Velasquez-Mercaso, 697 F. Supp. 292, 294 (S.D. Tex. 1988) (looking first at congressional intent); *but see* United States v. Felix-Gutierrez, 940 F.2d 1200, 1203-06 (9th Cir. 1991) ("Prior to giving extraterritorial effect to any penal statute, we must consider whether extraterritorial application would violate international law.").

[74] *See* ELECTRONIC FRONTIER, *supra* note 6, at 4 (outlining three-part approach for addressing unlawful conduct on Internet, which includes "evaluating the need for Internet-specific regulation of unlawful conduct through a framework of general policy principles, including the principle that online and offline, conduct should be treated consistently and in a technology-neutral way").

[75] In *Yahoo!, Inc. v. La Lique Contre Le Racisme et L'Antisemitisme*, a U.S. District Court for the Northern District of California considered a reverse scenario, that is, "whether the First Amendment protects speech originating within the United States that is expressly targeted at a foreign market." Yahoo!, Inc. v. La Lique Contre Le Racisme et L'Antisemitisme, 2001 WL 1381157, at *10 (N.D. Cal. 2001).

[76] *See First-ever Life Sentence Given for Child Pornography; Multimillion Dollar Enterprise Dismantled*, 1 Cybercrime L. Rep. (P & F) No. 10, at 3 (Aug. 13, 2001) (discussing indictment of two Indonesians and one Russian).

fraud related offenses.[79]

Presently, the United States does not have a federal criminal statute that speaks to issues of extraterritoriality for criminal acts. Reconfiguring extraterritorial jurisdiction can be accomplished internally within the United States by adopting general or specific jurisdiction statutes applicable to criminal offenses. A proposed federal criminal code, discussed below, considered a general provision pertaining to extraterritorial jurisdiction. This proposal, however, did not become a part of United States federal law.

A. Statutory Recognition of Extraterritoriality

In some instances, Congress provides clear statutory language indicating that the criminal conduct at issue may be prosecuted, irrespective of whether it occurred inside or outside this country. A clear congressional indication of extraterritorial application provides an easy resolution to questions of extraterritorial jurisdiction. For example, some criminal statutes are focused specifically on extraterritorial conduct, such as the Foreign Corrupt Practices Act.[80] Other statutes include explicit provisions of extraterritoriality, such as found in one of the key money laundering statutes.[81] These statutes provide a clear indication that Congress intended for the statutes to operate extraterritorially. In some instances, Congress will place restrictions on when the statute can have an extraterritorial application. For example, prosecutors have not been successful in charging foreign officials with conspiracy to commit a violation of the Foreign Corrupt Practices Act.[82] Likewise, the money

---

[77] *See Second Circuit Upholds Conviction of Founder of Offshore Internet Gambling Operation*, 1 Cybercrime L. Rep. (P & F) No. 10, at 7 (Aug. 13, 2001) (discussing affirmation of conviction for offshore Internet gambling site in Antigua).

[78] *See Russian Programmer Accused of Writing Software to Unlock E-Books Released on Bond*, 1 Cybercrime L. Rep. (P & F) No. 10, at 8 (Aug. 13, 2001) (discussing arrest under Digital Millennium Copyright Act of Russian programmer while attending conference in United States).

[79] *Bogus FBI Company Snares Russian Hackers; Indictments Follow in Connecticut, Washington, and California*, 1 Cybercrime L. Rep. (P & F) No. 7, at 7 (July 2, 2001) (discussing federal indictment of Russians on "charges for breaking into computer systems, stealing credit card information, and attempting to extort payments from victim companies in exchange for computer security services").

[80] The Foreign Corrupt Practices Act criminalizes the bribery of foreign government officials by United States individuals and companies. *See* 15 U.S.C. §§ 78dd-1 to -3, 78ff (1994 & Supp. V 1999).

[81] *See* 18 U.S.C. § 1956 (1994 & Supp. V 1999); *see also* 18 U.S.C. § 1957 (1994) (permitting extraterritorial prosecution in certain circumstances).

[82] *See* United States v. Castle, 925 F.2d 831 (5th Cir. 1991) (holding that Congress

laundering statute has restrictions on when the extraterritorial provisions apply.[83]

Where language of extraterritoriality is absent from the statute, it becomes necessary for courts to look at congressional intent.[84] Specifically, courts attempt to discern whether Congress intended for the statute to have an extraterritorial application. Often, this inquiry can be a difficult task for courts.[85]

18 U.S.C. § 1030, the computer fraud statute, does not include an explicit extraterritorial provision that is exclusively focused on acts of fraud.[86] In recent amendments to § 1030, added as part of the "Uniting and Strengthening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" ("U.S.A. Patriot Act"), Congress added the language "including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[87] This new provision is included as part of section 814 of the Act, a section regarding "deterrence and prevention of cyberterrorism." Although the focus of

---

intended to limit the application of the Foreign Corrupt Practices Act to a "well defined group of persons"); *see also* H. Lowell Brown, *Extraterritorial Jurisdiction Under the 1988 Amendments to the Foreign Corrupt Practices Act: Does the Government's Reach Now Exceed its Grasp?*, 26 N.C. J. Int'l L. Com. Reg. 239, 292 (2001) (discussing how Congress did not amend the Foreign Corrupt Practices Act to permit prosecution of "foreign nationals" who were not "issuers" under the Act).

[83] Section 1956(f) reads:

> (f) There is extraterritorial jurisdiction over the conduct prohibited by this section if —
>
> > (1) the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and
> >
> > (2) the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.

18 U.S.C. § 1956(f) (1994).

[84] *See Ellen S. Podgor, Globalization and the Federal Prosecution of White Collar Crime*, 34 AM. CRIM. L. REV. 325, 336-40 (1997) (interpreting congressional intent to incorporate extraterritoriality into white-collar crime statutes).

[85] Lea Brilmayer aptly states, "[p]resumptions of legislative intent are something of a Frankenstein monster: Easy to create, but hard to control." Lea Brilmayer, *The Extraterritorial Application of American Law: A Methodological and Constitutional Appraisal*, 50 LAW & CONTEMP. PROBS., Summer 1987, at 11, 16.

[86] The British Misuse Act presents a contrasting approach by including specific provisions pertaining to jurisdiction. *See* Steve Shackelford, Note, *Computer-Related Crime: An International Problem in Need of an International Solution*, 27 TEX. INT'L L.J. 479, 501-04 (1992).

[87] H.R. 3162, 107th Cong. § 814(d)(1) (2001).

the U.S.A. Patriot Act was on acts of cyberterrorism, the new provision is added into a definition section of a "protected computer," a provision that can apply equally to acts of both terrorism and fraud.[88] The extent to which courts will assume that Congress has explicitly spoken with respect to computer acts involving fraud that affects the United States, remains to be seen.

When the prosecution proceeds under § 1030, it is restricted to the seven specific activities that are expressed in the statute.[89] A wider range of fraudulent conduct can be the subject of a criminal prosecution if prosecutors use 18 U.S.C. § 1343, the federal wire fraud statute.[90] Section 1343 does not offer a definitive resolution of whether extraterritorial application will be permitted.[91] Therefore, it becomes necessary for the judiciary to ascertain whether Congress intended for prosecutors to use the statute for conduct occurring outside the United States. Other statutes also criminalize acts committed with a computer, and these statutes can also require judicial inquiry into whether extraterritorial application should be permitted.[92]

The classic judicial approach to extraterritorial criminal application is found in the Supreme Court case of *United States v. Bowman*,[93] where the Court stressed the importance of determining congressional intent in the absence of express statutory language. In *Bowman*, the Court held that there is a presumption against extraterritorial application when the crime was "against private individuals or their property."[94] If, however,

---

[88] 18 U.S.C. 1030(a)(4) (1994 & Supp. V 1999).

[89] *See* ELLEN S. PODGOR & JEROLD H. ISRAEL, WHITE COLLAR CRIME IN A NUTSHELL, 237-41 (2d ed. 1997).

[90] The breadth of the wire fraud statute permits the prosecution of any "scheme or artifice to defraud" that involves an interstate or foreign transmission "by means of wire, radio, or television communication." 18 U.S.C. § 1343 (1994 & Supp. V 1999). *See also* PODGOR & ISRAEL, *supra* at note 89, at 71-72.

[91] *See* United States v. Boots, 80 F.3d 580, 587-88 (1st Cir. 1996) (holding that U.S. wire fraud could not be used to prosecute scheme to defraud foreign government of tax revenue); *but see* United States v. Trapilo, 130 F.3d 547, 552 (2d Cir. 1997) (holding that U.S. wire fraud statute could be used in prosecuting scheme to defraud foreign government of tax revenue).

[92] *See* Baker, *supra* note 46, at 79-91. *See also* Marc S. Friedman & Camille Otero-Phillips, *Internet Crime and Abuse: Latest Developments*, 6 E-COM. L. REP. 2 (1999) (discussing different federal statutes that can be used to prosecute computer-related crimes).

[93] 260 U.S. 94 (1922).

[94] The Court in *Bowman* explained:

> Crimes against private individuals or their property, like assaults, murder, burglary, larceny, robbery, arson, embezzlement, and frauds of all kinds, which affect the peace and good order of the community, must, of course, be committed within the territorial jurisdiction of the government where it may properly

the crime was "not logically dependent on the[] locality for the government's jurisdiction," then an extraterritorial application might be permitted.[95] Today, courts have moved further from the restrictions and presumptions set forth in *Bowman*.[96] Generally, courts permit extraterritorial jurisdiction in criminal cases if the criminal conduct affected or was intended to affect individuals in the United States.

B. *International Bases*

Where some courts stress the importance of statutory interpretation, other courts focus on international law and whether extraterritoriality should be permitted under the consensual rules of international law. International law focuses on three forms of jurisdiction: jurisdiction to prescribe, adjudicate, and enforce.[97] In the United States, the ability to

---

exercise it. If punishment of them is to be extended to include those committed outside [sic] of the strict territorial jurisdiction, it is natural for Congress to say so in the statute, and failure to do so will negate the purpose of Congress in this regard.

Id. at 98.

[95] The *Bowman* Court again explained:

> But the same interpretation should not be applied to criminal statutes which are, as a class, not logically dependent on their locality for the government's jurisdiction, but are enacted because of the right of the government to defend itself against obstruction, or fraud wherever perpetrated, especially if committed by its own citizens, officers, or agents. Some such offenses can only be committed within the territorial jurisdiction diction of the government because of the local acts required to constitute them. Others are such that to limit their locus to the strictly territorial jurisdiction would be greatly to curtail the scope and usefulness of the statute and leave open a large immunity for frauds as easily committed by citizens on the high seas and in foreign countries as at home.

Id.

[96] *See, e.g.*, United States v. Pizzarusso, 388 F.2d 8 (2d Cir. 1968) (holding that United States District Court had jurisdiction to indict and convict non-U.S. citizen for false statements made on visa application submitted to consular official working outside United States).

[97] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 401 (1987):

> § 401 Categories of Jurisdiction:
>
> Under international law, a state is subject to limitations on: (a) jurisdiction to prescribe, *i.e.*, to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things, whether by legislation, by executive act or order, by administrative rule or regulation, or by determination of a court; (b) jurisdiction to adjudicate, *i.e.*, to subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the state is a party to the proceedings; (c) jurisdiction to enforce,

adjudicate and enforce is dependent upon first acquiring jurisdiction to prescribe via legislative, executive, judicial, or administrative rule, ruling, or regulation. While jurisdiction to prescribe is normally reflected by examining the relation of the crime, victims, or perpetrator to the country seeking jurisdiction, cyberspace presents new considerations for making the determination of the appropriate place of jurisdiction.[98] These new considerations result in part because the ease of securing an international base of jurisdiction is multiplied in the world of cyberspace.

1. Jurisdictional Bases

The five most common bases for finding international jurisdiction to prescribe are premised upon principles of territoriality, nationality, passive personality, protective principle, or universality.[99] In some cases more than one jurisdictional base is used by a court to approve the prosecution of extraterritorial conduct.[100] These jurisdictional bases are

---

i.e., to induce or compel compliance or to punish noncompliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other nonjudicial action.

[98] Denis T. Rice, *Jurisdiction in Cyberspace: Which Law and Forum Applies to Securities Transactions on the Internet?*, 21 U. PA. J. INT'L ECON. L. 585, 595-96 (2000) ("[J]urisdictional principles are difficult to apply to the Internet, which is a largely boundless medium.")

[99] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 (1987):

§ 402 Bases of Jurisdiction to Prescribe:

Subject to § 403, a state has jurisdiction to prescribe law with respect to:

(1) (a) conduct that, wholly or in substantial part, takes place within its territory;

(b) the status of persons, or interests in things, present within its territory;

(c) conduct outside its territory that has or is intended to have substantial effect within its territory;

(2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and

(3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.

[100] *See, e.g.*, Chua Han Mow v. United States, 730 F.2d 1308, 1311-13 (9th Cir. 1984) (applying both objective territorial and protective principles to establish jurisdiction); United States v. Roberts, 1 F. Supp.2d 601, 607 (E.D. La. 1998) (applying both objective territorial and passive personality principles to establish jurisdiction).

not unique to criminal law, applying equally to cyberspace jurisdiction questions that arise in the civil sphere.[101]

The most common base of jurisdiction used by U.S. courts is territorial jurisdiction, jurisdiction premised upon the locus of the crime. Obviously, the United States has territorial jurisdiction over a perpetrator when the criminal act occurs in this country. Territorial jurisdiction does not raise controversial issues with respect to jurisdiction, except to the extent that this type of jurisdiction is too limited. Attorney Gary Born, in demonstrating the obsolete nature of using a territorial principle, argues for a new approach, one in which "courts could presume that Congress has extended federal law to the limits prescribed by the principles of international law currently prevailing in the United States."[102]

Over time, territorial jurisdiction has expanded to include not only acts within the locus, but also acts that are an extension of the locus.[103] This approach, called the objective territorial principle, has been endorsed wholeheartedly in the United States.[104] Where the strict territorial approach referred to acts committed within the jurisdiction, the objective territorial approach included acts that affected those within the jurisdiction, although committed extraterritorially.

In *Strassheim v. Daily*,[105] the Supreme Court described the objective territorial principle as "[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it."[106] The objective territorial principle is a common base of extraterritorial jurisdiction in the

---

[101] Wilske & Schiller, *supra* note 10, at 117 (discussing jurisdictional issues involved in state regulation of cyberspace).

[102] Gary B. Born, *A Reappraisal of the Extraterritorial Reach of U.S. Law*, 24 LAW & POL'Y INT'L BUS. 1, 82 (1992).

[103] *See id.* at 21-29 (discussing erosion of territorial presumption).

[104] Historical literature also supports a territorial approach that includes acts both within the territory and that affect the territory. In 1906, Professor John Bassett Moore wrote that, "The principle that a man who outside of a country willfully puts in motion a force to take effect in it is answerable at the place where the evil is done, is recognized in the criminal jurisprudence of all countries." JOHN BASSETT MOORE, 2 A DIGEST OF INTERNATIONAL LAW 244 (1906); *see also* Born, *supra* note 102, at 22. The extension of the territorial principle to include effects on the territory is not exclusive to the United States. *See* The Case of the S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J., (ser. A), No. 10 (extending territorial jurisdiction to include its effects).

[105] 221 U.S. 280 (1911).

[106] *Id.* at 285. Subjective territoriality differs in that it "aims to assign jurisdiction to the courts of a state with respect to offenses with a constituting element that occurred in that state's territory." Pierre Trudel, *Jurisdiction Over the Internet: A Canadian Perspective*, 32 INT'L LAW. 1027, 1036 (1998).

United States,[107] with courts often permitting United States drug prosecutions for conduct that occurs outside this country when the conduct could have a detrimental effect in this country.[108] The mere intent to commit an act in the United States has been sufficient for a finding of extraterritorial application premised upon an objective territorial principle.[109]

The nationality principle is premised upon the nationality of the perpetrator. The United States seldom uses this principle to justify an extraterritorial application.[110] An example of the United States applying this principle to secure extraterritorial jurisdiction is found in a case when the perpetrator, a United States citizen, is accused of making false statements on a Customs Declaration form. Despite the fact that the act occurred outside the United States, the prosecution could establish extraterritoriality based upon the nationality of the accused.[111] This principle is also used when a United States citizen commits a United States tax offense while living outside this country.

Jurisdiction based on the nationality of the victim is the essence of the passive personality principle.[112] Because this principle allows the United States to assume jurisdiction over an individual in another country merely because the victim of the crime is a United States citizen, it has been criticized for the "intrusion on sovereignty" of another state.[113]

Jurisdiction can also be premised upon a protective principle, "which permits a nation to assert jurisdiction over a person whose conduct outside the nation's territory threatens the nation's security or could

---

[107] This principle is *also* recognized worldwide. *See id.* at 1035-36.

[108] *See, e.g.*, Chua Han Mow v. United States, 730 F.2d 1308, 1311-13 (9th Cir. 1984) (using objective territorial principle and protective principle as basis for United States prosecution of extraterritorial narcotics offenses); United States v. King, 552 F.2d 833 (9th Cir. 1976) (holding that prosecution in United States for distribution of heroin that occurred in Japan is constitutional). The "effects test" is not limited to cases that are drug-related. *See* Michael J. Calhoun, Comment, *Tension on the High Seas of Transnational Securities Fraud: Broadening the Scope of United States Jurisdiction*, 30 LOY. U. CHI. L.J. 679 (1999) (discussing use of "effects test" in cases of securities fraud).

[109] United States v. Ricardo, 619 F.2d 1124, 1129 (5th Cir. 1980).

[110] *See* Geoffrey R. Watson, *Offenders Abroad: The Case for Nationality-Based Criminal Jurisdiction*, 17 YALE J. INT'L L. 41, 83 (1992) (concluding that United States should not reject use of nationality principle to acquire extraterritorial jurisdiction).

[111] United States v. Walczak, 783 F.2d 852, 854 (9th Cir. 1986).

[112] *See* United States v. Roberts, 1 F. Supp. 2d 601 (E.D. La. 1998) (applying passive personality principle for charges of sexual abuse of minor where victim was U.S. citizen and act was alleged to occur on board cruise ship).

[113] *See* Geoffrey R. Watson, *The Passive Personality Principle*, 28 TEX. INT'L L.J. 1, 14-18 (1993) (discussing arguments used to oppose use of passive personality principle).

potentially interfere with the operation of its governmental functions."[114] Terrorism targeted against the defense department is an example of criminal activity that falls under this principle.

Finally, matters of human rights often find extraterritorial jurisdiction premised on the universality principle, a principle that permits prosecution of "certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism."[115]

2. A Limit on Jurisdictional Bases

A limitation that is placed upon jurisdiction to prescribe is that of reasonableness.[116] The Restatement (Third) of Foreign Relations Law §

---

[114] United States v. Gonzalez, 776 F.2d 931, 938 (11th Cir. 1985).

[115] United States v. Yunis, 924 F.2d 1086, 1091 (D.C. Cir. 1991); *see also* Kenneth C. Randall, *Universal Jurisdiction Under International Law*, 66 TEX. L. REV. 785, 790-91 (1988)(arguing that states have right to assume universal jurisdiction over crimes listed in coventions).

[116] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403 (1987):

> § 403 Limitations on Jurisdiction to Prescribe:
>
> (1) Even when one of the bases for jurisdiction under § 402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable.
>
> (2) Whether exercise of jurisdiction over a person or activity is unreasonable is determined by evaluating all relevant factors, including where appropriate:
>
> (a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;
>
> (b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect;
>
> (c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is *generally* accepted;
>
> (d) the existence of justified expectations that might be protected or hurt by the regulation;
>
> (e) the importance of the regulation to the international political, legal, or economic system;

403 lists a host of factors that can be considered in assessing the reasonableness of the jurisdiction to prescribe.[117] For example, the "link between the activity and the territory of the regulating state" needs to be considered in determining whether the jurisdiction is reasonable.[118] Reasonableness is important to assure comity, the reciprocal respect for another countries laws.[119]

Despite the importance, however, of the reasonableness standard, it seldom serves to preclude a prosecution of drug activity occurring abroad.[120] In *Hartford Fire Insurance Co. v. California*,[121] the Supreme Court placed comity concerns as a consideration only if the court determined that the statute did not cover the specific conduct.[122] Constitutional restraints also have not precluded findings of extraterritoriality in criminal cases.[123] Since the computer act is unlikely to be the result of a

---

(f) the extent to which the regulation is consistent with the traditions of the international system;

(g) the extent to which another state may have an interest in regulating the activity; and

(h) the likelihood of conflict with regulation by another state.

(3) When it would not be unreasonable for each of two states to exercise jurisdiction over a person or activity, but the prescriptions by the two states are in conflict, each state has an obligation to evaluate its own as well as the other state's interest in exercising jurisdiction, in light of all the relevant factors, in Subsection (2); a state should defer to the other state if that state's interest is clearly greater.

[117] *Id.*

[118] *Id.* at § 403(2)(a).

[119] *Id.* at § 403(3).

[120] There is a special approach to determining reasonableness when the case involves drug activity. *See, e.g., In re* Grand Jury Proceedings (Marsoner), 40 F.3d 959, 966 (9th Cir. 1994) (allowing United States interests to outweigh Austrian interests); United States v. Noriega, 746 F. Supp. 1506, 1515 (S.D. Fla. 1990) ("In assessing the reasonableness of extraterritorial jurisdiction, one of the factors to be considered is 'the character of the activity to be regulated, including the importance of regulation to the regulating state and the degree to which the desire to regulate is *generally* accepted'." (quoting RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403(1)(c) (1987))). *But see* United States v. Javino, 960 F.2d 1137 (2d Cir. 1992) (finding it unreasonable to apply firearms statute to manufacturers unless firearm is imported into United States); Boureslan v. Aramco, 857 F.2d 1014, 1025 n.10 (5th Cir. 1988) (King, J., dissenting) ("No court has applied the reasonableness test as part of the threshold inquiry to determine whether a statute may, as a general matter, be applied extraterritorially.").

[121] 509 U.S. 764 (1993).

[122] *Id.* at 797 n.24. (disagreeing with Justice Scalia's dissent that comity should factor into determination whether Sherman Act applies to extraterritorial conduct).

[123] 1 NAT'L COMM'N ON REFORM OF FED. CRIMINAL LAWS, WORKING PAPERS 70 (1970)

legislative or executive act of another country, the "act of state doctrine" will not serve to limit extraterritoriality in the case of a computer crime.[124]

3. Criminal Jurisdiction in Cyberspace

Applying these jurisdictional bases to cyberspace produces a result that one does not find when these jurisdictional bases are used with other substantive crimes. Most notable in this regard is the fact that a single computer offense, even one prosecuted under the specific computer fraud statute found in 18 U.S.C. § 1030, can be premised on a variety of different jurisdictional bases.[125] Where the computer conduct involves terrorism, the protective and universal principles might apply. When an individual is filing a false United States government form via computer, and that individual is outside the United States, nationality may be the appropriate base for jurisdiction. Likewise, when a United States citizen deliberately engages in criminal conduct beyond the borders of this country in order to circumvent jurisdictional principles, application of a nationality principle may be warranted.

Examining the jurisdictional bases as applied to computer conduct provides a strong argument for using a "technologically neutral" approach to the prosecution of computer crime. Seeing computers as merely the means for the commission of the criminal conduct appears warranted given the array of jurisdictional bases that might apply to computer related conduct. Focusing on the conduct, as opposed to the means in which the conduct is effectuated, would appear at first blush to provide a fair and neutral method of determining whether there is jurisdiction to prosecute in the United States.

[hereinafter REFORM WORKING PAPERS]; *see also* Michael D. Ramsey, *Escaping "International Comity"*, 83 IOWA L. REV. 893 (1998) (discussing extraterritorial legislation).

[124] *Id.* at 914-17 (discussing "act of state" doctrine). The act-of-state doctrine is a "common law principle that prevents U.S. courts from questioning the validity of a foreign country's sovereign acts within its own territory." BLACKS LAW DICTIONARY 35 (7th ed. 1999).

[125] A section of the computer fraud statute speaks to trafficking that "affects interstate or foreign commerce." 18 U.S.C. § 1030(a)(6). This, however, is an element of the offense necessary for a prosecution, as opposed to being a basis for proceeding with a prosecution of conduct outside the United States. For example, the wire fraud statute requires as an element of the offense that the communication be "in interstate or foreign commerce." 18 U.S.C. § 1343. Such a requirement, however, does not mean that this section automatically authorizes every extraterritorial application. *See* United States v. Boots, 80 F.3d 580 (1st Cir. 1996) (refusing to allow wire fraud convictions where object of scheme was to defraud foreign government).

There is, however, a basic flaw in this analysis. To find jurisdiction applicable based upon the conduct, irrespective of the use of a computer to effectuate that conduct, disregards the unique nature of the means for committing the crime.

4. Jurisdiction for Computer Fraud Prosecutions

Using computer fraud as an example, a computer fraud committed by someone outside the United States could easily come under the objective territoriality, nationality, passive personality, and protective principles. The ease with which computer fraud acts outside the United States could be prosecuted within this country is in large part because the medium, the computer, has the ability to operate on a global network. It is possible that the individual committing the act deliberately targeted United States individuals, businesses, or the government. It can also be the case that the perpetrator of the fraud had no knowledge of who would be the recipients of his or her fraud. The individual committing the act might have no intent to perpetrate an auction fraud on individuals in the United States, but by placing the item for sale on the web, he or she allows for individuals throughout the world to access that information and thus be victims of the fraud.

Any computer act occurring outside the United States, where victims of the crime are in the United States, may conceivably become subject to United States prosecution under an objective territorial principle. Because of the global nature of the medium, the objective territorial doctrine could possibly be met by any act that might have a substantial effect in this country. Unlike similar crimes that are premised upon the means for committing the act, such as mail and wire fraud, the jurisdiction for prosecuting a computer offense can easily be obtained in the United States. Where the mails and wires are likely to have a set number of participants in the activity, computers can have a limitless number of individuals who can be victimized by the crime. Also, unlike the mails and wires, the location where the perpetrator acts may be masked by multiple links that may proceed through several countries prior to a message being received by the victims. In the case of computer fraud, if existing principles are adhered to, it would be rare to exclude an extraterritorial prosecution as having an insufficient base for jurisdiction, if individuals, the government, or businesses in the United States are injured by the conduct of the perpetrator.[126]

---

[126] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 cmt. d (1987):

Requiring an intent to harm individuals in the United States might not limit the United States' acquisition of jurisdiction to prosecute computer crimes that are committed outside its borders.[127] Because of the global nature of cyberspace, intent could easily be inferred by the very fact that the individual placed the item onto the Internet. A defendant could hardly argue that they did not intend individuals from a certain country to retrieve the message when the Internet by its very nature has global possibilities. Additionally, issues of jurisdiction are rarely afforded a mens rea requirement. The mere fact that the jurisdiction element is satisfied and proof is present in court may be sufficient to meet the venue and jurisdiction requirements of a statute.[128]

Obviously, U.S. prosecutors will not choose to prosecute all computer fraud offenses that occur in the international arena. For example, the United States did not prosecute the individual alleged to be responsible for the "I Love You" worm, despite damages in the billions.[129] Discretion, a significant part of prosecutorial power can play a factor in limiting the number of cases brought in this country. Resources can also play a significant role, in that police, prosecutors, and judges do not have

---

> (d) Effects principle. Jurisdiction with respect to activity outside the state, but having or intended to have substantial effect within the state's territory, is an aspect of jurisdiction based on territoriality, although it is sometimes viewed as a distinct category. The effects principle is not controversial with respect to acts such as shooting or even sending libelous publications across a boundary. It is generally accepted with respect to liability for injury in the state from products made outside the state and introduced into its stream of commerce. Controversy has arisen as a result of economic regulation by the United States and others, particularly through competition laws, on the basis of economic effect in their territory, when the conduct was lawful where carried out. This Restatement takes the position that a state may exercise jurisdiction based on effects in the state, when the effect or intended effect is substantial and the exercise of jurisdiction is reasonable under § 403. . . .

[127] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 cmt. d (1987):

> . . . Cases involving intended but unrealized effect are rare, but international law does not preclude jurisdiction in such instances, subject to the principle of reasonableness. When the intent to commit the proscribed act is clear and demonstrated by some activity, and the effect to be produced by the activity is substantial and foreseeable, the fact that a plan or conspiracy was thwarted does not deprive the target state of jurisdiction to make its law applicable.

[128] *See, e.g.*, United States v. Bryant, 766 F.2d 370 (8th Cir. 1985) (finding that defendant does not have to know whether wire transmission went interstate as long as it actually did proceed interstate).

[129] *See* Jovi Tanada Yam, *Cybercrime Treaty Under Way*, BUSINESSWORLD (Manila), May 3, 2001, at 9, *available at* 2001 WL 17164125.

unlimited money and time to permit the prosecution of all crimes that might meet the applicable criminal and jurisdiction requirements of law.[130]

Discretion, however, permits prosecutors to pick and choose those offenses upon which they wish to proceed. Doctrines of fairness and equity can be seriously undermined when the entire realm of computer fraud offenses can be prosecuted, but prosecutors choose only a small slice of the actions to proceed against.[131] This problem is particularly noteworthy when the prosecution is against individuals outside the United States, who may not be accustomed to a similar discretionary process in the charging of individuals for commission of crimes.

If one contrasts the use of international bases of jurisdiction in computer fraud with the applications in another form of criminal activity, such as the sale of drugs, the unique nature of computerization is apparent. If someone sells drugs outside the United States with the purpose of allowing the drugs to eventually be sold in this country, the drug seller may not know the specific person who will receive the drugs. Nevertheless, the individual clearly has the intent to sell drugs in the United States and therefore meets the objective territorial principle for the effect that the conduct has in this country. In contrast, computers may not be targeted to a single country or to specific individuals within a country. The very global nature of the means used in distributing the criminal act places no limits on the territories in which the conduct can be accessed, except to the extent a country limits incoming web sites or people in the country lack the technology to access the fraudulent conduct. A claim of "unreasonableness" in acquiring jurisdiction in the United States stands little chance of success because the computer act clearly can have a "substantial, direct, and foreseeable effect upon or in

---

[130] The Reporter's Notes to § 403 of the Restatement confirm that:

> Prosecutions for activities committed in a foreign state have *generally* been limited to serious and universally condemned offenses, such as treason or traffic in narcotics, and to offenses by or against military forces. In such cases the state in whose territory the act occurs is not likely to object to regulation by the state concerned.

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403 n.8. In recent years, however, the United States has used its extraterritorial powers in prosecutions outside the realm of these categories. *See, e.g.*, United States v. Nippon Paper Indus. Co., Ltd., 109 F.3d 1 (1st Cir. 1997) (discussing prosecution of corporation for antitrust violation where activities occurred outside United States but had substantial effects in this country).

[131] Ellen S. Podgor, *The Ethics and Professionalism of Prosecutors in Discretionary Decisions*, 68 FORDHAM L. REV. 1511 (2000).

the territory" of the United States.[132]

C. A Proposed Federal Approach

Although Congress has addressed extraterritoriality in some federal statutes,[133] there is no general extraterritorial jurisdiction provision in the federal criminal code.[134] In 1970, however, the National Commission on Reform of Federal Criminal Law considered just such a provision.[135] In considering a possible general approach to extraterritoriality, the National Commission on Reform of Federal Criminal Law provided a model statute that premised extraterritorial jurisdiction upon a list of conduct included within the statute.[136] For example, presidential

---

[132] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403(2)(a) (1987).

[133] *See supra* notes 80-83 and accompanying text.

[134] *See* REFORM WORKING PAPERS, *supra* note 123, at 71 (1970).

[135] *Id.* at 69-76.

[136] NAT'L COMM'N ON REFORM OF FED. CRIMINAL LAW, FINAL REPORT § 208 (1971):

§ 208 Extraterritorial Jurisdiction.

Except as otherwise provided by statute or treaty, extraterritorial jurisdiction over an offense exists when:

(a) on the following is a victim or intended victim of a crime or violence: the President of the United States, the President-elect, the Vice-President, or, if there is no Vice-President, the officer next in the order of succession to the office of President of the United States, the Vice-President-elect, or any individual who is acting as President under the Constitution and laws of the United States, a candidate for President or Vice-President or any member or member designate of the President's cabinet, or a member of Congress, or a federal judge;

(b) the offense is treason, or is espionage or sabotage by a national of the United States;

(c) the offense consists of a forgery or counterfeiting, or an uttering of forged copies or counterfeits, of the seals, currency, instruments of credit, stamps, passports, or public documents issued by the United States; or perjury or a false statement in an official proceeding of the United States; or a false statement in a matter within the jurisdiction of the government of the United States; or other fraud against the United States, or a theft of property in which the United States has an interest, or, if committed by a national or resident of the United States, any other obstruction of or interference with United States government function;

(d) the accused participates outside the United States in a federal offense committed in whole or in part within the United States, or the offense constitutes an attempt, solicitation, or conspiracy to commit a federal offense within the United States;

assassination would be subject to United States prosecution, irrespective of whether the act occurred inside or outside the United States, and irrespective of whether the individual committing the crime was a United States citizen or alien.[137]

A general jurisdiction statute that is conduct-related could prove effective in limiting jurisdiction to specific activities. Since computer criminality touches many types of conduct, such as terrorism, espionage fraud, and theft, the computer would in essence be used as a means for committing traditional crimes. When the traditional crimes are specifically listed, and computer use to commit the crime is accounted for in the wording of the statute, jurisdiction is not limitless. The proposed statute of the National Commission on Reform of Federal Criminal Law provided significant limits to the circumstances in which prosecutors might proceed extraterritorially.[138]

If, however, the general jurisdiction provision were to mirror the objective territorial principle in international law, thus placing computers in a neutral setting with offenses that are not related to technology, there would be few limits to what could be prosecuted in the United States. A general provision of extraterritoriality based merely upon whether the conduct affects individuals within the United States would allow prosecutors to proceed whenever there were victims in this country of the computer fraud.

(e) the offense is a federal offense involving entry of persons or property into the United States;

(f) the offense is committed by a federal public servant who is outside the territory of the United States because of his official duties or by a member of his household residing abroad or by a person accompanying the military forces of the United States;

(g) such jurisdiction is provided by treaty; or

(h) the offense is committed by or against a national of the United States outside the jurisdiction of any nation.

See also REFORM WORKING PAPERS, *supra* note 123, at 69-76; Kenneth R. Feinberg, *Extraterritorial Jurisdiction and the Proposed Federal Criminal Code*, 72 J. CRIM. L. & CRIM. 385 (1981) (noting that then-proposed federal criminal code codified existing case law).

[137] *See* REFORM WORKING PAPERS, *supra* note 123, at 74.

[138] *Id.*

III. INTERNATIONAL INITIATIVES AND PERSPECTIVES

There have been several groups and conferences focused on tackling cybercrime through international cooperation.[139] Although one might expect universal acceptance of all of these initiatives, scholars have noted some significant deficiencies in some of these proposals.[140] This section critically examines three perspectives on jurisdiction over cybercrime.

First, international proposals such as the recent Council of Europe Draft Convention on Cybercrime provide a global approach to fighting computer crimes.[141] Although the Council of Europe Draft Convention on Cybercrime suggests ways to approach conflicts that might arise between countries that are deciding which country will prosecute a computer crime, this proposal does not limit existing ways for the United States to secure extraterritorial jurisdiction. Another report, coming out of a conference held at Stanford University, suggests modifications to the Council of Europe Draft Convention on Cybercrime and provides a more detailed approach to extraterritorial jurisdiction. Finally, using concepts from the law of international space also suggests a way for handling issues of jurisdiction with respect to computer crimes.

A. Council of Europe Draft Convention on Cybercrime

After an extensive study of cybercrime that included reviewing and revising multiple drafts of a treaty, the Council of Europe Draft Convention on Cybercrime publicly aired its conclusions. Non-member nations, such as Canada, the United States, and Japan, participated in

---

[139] *See supra* note 12; *see also* Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM(2000)890 final at 7-9 (discussing variety of international discussions and proposals on cybercrime), *available at* http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComm/EN.html. There are also international discussions relating to considerations for an "international standard instrument" for cyberspace. *See, e.g.*, THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW (UNESCO, Law of Cyberspace Series Vol. 1, 2000) (examining issues related to UNESCO-prepared articles on development of a possible international structure for cyberspace).

[140] *See generally* ALDRICH, *supra* note 14 (examining efforts of European countries, United States, and Japan to create international computer crime standards).

[141] There have been many other international bodies that have been examining cybercrime issues. *See generally* Michael A. Sussman, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium*, 9 DUKE J. COMP. & INT'L L. 451, 476-88 (1999) (discussing multi-lateral organizations that have examined computer crime issues).

many of the negotiations on this treaty.[142] Although the draft treaty provides a section outlining how international cybercrime jurisdiction questions ought to be resolved, the treaty provides few limitations to existing principles governing United States extraterritorial jurisdiction. Should this treaty become a reality, and should the United States become a party to this treaty,[143] the United States would still have the option to proceed with a prosecution if national law permitted the action. The treaty does offer the possibility that an increased number of countries will add substantive and procedural provisions to combat computer fraud related offenses, thus making it unnecessary for the United States to intervene in the prosecution of these crimes. Many countries have already moved toward the adoption of criminal laws that focus on computer crimes.[144]

Jurisdiction under the proposed treaty includes four categories: "in its territory," "on board a ship flying the flag," "on board an aircraft registered under the laws of that Party," or "by one of it nationals if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."[145] Countries, however, are not bound to accept these possible

---

[142] Press Release, Council of Europe, First Draft of International Convention Released for Public Discussion (Apr. 27, 2000), *available* at http://www.usdoj.gov/criminal/cybercrime/coepress.htm.

[143] U.S. businesses have expressed concerns over this treaty. *See U.S. Business Interests, Rights Groups Still Dislike Internet Crime Treaty*, 1 Cybercrime L. Rep. (P & F) No. 6, at 14 (June 4, 2001) (discussing three major concerns that businesses were expressing with regard to this treaty).

[144] *See generally* Chief Judge Stein Schjolberg, *The Legal Framework - Unauthorized Access to Computer Systems, Penal Legislation in 41 Countries* (outlining international developments in computer-crime legislation and providing excerpts of such legislation currently in force in 41 countries), *available at* http://www.mossbyrett.of.no.info/legal.html (last modified Oct. 1, 2001).

[145] Draft Convention, *supra* note 12, at §3, art. 22.

> Article 22 — Jurisdiction:
>
> (1) Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offense established in accordance with Articles 2 – 11 of this Convention, when the offence is committed:
>
> (a) in its territory; or
>
> (b) on board a ship flying the flag of that Party; or
>
> (c) on board an aircraft registered under the laws of that Party; or
>
> (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial

ways to attain jurisdiction. Thus, countries like the United States that seldom premises jurisdiction upon a nationality principle[146] could easily ignore nationality as a base for acquiring jurisdiction. Significantly, the draft treaty "does not exclude any criminal jurisdiction exercised in accordance with domestic law."[147] Although the treaty provides for the resolution of conflicts between jurisdictions when multiple countries have jurisdiction, it offers no constraints upon countries that might have a legitimate basis for proceeding under their domestic law.[148] The net result is that the United States could easily proceed with a prosecution in cases where the computer fraud significantly affects individuals in this country. Thus, computer crimes occurring outside the United States may nonetheless be subject to criminal prosecution by this country if the crimes meet an objective territorial principle of jurisdiction and there is no explicit language in the statute precluding an extraterritorial application.

B. The Stanford Conference

The Council of Europe treaty is not the only international consideration on how best to combat international computer crime. Jointly sponsored by the Hoover Institution, The Consortium for

---

jurisdiction of any State.

(2) Each State may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof.

(3) Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.

(4) This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.

(5) When more than one Party claims jurisdiction over an alleged offense established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Id.

[146] *See* Watson, *supra* note 110, and accompanying text.

[147] Draft Convention, *supra* note 12, at art. 22.

[148] *Id.*

Research on Information Security & Policy (CRISP) and the Center for International Security and Cooperation (CISAC), a report titled "*A Proposal for an International Convention on Cybercrime and Terrorism*" was released in August 2000. This report is also referred to as the "Stanford Draft International Convention to Enhance Security from Cybercrime and Terrorism" (Stanford Draft).[149] The Stanford Draft calls for a multilateral convention and states that "it builds upon the draft Convention on Cybercrime proposed by the Council of Europe."[150] Like the Council of Europe Report, it defines offenses and stresses international cooperation in both the investigation and prosecution of computer crimes. Unlike the Council of Europe treaty, however, the Stanford Draft provides an explicit ordering of jurisdiction when conflicts arise between countries.[151] Thus, the draft allows for prosecution at the locus of the initial activity, as well as objective territorial jurisdiction when the activity has a substantial effect on those asserting jurisdiction within the country.

The Stanford Draft specifically comments on international fraud, noting the array of potential places for jurisdiction.[152] This draft report states that nations have asserted jurisdiction of transnational fraud "on the basis of any significant connection to the conduct involved."[153] Since cybercrime can easily involve multiple jurisdictions, the draft report takes the position that enforcement here should "be limited to cybercrimes that are universally condemned."[154] The mere accessing of a web site, for example, would probably not confer jurisdiction under this proposal.[155]

---

[149] *See* Abraham D. Sofaer et al., *A Proposal for an International Convention on Cyber Crime and Terrorism* (Aug. 2000), *available at* http://www.oas.org/juridico/english/monograph.htm. This Report was an outgrowth of a December 1999 conference held at Stanford University. *Id.* at Executive Summary.

[150] *Id.*

[151] *Id.* at art. 5, § 4.

[152] According to the commentary on the draft convention:

> Among these are the States where a fraud was planned, where an effort to defraud was initiated, where individuals worked at implementing the fraud, where or through which communications were made that were intrinsic to the fraud, where the victims were located, and where the fraud had material and intended effects.

Id. at Commentary on the Draft Convention, 2. Jurisdiction.

[153] *Id.*

[154] *Id.*

[155] *Id.*

The specific ordering of which country would have priority in prosecuting differentiates this Report from the Council of Europe Treaty. The Stanford Draft lists the jurisdiction priorities as follows: (1) the location where the alleged act was committed, (2) the place of substantial harm, (3) nationality, (4) where the alleged offender is found, and (5) any place with a "reasonable basis for jurisdiction."[156] If this proposal is accepted, it could alleviate some of the concerns that are expressed in this Article. Specifically, an express list of jurisdictional priorities would assist in restraining a prosecutor's discretion in deciding whether to proceed with crimes that involve extraterritorial conduct.

C. *International Space Jurisdiction*

Attorney Darrel Menthe has suggested that perhaps cyberspace should be analogized to jurisdiction in international space.[157] Under this approach, the nationality of the perpetrator, as opposed to territoriality, is the key component for determining jurisdiction in "outer space, Antarctica, and the high seas."[158] Numerous problems, however, can arise if this approach is applied to computer fraud crimes. For example, would the United States be willing to forego criminal prosecution when the act occurred within its territory, but was committed by an individual who was not a United States citizen? If both the United States and the country to which the perpetrator was a national wanted to proceed with a criminal prosecution, who would have priority? Is it practical to proceed with a prosecution in another country when the initial act occurs in the United States, the perpetrator is located within this country, and all the evidence is located here?

These questions emphasize the differences between international space and cyberspace. Where international space generally has no links to any particular country, justifying the use of a nationality approach, cyberspace can offer some distinct ties to a jurisdiction.[159] This is

---

[156] *Id.* at art. 5, § 4.

[157] *See generally* Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. TECH. L. REV. 69, 70 (1998) (discussing how jurisdiction theories of international space would work in cyberspace);. *see also* Anna Maria Balsano, *An International Legal Instrument in Cyberspace? A Comparative Analysis with the Law of Outer Space*, THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW (UNESCO, Law of Cyberspace Series Vol. 1, 2000) (discussing comparisons and contrasts between cyberspace law and outer space law).

[158] Menthe, *supra*, note 157, at 83.

[159] Another difference between cyberspace law and space law can be found in the origins of these two forms of law. In contrast to cyberspace, which has an array of existing national laws, "the regulation of outerspace activities does not originate from national

especially true when the perpetrator commits the initial act within the confines of a specific country that seeks to prosecute that person. When there are specific links between the perpetrator of a cybercrime to a particular jurisdiction, the use of a nationality approach, as employed in outer space appears to be unnecessary. Thus, although the virtual nature of cyberspace makes jurisdiction premised upon nationality a possible consideration, as it has in the context of outer space, it is equally important to remember that cyberspace can have connections to a particular jurisdiction that might not be as evident in the context of international space.

IV. RAMIFICATIONS OF EXTRATERRITORIAL PROSECUTION OF CRIMINAL COMPUTER FRAUD

Under existing norms, the five bases of international jurisdiction may serve as different avenues that can be used to obtain jurisdiction for a criminal prosecution in the United States. To permit jurisdictional sufficiency, however, merely by having a prosecutor connect a line with one of these international bases of jurisdiction raises both substantive and procedural concerns. These concerns are particularly pronounced in the areas of fraud, where the very global nature of the computer may stretch the breadth of what will be considered a permissible place for prosecution.

In looking at the substantive issues raised by permitting the United States to prosecute computer fraud crimes occurring outside the country, it is significant that there is a disparity among countries with respect to levels of available technology. This disparity creates questions as to whether United States punishment theories will be successful in preventing future computer fraud crimes that are occurring in less advanced countries. Further, the overlapping approach to fraud in the United States, with acts crossing into both civil and criminal spheres, is not mirrored in all countries. Thus, what may be considered criminal in the United States may not be criminal in another country. Additionally, the imposition of the United States penal system on individuals who reside and act outside the United States raises both political and legal questions.

Procedural issues can also arise in the context of prosecuting extraterritorial computer fraud crimes. Cybercrime places law enforcement in a new realm that is filled with obstacles that impede the

---

laws." *See* Balsano, *supra* note 57, at 141.

detection of criminal conduct. For example, the anonymity of most cyber-criminals can play a role in limiting the ability of police to discern the perpetrator of the crime.[160] This problem of tracing the perpetrator can impede the determination of what is the appropriate jurisdiction for proceeding with a prosecution. Equally problematic is securing the individual and the evidence necessary to prosecute the crime. For example, law enforcement must consider whether it is acceptable for the United States to abduct a person from another country in order to prosecute them for a computer fraud act.

This sampling of substantive and procedural issues that can accrue by a loose extraterritorial policy in the United States is not, in all cases, exclusive to computer fraud acts. For example, there have been criticisms in other contexts related to the government's kidnapping and luring of individuals into the United States. This problem has been particularly apparent in the prosecution of individuals charged with drug offenses. In the contexts where there is already debate over problematic practices such as kidnapping and luring, the use of these same practices in the computer fraud context may not present unique issues. The breadth of people and places, however, that can become subject to United States jurisdiction in cases of criminal computer fraud can amplify existing problems.

A. Punishment

The use of criminal law, as opposed to civil actions, is to a large extent predicated on the appropriateness of punishment. After all, "a person convicted of a crime is punished."[161] Whether one approaches punishment from a retributive or utilitarian perspective, there is still the question of the propriety of punishing conduct that occurred extraterritorially. If another country does not punish the activity, should the United States use its enforcement powers to stop the individual who is outside the United States but harming individuals within this country?[162]

Although the World Wide Web has reached a level of globalization, governments have not. Countries may operate in international

---

[160] *See* Charney & Alexander, *supra* note 18, at 942 ("One important feature of the Internet is the availability of anonymous communications.").

[161] JOSHUA DRESSLER, UNDERSTANDING CRIMINAL LAW 1 (3d ed. 2001).

[162] *See* Patrick J. Fitzgerald, *The Territorial Principle in Penal Law: An Attempted Justification*, 1 GA. J. OF INT'L & COMP. L. 29 (1970) (discussing justifications for territorial principle using punishment theory).

commerce; they may even participate in international treaties and support international initiatives that serve to address a wide array of world problems. This type of global activity does not, however, carry over into enforcing the criminal laws of individual countries.

Basic notions of justice require that individuals need to know of the existence of the criminal laws, unless the law is of a strict liability nature. To punish without knowledge of the criminality does not comport with the essence of modern punishment theories. One cannot deter conduct that a perpetrator does not know to be criminal, nor can one rehabilitate an individual, unless they are aware of the criminality of their actions. To permit rehabilitation and deterrence to emanate solely from the punishment, rather than from the knowing violation of that criminal act, deprives the perpetrator of due process. It seems odd that a progressive country, such as the United States, would resort to punishing computer fraud acts outside the country of individuals who had not been privy to a criminal structure that deemed the activity wrong.

Likewise, one cannot say that criminal computer fraud is inherently wrong and therefore subject to automatic criminal status.[163] If this proposition were true, than all countries would have realized the inherent criminal nature of computer fraud and prohibited the conduct in their criminal code. The reality, however, is that countries do not always criminalize fraudulent computer conduct. Moreover, even if they do, countries do not necessarily criminalize the conduct in the same manner as it is prohibited in the United States.[164]

To some degree, whether a particular activity reaches the level of fraud can be determined by a community standard. What may be fraud in one community could be accepted practice in another community. For example, in *United States v. Brown*,[165] the defendants faced charges of mail fraud for their alleged selling of real estate at high prices. Circuit Judge Edmundson found that although the defendants might have engaged in "sharp conduct, manipulative acts, or unethical transactions," this conduct did not amount to fraud for purposes of the mail fraud statute.[166] Looking at this real estate transaction in the context of the "openness of

---

[163] *See* Ratzlaf v. United States, 510 U.S. 135, 149 (1994) (holding that defendant must know that structuring of monetary transaction was unlawful conduct).

[164] For example, the Philippines did not prohibit the conduct surrounding the "I Love You" virus until one month after the incident. *See* Yam, *supra* note 129, at 9 (discussing how Philippine Congress passed Electronic Commerce Law, which prohibited this conduct, one month later).

[165] 79 F.3d 1550 (11th Cir. 1996).

[166] *Id.* at 1562.

the Florida real estate market," the court found no violation of the fraud statutes.[167]

If alleged fraud is placed in the context of a computer crime, what is the community standard that should be used to determine whether the conduct is in fact fraudulent? Will it be the community of Internet users, the community from which the perpetrator comes, or the community of the victims?[168] There is, obviously, no easy answer. The unavailability of a clear answer militates against the United States imposing punishment on persons who operate under community standards very different from our own.

B. The Merging of Civil and Criminal Fraud

The standards adopted to regulate civil computer activity are not necessarily applicable to criminal activities. This differentiation exists in part because the presumption of innocence and the reasonable doubt burden accorded the criminally accused does not match that used in civil cases. Civil wrongs do not entail jail time, are not premised on the same punishment theories, and do not carry the stigma that is associated with criminal penalties. Where individuals bring civil actions, the state or federal government is the source of a criminal prosecution.[169] Additionally, constitutional amendments provide individuals with certain protections in criminal matters, such as the prohibition against double jeopardy.

Fraud is peculiar in that it crosses into both the civil and criminal areas. Fiduciary wrongs and the deprivation of the right to honest services might be the subject of a civil action, administrative hearing, or criminal charge. For example, a tax fraud or securities fraud may result in a criminal prosecution, or alternatively in administrative penalties. Individual prosecutors in the United States often have the choice of the forum in which to proceed.

Determining what constitutes a criminal fraud also presents problems. The breadth of the concept permits generic fraud statutes to encompass a wide array of conduct. Criminal fraud prosecutions that at one time

---

[167] *Id.*

[168] *See generally* William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community*, 30 WAKE FOREST L. REV. 197, 200-02 (1995) (providing an overview of different communities in cyberspace).

[169] *See generally* Edward M. Wise, *International Crimes and Domestic Criminal Law* 38 DEPAUL L. REV. 923, 923-924 (1989) (discussing distinction between civil and criminal actions).

were limited to public wrongs have now extended into prosecutions of private individuals who have wronged other private parties.[170]

Because different types of fraud conduct are not uniquely criminal in all jurisdictions, it is important to recognize this diversity of views in approaching extraterritorial prosecution. National prosecution for conduct occurring outside this country is more suspect if the country where the conduct occurs does not penalize the activities of the individual.

C. Imposing United States Law on Other Nations

Substantive laws may differ among countries.[171] What may be legal in one country may not in fact present a violation of community norms in another country. The prosecution of technology related offenses that are initiated in countries outside the United States raises concerns when one is imposing the community norms of the United States on these other countries. It is easy to meet the "affect" test for extraterritorial criminal jurisdiction, but is this where the United States should place its criminal justice resources and exposure?[172] This question may implicate the resolution of jurisdiction issues with respect to all computer crimes.

Take, for example, the phenomenon of Internet gambling. The United States gaming industry may now include international sports betting and other Internet gaming activities that are legal in the country where the conduct is initiated. Clearly, the medium of the Internet permits online gambling to be accessible in countries that do not legalize gaming activity. Does this accessibility alone amount to sufficient jurisdiction for prosecution? Do individuals operating the online gambling need to secure a license in all countries in which the item may be accessed? Should 18 U.S.C. §1084, a statute that regulates wagering, be used for prosecuting conduct that originally begins outside this country? Imposing United States legal standards of fraud on individuals in other countries may not be welcomed in all countries.

---

[170] John C. Coffee, *Modern Mail Fraud: The Restoration of the Public/Private Distinction*, 35 AM. CRIM. L. REV. 427 (1998).

[171] The money-laundering laws of the United States are not replicated in all countries. *See* Bruce Zagaris, *A Brave New World: Recent Developments in Anti-Money Laundering and Related Litigation Traps for the Unwary in International Trust Matters*, 32 VAND. J. TRANSNAT'L. 1023 (1999) (discussing international initiatives to combat money laundering).

[172] Bruce Zagaris, *Technology Trumps the Law in International Gaming*, Gaming Enforcement II, Am. Bar Assoc. Cntr. For Continuing Legal Educ., N98GENB ABA - LGLED C-21, C-54 (1998).

One may argue that technologically advanced and better financed countries are in a better position to proceed with a prosecution and should therefore assume the role of world prosecutor. One may also argue that permitting an expansive policy of extraterritoriality will result in forum shopping, where each country involved can look for the place with the law most favorable for its side.[173] Countries that wish to mutually agree on who should proceed with a prosecution will not be precluded from taking this posture by limiting United States extraterritorial jurisdiction. Agreements between countries that foster international relations are encouraged by limiting extraterritorial jurisdiction. Permitting, however, country shopping that is contested by the home jurisdiction of the individual suspected of committing the crime, raises questions of whether international comity is truly being applied.

Extraterritoriality can be a political decision with political ramifications. A negative aura can be associated with assertions of extraterritorial application that assumes jurisdiction over individuals in other countries.[174] Ultimately, this unwelcome assertion of jurisdiction can seriously implicate foreign policy.

D. Constitutional Considerations

Constitutional and legal rights may also play a factor in how criminality is treated in countries outside the United States. There have been constitutional concerns with regard to privacy rights and First Amendment issues. Other constitutional considerations that can influence a United States prosecution include issues involving search and seizure and self-incrimination.[175]

The level of privacy afforded to citizens is not a consistent norm among the countries of this world. Governmental practices of monitoring individual systems can differ.[176] One does not always find

---

[173] *See generally* Symposium, *Post-Cold War International Security Threats: Terrorism, Drugs, and Organized Crime*, 21 MICH. J. INT'L L. 527, 663 (2000).

[174] *See* Brilmayer, *supra* note 85, at 21 ("There are two sources of dissatisfaction with American expansionist tendencies, one practical and one theoretical."); Joseph P. Griffin, *Foreign Governmental Reactions to U.S. Assertions of Extraterritorial Jurisdiction*, 6 GEO. MASON L. REV. 505, 505 (1998) ("Foreign governments have reacted with vehemence towards the extraterritorial enforcement of U.S. antitrust laws in a number of circumstances.").

[175] *See* WISE & PODGOR, *supra* note 2, at 243-82.

[176] *See* Suzanne Daley, *French Prosecutor Investigates U.S. Global Listening System*, N.Y. TIMES, July 5, 2000, at A9 (discussing French investigation of U.S. "Echelon" electronic surveillance system).

comparable First Amendment rights as one finds in the United States. The Internet clearly complicates the right of privacy and the extent to which privacy rights can protect Internet conduct.[177] Although the Council of Europe recommended "guidelines for the protection of individuals with regard to the collection and processing of personal data on informational highways,"[178] one cannot be assured that these recommendations will be adhered to by other countries throughout the world.

Examining the issue of imposing one nation's laws on another nation in a reverse scenario highlights the possible national ramifications of permitting extensive extraterritorial prosecutions. For example, in some countries, a persons' speech may constitute criminal conduct, said conduct being perfectly legal within the United States.[179] Are we willing to accept the extraterritorial jurisdiction of that country to prosecute United States citizens for speech committed over the Internet? Will we authorize extradition of United States citizens for fraud related conduct that is not considered fraud in this country or is protected by the First Amendment? The imposition of United States law on citizens of another country can have repercussions if foreign countries decide to prosecute United States citizens for activity occurring within the United States.

E. Identity

Traditional crimes are not inundated with issues of identity once an individual has been charged with a crime. In the context of traditional crimes, identity questions occur in instances where the perpetrator is unknown and the crime remains unsolved, or the crux of the defense centers on whether the defendant did in fact commit this offense. In cybercrime, however, merely discerning and proving the identity of the

---

[177] *See* Eugene Volokh, *Cyberspace and Privacy: A New Legal Paradigm?*, 52 STAN. L. REV. 1049, 1050-51 (2000) (discussing "information privacy" and free speech).

[178] Council of Europe, Committee of Ministers to Member States for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways, Recommendation No. R(99)5 (adopted Feb. 23, 1999), *available at* http://www.coe.fr/dataprotection/rec/elignes.htm.

[179] *See German and U.S. Clash Over Efforts to Crack Down on Neo-Nazi Web Sites in the U.S.*, 17 Int'l Enforcement L. Rep. No. 2, at ¶ VI.A.64 (Feb. 2001) (discussing controversy between United States and Germany in that Germany wishes to "crack down extraterritorially on Neo-Nazi hate crimes" and United States wishes to maintain individuals First Amendment rights within United States), *see also* Yahoo!, Inc., v. La Ligue Contre Le Racisme et L'Antisenitisme, 2001 WL 1381157, at *9-10 (N.D. Cal. 2001) (ruling that Yahoo! was not subject to French laws criminalizing auctioning of Nazi memorabilia, when conduct was protected by First Amendment).

perpetrator can be a significant problem for law enforcement.

The anonymity of the person committing the act may be difficult to detect in the trail left throughout the world.[180] Anonymity places a greater burden on the government to discern the source of the criminal conduct in order to find not only the appropriate person to prosecute, but also the appropriate place for this prosecution.[181] Countries need to be encouraged to pursue transgressions of the law, despite the fact that the results of the investigation may not produce a prosecution in the jurisdiction doing the investigation. Increased international cooperation, in both the investigation and procurement of evidence, can assist in this regard. Limitations on national jurisdiction need to be mindful of the problems that can arise when a perpetrator acts anonymously.

Even if the source of the conduct is detected, substantive legal questions can still arise as to who will be liable for the criminal conduct. Will it be limited to the person who initially places the item onto the Internet? Will it include individuals who receive the item and then pass it on to others? Will we use conspiratorial liability to go after the Internet Service Provider for allowing the fraudulent conduct to continue to persist on the Internet? The new medium for the crime raises a host of substantive and procedural issues that may implicate the ability to prosecute the person or persons committing the offense. Equally problematic here is that differing laws may offer a host of different resolutions to these questions.

F. Kidnapping and Luring the Perpetrator to the United States

Bringing computer crimes under United States jurisdiction opens the door to procedural actions to secure the individual's presence in the United States. Although extradition presents a formal legal process for obtaining the accused, it is only one source used to procure defendants who are outside the United States. The United States has also used kidnapping and luring to obtain individuals to answer charges levied against them. These informal processes can avoid adherence to the Rule of Speciality,[182] dual criminality,[183] pledges against using the death

---

[180] *See generally* George du Pont, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. & TECH. L. REV. 191 (2001) (discussing ongoing development of law governing anonymity in cyberspace), *available at* http://www.mttlr.org/volseven/duPont.html.

[181] *See* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1750 (1995) ("The ability to appear invisibly on a network and slander, or harass or assault, certainly will increase the incidence of those on the network who slander, or harass or assault.").

[182] *See* United States v. Lui Kin-Hong, 110 F.3d 103, 113 (1st Cir. 1997) ("Speciality has

penalty,[184] and extradition precluded by the political offense exception.[185] The use of abduction to obtain defendants has been used in the United States[186] despite the fact that this practice may be in violation of "general international law principles" and may be "shocking."[187]

The actions of the United States in procuring individuals to stand trial for drug related offenses shows the importance of limiting jurisdiction and limiting discretion prior to computer crimes becoming a new top priority of United States prosecutors. For example, in *United States v. Alvarez-Machain*,[188] the Supreme Court allowed the abduction of a defendant doctor from Guadalajara, Mexico, who was "indicted for participating in the kidnap and murder" of a drug enforcement agent and Mexican pilot. The government did not use extradition to obtain the accused, despite the existence of a United States and Mexico Extradition Treaty. Because the treaty did not preclude forcible abductions, the Court permitted the government's actions.[189] Indeed, there are few instances in which the courts have used their supervisory powers to restrict the government's use of kidnapping and luring to secure the presence of individuals for trial.[190]

Computer offenses are not immune to aggressive police action in instances of alleged international criminal activity. Recently, the Federal Bureau of Investigation established an undercover operation in the United States in order to "snare Russian hackers."[191] In addition to

---

two basic components. First, the requesting state may not try the fugitive for any crimes other than the specific crime for which extradition was sought and granted. Second, the requesting state may not re-extradite the fugitive to a third state.").

[183] Dual criminality requires the crime to be a serious crime and to have a comparable crime in the jurisdiction that the defendant is being extradited from. *See In re* Extradition of Russell, 789 F.2d 801, 803 (9th Cir. 1986).

[184] *See generally* WISE & PODGOR, *supra* note 2, at 477-95.

[185] *See* Quinn v. Robinson, 783 F.2d 776, 791 (9th Cir. 1986) (discussing parameters of political offense exception).

[186] *See, e.g.*, United States v. Noriega, 117 F.3d 1206 (11th Cir. 1997) (defendant abducted from Panama); United States v. Matta-Ballesteros, 71 F.3d 754 (9th Cir. 1995) (defendant abducted from Honduras).

[187] *See* United States v. Alvarez-Machain, 504 U.S. 655, 669 (1992).

[188] *Id.*

[189] The doctor in this case was acquitted at his trial. *See* Alvarez-Machain v. United States, 107 F.3d 696 (9th Cir. 1997) (discussing case of Dr. Alvarez-Machain for charges he filed under the Federal Tort Claims and Torture Victim Protection Acts).

[190] *See* United States v. Toscanino, 500 F.2d 267 (2d Cir. 1974).

[191] *Bogus FBI Company Snares Russian Hackers; Indictments Follow in Connecticut, Washington, and California*, 1 Cybercrime L. Rep. (P & F) No. 7, at 7 (July 2, 2001) (discussing federal indictment of Russians on "charges for breaking into computer systems, stealing credit card information, and attempting to extort payments from victim companies in

luring the defendants to the United States, the FBI used a computer program that permitted them to record keystrokes of the defendants in order to obtain significant data from the use of their computers.[192]

Increased extraterritorial prosecution of computer fraud actions raise flags as to whether practices of luring and kidnapping will become prevalent in this new aspect of the law. With increasing public pressure on curtailing fraud activity, promoting comity may be second seated to practices that would allow the United States to dominate the role of prosecutor of computer related offenses.

V. LIMITING EXTRATERRITORIAL PROSECUTION OF COMPUTER FRAUD

In anticipation of increased computer fraud criminal activity that extends beyond the borders of the United States, it is important to consider appropriate ways to temper national jurisdiction to properly address the criminality but also avoid the possible ramifications, outlined above, of an expansive policy. Congressional recognition of this issue is a first step in the process. By addressing the extraterritorial prosecution of computer fraud crimes in existing or new statutes, a definitive congressional intent would be apparent. Alternatively, there needs to be reconsideration of how objective territoriality applies in the context of computer crimes. What will be considered a reasonable connection for cybercrime fraud jurisdiction may likewise assist in reigning in unlimited and unmonitored prosecutorial discretion.

A. Specific Congressional Language

Modifying 18 U.S.C. § 1030 to consider its extraterritorial application in the specific context of computer fraud acts would certainly assist in providing a clear congressional indication of when it is proper to prosecute conduct occurring outside the United States. The very nature of this statute would allow for consideration of extraterritoriality with respect to each aspect of the statute. Thus, a modified § 1030 would differentiate between crimes that involved the protection of the United States and crimes that focused on consumers within this country. The act of a terrorist breaking into a government computer may warrant an extraterritorial application, as the legislature appears to consider it such in its recent amendment that authorizes extraterritorial application where the computer outside the United States "affects interstate or

---

exchange for computer security services").

[192] *Id.*

foreign commerce or communication of the United States." But where the perpetrator of a crime produces a fraudulent online auction that is intended for consumers in countries outside the United States, extraterritorial criminal jurisdiction may not be needed. Placing specific jurisdictional language in the statute would allow Congress to make the choice of when an extraterritorial criminal application might be proper and when individuals should be left to pursue their private civil remedies.

Congress could also define certain situations in which an "intent to affect" the United States might be a basis for consideration in deciding issues of jurisdiction. For example, Congress could include acts by individuals who deliberately try to evade federal prosecution by committing a computer act outside the United States. Thus, a perpetrator who leaves this country to commit a computer crime in a country that permits the conduct could not avoid criminal prosecution in the United States. In contrast, individuals who intend their communication for a specific jurisdiction might not be subjected to prosecution by every other possible jurisdiction.

Obviously, congressional clarification in the computer fraud statute will not curtail all extraterritorial applications for computer fraud crimes. Prosecutors still have other statutes, such as wire fraud, that can be used to circumvent extraterritorial restrictions that might be placed in the computer fraud statute. One hopes that courts will not allow innovative prosecutorial charging that is used to circumvent criminal conduct that Congress sought to restrict.[193]

B. Reconfiguring Objective Territoriality

Objective territoriality requires that the activity result in a substantial effect on the United States. Permitting extraterritorial jurisdiction whenever the conduct has a substantial effect on the United States offers few limitations when the medium for the crime is a computer. After all, the economic effects on both individuals and businesses by a juvenile hacker can be enormous. Requiring a substantial effect on the United State government, as opposed to a substantial effect on individual citizens, could differentiate between acts that are focused on the general public and acts that have disadvantages to individuals.

---

[193] *See, e.g.*, United States v. Castle, 925 F.2d 831 (5th Cir. 1991) (prohibiting use of conspiracy statute to circumvent exclusion of foreign officials in Foreign Corrupt Practices Act).

United States v. Bowman provides some useful language that draws clear lines for extraterritorial criminal jurisdiction. In *Bowman*, the Supreme Court notes that "[c]rimes against private individuals or their property, like assaults, murder, burglary, larceny, robbery, arson embezzlement and fraud of all kinds, which affect the peace and good order of the community, must of course be committed within the territorial jurisdiction of the government." The Court contrasts these crimes against private individuals with crimes against the government. Although *Bowman* uses language regarding crimes "not logically dependent on their locality," language that might serve to include all computer acts and its separation of private and governmental crimes is an important distinction that can serve as a model for limiting the objective territorial principle.

It will not diminish the effectiveness of our criminal process to leave to another country the option of proceeding with criminal charges in instances where private individuals in the United States are victims of a fraud. Individuals committing acts here would still be subject to criminal punishment. Likewise, individuals who deliberately leave the country to commit a fraud on United States citizens could face prosecution by the United States. Finally, individuals who are not prosecuted in another country could face civil action by the individual or business that are the victims of the perpetrator's actions.

C. Enforcing the Reasonableness Doctrine

Alternatively, the courts could adhere strictly to the "reasonableness" standards set forth in section 403 of the Restatement (Third) of the Foreign Relations Law of the United States. Section 403 places issues of comity at the forefront of considerations of whether extraterritorial application is warranted.[194] Allowing a prosecution merely because it is not specifically excluded by a treaty places few limits on what will be considered reasonable.

The "reasonableness" standard needs to be examined contextually, and not applied merely in the abstract. Courts need to assess "reasonableness" not merely by examining the specific language of the

---

[194] Justice Scalia took this position in his dissenting opinion in *Hartford Fire Insurance Co. v. California*, 509 U.S. 764, 817-18 (1993), a civil case that considered international law principles in deciding whether the Sherman Act should be applied extraterritorially. Justice Scalia, however, joined the majority in *Alvarez-Machain* in permitting the abduction of an individual from Mexico despite its implications to international law. United States v. Alvarez-Machain, 504 U.S. 655, 669 (1992).

regulation, but by also considering the ramifications of permitting the prosecution. Allowing a prosecution when the abduction of the defendant may be "shocking" and possibly in "violation of general international law principles"[195] hardly considers the reasonableness of implementing the applicable law. Public pressure to curtail criminal activity should not be the motivating factor for permitting an extraterritorial prosecution.

By adopting both an abstract and contextual examination of "reasonableness," one can focus on all aspects of having the specific conduct prosecuted in the United States. In the context of computer fraud, this approach would allow for reflecting on factors such as whether the crime would in fact be punishable in the place where the individual committed the act. This approach would also permit considerations of how the prosecution might affect issues of international comity. Applying a "reasonableness" standard to both the conduct, the intent of the individual, the country where it occurred, and the rules of that country would serve to reinforce general principles of punishment that operate in the United States. Merely having a substantial effect on individuals in the United States would not be a controlling factor in the decision to pursue extraterritorial prosecution. Courts can appropriately make distinctions between transgressions involving computer fraud and those involving computer terrorism, with the latter being considered a more likely candidate for extraterritorial criminal prosecution.

CONCLUSION

Will restrictions on the United States prosecution of computer crimes mean that some individuals will not be punished for their commission of computer crimes outside the United States? Will limiting the breadth of national jurisdiction mean that victims of computer fraud in the United States may not be satisfied that our penal system is deterring future activities? The answer to both of these questions is yes. There will be instances where countries do not have sufficient laws to properly punish individuals, where countries will decide not to prosecute these individuals, and where people will not be punished for crimes that affect individuals in the United States.

Hopefully, users of computers in the United States will become educated to these possibilities and act with some skepticism when

---

[195] *See Alvarez-Machain*, 504 U.S. at 669.

operating in the global marketplace.[196] Certainly, existing and future technology can be used to advise those in the marketplace on how to be aware of and avoid fraudulent activities.[197] Likewise, international initiatives may provide a future avenue for relieving some of the ramifications of not having the United States dominate the criminal justice spectrum. The United States has moved in this direction in another context by trying to persuade other countries to adopt anti-bribery laws similar to our Foreign Corrupt Practices Act.[198]

Clearly, law enforcement needs to be bolstered to deal with new and developing technologies.[199] In this regard, joint measures between law enforcement and private industry have already made many inroads.[200] Continued efforts in the international sphere can certainly assist. In the meantime, however, the U.S. law enforcement should tread carefully in imposing its jurisdiction throughout the world. It is one thing to lead the charge in prosecuting international computer fraud crimes; it is another, however, to take charge. Until sufficient international measures are operational, it is important for the United States to remind itself that it is not the world's police, prosecutor and court.

---

[196] Computer users are likely to be more sophisticated in the faults of technology and the possibilities of fraud in the marketplace. *See* Rice, *supra* note 98, at 586 (discussing how American Bar Association Project on Cyberspace noted that "Internet, in many ways, has engendered a breed of 'super-consumers' that should be viewed on par with business customers").

[197] *See* Steven Salbu, *Information Technology in the War Against International Bribery and Corruption: The Next Frontier of Institutional Reform*, 38 HARV. J. ON LEGIS. 67 (2001) (discussing monitoring of criminal bribery activity through use of information technology); *see also Challenges Posed by Cross-Border Fraud on Internet Lead to International Effort*, 1 Cybercrime L. Rep. (P & F) No. 3, at 6 (May 7, 2001). New linking of databases may also assist in fighting computer fraud. *See Markup of Anti-Fraud Database Bill Delayed Over Due Process Concerns*, 1 Cybercrime L. Rep. (P & F) No. 4, at 10 (May 21, 2001); *Reps. Rogers, Oxley Introduce Legislation to Link Government Antifraud Databases*, 1 Cybercrime L. Rep. (P & F) No. 2, at 9 (Apr. 23, 2001).

[198] *See Transnational Bribery: Effort to Implement OECD Anti-Corruption Convention Continues*, 16 Int'l Enforcement L. Rep. XIV, A, at 753 (May 2000).

[199] *See Cybercrime: Special Joint Hearing Before the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee*, 106th Cong. (Feb. 29, 2000) (statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation) (discussing need to keep "law enforcement on the cutting edge of cyber crime"), *available at* http://www.usdoj.gov/criminal/cybercrime/vatis.htm; Marc S. Friedman & Kristin Bissinger, *'Infojacking': Crimes on the Information Superhighway*, 9 PROPRIETARY RTS. 2, 10 (May 1997) ("Another hurdle facing prosecutors and investigators of computer crime is their lack of technical understanding and experience."); *see also* Greg Farrell, *Police Have Few Weapons Against Cyber-Criminals*, USA TODAY, Dec. 6, 2000, at 5B; Charney & Alexander, *supra* note 22 at 944 - 47 (discussing the need for more law enforcement training).

[200] *See* Gonzalez Statement, *supra*, note 65 (discussing private-sector cooperation).

***