NOTES

CYBER CRIME 2.0: AN ARGUMENT TO UPDATE THE UNITED STATES CRIMINAL CODE TO REFLECT THE CHANGING NATURE OF CYBER CRIME

CHARLOTTE DECKER*

I. INTRODUCTION

In 1945, two engineers at the University of Pennsylvania invented the first general-purpose electronic computing device—the Electronic Numerical Integrator and Computer ("ENIAC").[1] The ENIAC was capable of 5000 simple calculations a second, yet it took up the space of an entire room, "weighed 30 tons, and contained over 18,000 vacuum tubes, 70,000 resistors, and almost 5 million hand-soldered joints."[2] This machine cost over $1 million dollars, equivalent to roughly $9 million today.[3] Over the next thirty years integrated circuits shrunk, yielding microprocessors able

* Class of 2008, University of Southern California Gould School of Law; B.A. History and Markets/Management 2005, Duke University. I am especially grateful to Brian Hoffstadt for his keen guidance throughout the writing of this Note, and to the editors and staff of the University of Southern California Law Review for their hard work. I also would like to thank Gabriel Morgan for fostering a healthy sense of competition in law school and in life, and my parents and siblings for their support and encouragement.

1. See Kevin W. Richey, The ENIAC (1997), http://ei.cs.vt.edu/~history/ENIAC.Richey.HTML for a comprehensive account of the invention of the ENIAC.

2. Mark G. Tratos, *Entertainment on the Internet: The Evolution of Entertainment Production, Distribution, Ownership, and Control in the Digital Age*, 862 PLI/PAT 127, 155 (2006).

3. *See* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, BUDGET OF THE UNITED STATES GOVERNMENT, FISCAL YEAR 2005: HISTORICAL TABLES 184–85 tbl.10.1 (2004), *available at* http://www.gpoaccess.gov/usbudget/fy05/sheets/hist10z1.xls (comparing the GDP Deflator Index for 1945 and 2007).

to perform millions and billions of calculations per second with new storage media able to hold megabits and gigabits of data. As a result, computers became smaller, more advanced, and dramatically less expensive. Still, prior to the late-1980s, these and other computers were "solely the tool[s] of a few highly trained technocrats."[4] In the mid-1980s, only 8.2 percent of American households contained computers.[5] American public businesses, universities, and research organizations used only 56,000 large "general purpose" computers and 213,000 smaller "business computers"; private businesses used another 570,000 "mini-computers" and 2.4 million desktop computers[6]; and the federal government employed between 250,000 and 500,000 computers.[7]

However, in recent years, two things have changed. First, in the early 1990s, the cost of computers began a rapid decline, reaching a point by the mid-1990s at which the capabilities and prices of personal computers made them available to the mass market.[8] According to the most recent census data, personal computers can now be found in almost seventy million American households, or 62 percent of all American homes.[9] These home computers are not much larger than the average sewing machine of several decades earlier, yet they are vastly more powerful and complex than anything envisioned by the creators of the ENIAC.[10] The average American has come to rely upon these powerful yet relatively easy to use computers both to perform various analytical functions and to act as repositories for information.

The second major development has been the rapid evolution of networking technologies and declining cost of connectivity, which has set the stage for the widespread commercialization of the Internet.[11] The Internet, like computers, grew out of the Defense Department's advanced research and was initially a tool of the federal government and certain

4. Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 455 (1990).

5. 132 CONG. REC. H3277 (daily ed. June 3, 1986) (statement of Rep. Nelson).

6. *Id.*

7. *See* S. REP. NO. 99-432, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2479.

8. *See* Tratos, *supra* note 2, at 156–57.

9. *See* JENNIFER CHEESEMAN DAY, ALEX JANUS & JESSICA DAVIS, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003, at 2 (2005).

10. Indeed, personal computers are able to perform complicated storage, retrieval, and analytical processes well beyond the capabilities of the technology used to plan, manage, and execute the landing of men on the moon a bit more than two decades earlier.

11. *See* Tratos, *supra* note 2, at 157–59 (discussing the development of a new Internet backbone).

academic research institutions.[12] With the advent of "hypertext markup language," the *lingua franca* of Internet browsers and the World Wide Web, use of the Internet spread rapidly to businesses and homes. It is estimated that three-quarters of all Americans now have access to the Internet and spend an average of twelve-and-a-half hours per week online.[13]

These changes in computing and networking have created an environment in which people increasingly gather in cyberspace to interact socially and commercially. And, like any other gathering place, such an environment creates ample chances for the opportunist to prey upon the unsophisticated, uninformed or naïve. Corresponding to the increase of the use of the Internet by households and businesses, the prevalence of crime in cyberspace has rapidly increased.

Initially, criminal activity in cyberspace was aimed at governments, banks, and other organizations that were early adopters of advanced computing and networking technologies. But now that computers are found in most homes and almost every business, experts warn there is "likely to be a greater proliferation in the number and types of businesses that will be potential victims of cyber-crimes."[14] The expansion in the class of targets of computer crime is also coupled with a wholesale growth in the number of people able and willing to commit cyber crimes.[15]

The costs of cyber crime cannot be ignored. Cyber crime costs the global economy billions of dollars each year,[16] which translates into lost

12. For an interesting read tracing the early prototype of the Internet to its modern incarnation, see KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1998).

13. Steven Levy, *No Net? We'd Rather Go Without Food*, NEWSWEEK, Oct. 11, 2004, at 14.

14. Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 203 (2006).

15. *Id.* at 205. Growth of cyber criminals is occurring on two axes: first, the number of people who are technologically savvy enough to commit cyber crimes is growing exponentially. Second, a derivative market in cyber crime appears to be growing as "enablers"—"persons who use their technical expertise to create and then sell to others easy-to-use tools"—make it possible for nontechnologically savvy people to engage in cyber crime. *Id.*

16. Eric H. Holder, Jr., Deputy Attorney Gen., Remarks at the High-tech Crime Summit (Jan. 12, 2000), *available at* http://www.cybercrime.gov/dag0112.htm. In 2005, "computer-based crimes caused $14.2 billion in damage to businesses around the globe according to Computer Economics, an Irvine, California research firm." Cassell Bryan-Low, *To Catch Crooks in Cyberspace, FBI Goes Global*, WALL ST. J., Nov. 21, 2006, at A1. In the United States alone, the FBI estimates that cyber crimes cost companies and consumers $400 billion annually. Kevin Voigt, *Gangs Flooding the Web for Prey, Analysts Say*, CNN.COM, Dec. 20. 2006, http://www.cnn.com/2006/TECH/internet/12/20/cybercrime/index.html.

jobs, lost taxes, lost innovation, higher costs for consumers,[17] lost confidence in Internet commerce,[18] and stunted global trade.[19]

Perhaps the highest and most dangerous cost of cyber crime is the increased threat to national security. Much of our modern critical infrastructure is wholly dependant on networked computing—for example the air traffic control system, the power grid, the water supply systems, telecommunications networks, the financial sector, and critical government services such as emergency and national defense services—making it extraordinarily vulnerable to cybercrime.[20] Indeed, "the prospect of 'information warfare' by foreign militaries against our critical infrastructure is perhaps the greatest potential cyber threat to our national security."[21] As computer use continues to grow, "cyber attacks on critical infrastructure or military operations [are] a way to hit what [is perceived] as America's Achilles heel—our growing dependence on information technology in government and commercial operations."[22]

Still, experts warn the worst is yet to be seen; projections indicate "the number of Internet-enabled crimes will increase radically over the next few

17. *See* Holder, *supra* note 16.

18. The 2000 attacks on well-known Internet sites (eBay, Yahoo, and CNN among others) contributed to a 258-point drop on the Dow Jones Industrial Average and halted a three-day string of record-high closings on the NASDAQ composite index. *Cyber Attack: Roadblocks to Investigation and Information Sharing: Hearing Before the S. Judiciary Subcomm. on Tech., Terrorism, and Gov't Info*., 106th Cong. (2000) (statement of Sen. Kyl) [hereinafter Kyl Statement]. *See* Yang & Hoffstadt, *supra* note 14.

19. The weak enforcement mechanisms for protecting globally networked information create "an inhospitable environment in which to conduct e-business within a country and across national boundaries. . . . [which] can create barriers to [digital information] exchange and stunt the growth of [international] e-commerce." MCCONNELL INT'L, CYBER CRIME . . . AND PUNISHMENT?: ARCHAIC LAWS THREATEN GLOBAL INFORMATION 3 (2000) [hereinafter MCCONNELL, CYBER CRIME]. Several reports by McConnell International measured various countries' legislation in their readiness to address cyber crime in four categories: data-related crimes, network-related crime, crimes of access, and associated computer-related crimes. *Id.* According to these reports, thirty-three of the fifty-two countries surveyed have yet to update their laws to address *any* type of cyber crime; nine have enacted legislation to address five or fewer types of cyber crime; and ten countries have updated their laws to prosecute six to ten types of cyber crime. *Id.* These findings suggest that few countries are able to "demonstrate that adequate legal measures had been taken to ensure that that perpetrators of cyber crime would be held accountable for their actions." *Id.* at 2. Over half the countries in the McConnell reports were rated as needing "substantial improvement" to their information security. *Id.* at 3. *See also* MCCONNELL INT'L, RISK E-BUSINESS: SEIZING THE OPPORTUNITY OF GLOBAL E-READINESS (2000).

20. *See Fighting Cyber Crime: Efforts by Fed. Law Enforcement: Hearing Before the H. Comm. on the Judiciary*, 107th Cong. (2001) (statement of Michael Chertoff, Assistant Att'y Gen.); Holder, *supra* note 16.

21. *On Cybercrime: Hearing Before the Subcomm. for the Tech., Terrorism, and Gov't Info. of the Sen. Comm. on the Judiciary*, 106th Cong. (2000) (statement of Louis J. Freeh, Director, FBI) [hereinafter Freeh].

22. *Id.*

years."[23] The future of cyber crime presents lower consumer confidence in Internet security, stunted growth of e-commerce,[24] stifled trade,[25] and the serious threat of cyber terrorism.[26]

Cyber crime can be divided into two basic types: first, destructive or intrusive activity aimed at computers (or networks of computers) and the information contained on them, and second, crimes where computers are used as a tool for committing other, more traditional, illicit activities against persons or property.[27] Customarily, cyber crime, like other areas of criminal law, had been left to the states to regulate as an exercise of their police power. Expansion of federal criminal jurisdiction is a recent phenomenon, and largely a product of broad legislative and judicial interpretation of the Commerce Clause. However, the advent of attacks against the networks themselves and attempts to steal or destroy the information on these networks has led to increasing efforts by the federal government to intervene. By relying upon the Commerce Clause for authority, Congress has acknowledged the stateless, and indeed global, nature of the Internet by writing specialized criminal code sections.

As the nature and scale of the risk continue to evolve and grow, the question of the scope and capabilities of existing criminal law to address cyber crime becomes more acute. Part II of this Note provides a background of the evolution of cyber crime and discusses various examples of criminal activity in cyber space. Part III surveys current criminal law used to prosecute cyber crime. Part IV examines whether the current statutory framework for prosecuting cyber crime contains gaps in either its scope or breadth. Part V addresses how, if at all, these gaps should be filled.

This Note concludes that there are three areas not adequately covered by current federal criminal law: (1) the $5000 minimum loss threshold of

23. Steven M. Martinez, Acting Assistant Dir., Cyber Div., Remarks at Third Annual Cyber Security Summit 2005 (Feb. 9, 2005), *available at* http://www.fbi.gov/pressrel/speeches/martinez020905.htm.

24. Robert S. Mueller III, Dir., FBI, Speech before the Info. Tech. Assoc. of Am. Conference on Combating E-crime (Oct. 31, 2002), *available at* http://www.fbi.gov/pressrel/ speeches/itaa.htm.

25. *See* MCCONNELL, CYBER CRIME, *supra* note 19.

26. *See* Holder, *supra* note 16; Mueller, *supra* note 24.

27. The breakdown of computer crimes into three categories is borrowed from the Legislative Analysis of the Computer Fraud and Abuse Act of 1996. *See* Computer Crime and Intellectual Prop. Section, U.S. Dep't of Justice, *Legislative Analysis of the National Information Infrastructure Protection Act*, 2 ELECTRONIC INFO. POL'Y & L. REP. 240 (1997) [hereinafter *Legislative Analysis*]. A third category of computer crimes, where the computer is incidental to the crime, will not be discussed, as it is outside the scope of this Note. These crimes are prosecuted under traditional criminal code sections (that is, drug trafficking statutes, RICO, etc.).

the Computer Fraud and Abuse Act ("CFAA");[28] (2) exclusions in the definition of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act") for spIM;[29] and (3) the lack of specialized provisions for preventing or punishing phishing crimes. This Note concludes with specific recommendations for legislation to close those gaps.

II. CYBER CRIMES

The term "cyber crime," broadly defined as crimes "perpetrated over the Internet, typically having to do with online fraud,"[30] is generally thought to describe two main types of Internet-based behaviors: criminal activity targeting computers and the information stored on computers, and activities in which a computer is used to facilitate another, more traditional crime.[31]

A. CRIMES AIMED AT THE COMPUTER OR INFORMATION ON THE COMPUTER

The prevalence of crime in which the computer is the target is in some ways unremarkable; new technologies often spawn new crimes. In the same way that the introduction of the automobile in the nineteenth century created opportunities for criminal mischief targeting the car itself, perhaps cyber crime is the "natural result" of the introduction of computers into American society.[32] However, unlike the automobile, the cyber environment provides endless opportunities for criminal mischief, the boundaries of which extend far beyond the physical scope of a computer itself. Examples of crimes aimed at computers are: hacking, distributed denial-of-service attacks, extortionate hacking, theft of trade secrets, access device theft, and wiretap violations. Each of these crimes will be examined in some detail.

28. 18 U.S.C. § 1030(a)(5) (2000).

29. Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003, 15 U.S.C. §§ 7701–13 (Supp. IV 2004).

30. PCMAG.COM ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3 Dcybercrime&i%3D40628%2C00.asp (last visited July 31, 2008).

31. *See Legislative Analysis*, supra note 27.

32. *Id. See* Press Release, FBI (Nov. 20, 2003), *available at* www.fbi.gov/pressrel/pressrel03/sweep112003.htm (stating that as the computer's role in society continues to grow, criminal exploitation of the vulnerabilities of computers and information technology for illegal purposes is expected).

1. Hacking

A "hacker" is "[a] computer enthusiast who enjoys learning everything about a computer system or network and pushing the system to its highest possible level of performance through clever programming."[33] Absent some nefarious intent or use, hacking is not illegal under federal law.[34] However, hacking can easily migrate from a benign hobby to a criminal enterprise. In this sense, hacking is defined as the surreptitious breaking "into the computer, network, servers, or database of another person or organization."[35] When hackers mix with "fraudsters" and organized crime rings, the tools and effects of hacking can be, and are, used illegally for financial gain.[36] In this way, hacking has "becom[e] part of the modern criminal's toolbox."[37]

Until recently, hackers tended to target online information brokers and manufacturers and distributors of digital media;[38] however, the growth of the Internet has opened new avenues for hackers, and now any business that relies on computers and the Internet to conduct its daily affairs is vulnerable to cyber crime.[39] In the past year, between 25 and 50 percent of American businesses have found some sort of security breach in their computer networks.[40]

Attack tools have become more sophisticated in recent years as they

33. BRYAN PFAFFENBERGER, WEBSTER'S NEW WORD: DICTIONARY OF COMPUTER TERMS 247 (8th ed. 2000). *See also* 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 (2000); Victor Sabadash, *What Is Hacking*, COMPUTER CRIME RESEARCH CENTER, May 5, 2004, http://www.crime-research.org/news/05.05.2004/241. Apparently the "Hacker's credo" is:

> 1. Access to all computers should be unlimited and total.
> 2. All information should be free.
> 3. Mistrust authority—promote decentralization.
> 4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
> 5. You can create art and beauty on a computer.
> 6. Computers can change your life for the better.

Id. (quoting Deb Price & Steve Schmadeke, *Hackers Expose Web Weakness: There's No Defense Against Internet Assaults, Experts Confess, and Attackers Are Elusive*, DET. NEWS, Feb. 14, 2000, at A1).

34. *See* 18 U.S.C. § 1030 (2000 & Supp. IV 2004).

35. BLACK'S LAW DICTIONARY 730 (8th ed. 2004).

36. Cassell Bryan-Low, *Growing Number of Hackers Attack Web Sites for Cash*, WALL ST. J., Nov. 30, 2004, at A1.

37. *Id.*

38. Yang & Hoffstadt, *supra* note 14, at 203–04.

39. *Id.* at 204–05 (citing Robert Steinberg, *Advising Clients About Hacker Insurance*, L.A. LAWYER, Feb. 2003, at 60, for the proposition that most American businesses rely on the Internet and computers to run their affairs).

40. *Id.* at 201.

have also become easier to use.[41] The variety of "do-it-yourself" guides to hacking on the World Wide Web has made hacking more accessible than ever for the novice enthusiast.[42]

The result of hacking—disruption of networks and theft or destruction of data—presents a profound problem. The effects of such attacks include the inability of the attacked organization to conduct business, loss of consumer records, inability to produce products, negative media attention, forwarding or exposure of private information,[43] embarrassing Web site defacement, publication of confidential information, as well as harm to individuals at the hacked organization and in the general public.[44]

2. DDoS Attacks

A denial-of-service attack ("DoS") is a relatively primitive technique that overwhelms the resources of a computer or server and results in the denial of server access to other legitimate users of the service.[45] The attacker denies service by sending a stream of packets to a victim that either consumes some key resource, thus rendering it unavailable to legitimate clients, or provides the attacker with unlimited access to the victim machine in order to inflict damage.[46]

A distributed denial-of-service ("DDoS") attack is the natural cyber progression "in the search for more effective and debilitating denial of service attacks."[47] Instead of using just one computer, in a DDoS attack, a hacker places a daemon, or small computer program, on a third-party computer, which then deploys multiple "daemonized" computers of

41. Freeh, *supra* note 21.

42. *See, e.g.*, Charlie Demerjian, *How to Hack Biometrics*, INQUIRER, July 30, 2005, http://www.theinquirer.net/en/inquirer/news/2005/07/30/how-to-hack-biometrics; Eric S. Raymond, How to Become a Hacker (2001), http://www.catb.org/~esr/faqs/hacker-howto.html (last visited July 31, 2008); Hack a Day, http://www.hackaday.com/ (last visited July 31, 2008); HackThisSite.Org, http://www.hackthissite.org/ (last visited July 31, 2008).

43. The personal details of more than 100 million people have been exposed as a result of accidents and hacker attacks. *See* Voigt, *supra* note 16.

44. DAWN CAPPELLI ET AL., CARNEGIE MELLON UNIV., COMMON SENSE GUIDE TO PREVENTION AND DETECTION OF INSIDER THREATS 8 (2d ed. 2006), *available at* http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf.

45. An attacker may be able to prevent access to e-mail, web sites, online accounts (banking, etc.), or other services that rely on an affected computer. CERT Coordination Center, Denial of Service Attacks, http://www.cert.org/tech_tips/denial_of_service.html (last visited July 31, 2008).

46. Three main network exploits are used to overwhelm a system's server, each of which exploits a weakness in the way computers communicate with one another over the Internet: SYN Flood Attacks, UDP Flood Attacks, and ICMP Flood Attacks. For a comprehensive description of each type of attack, see Sinrod & Reilly, *supra* note 33, at 190–93.

47. *Id.* at 194.

unsuspecting users (referred to as "zombies") to cause a denial of service to legitimate users for some time.[48] A DDoS attack inflicts damage from a wider base of servers, making it more difficult for the target to block the attack.[49] Unlike hacks, which include a broad universe of attacks against a single computer, DDoS attacks are generally aimed at Internet Web sites and designed to overwhelm the pipeline to the Internet. Recent attacks have been launched for financial gain,[50] for political purposes,[51] and as technological warfare.[52] DoS and DDoS attacks cost American businesses $2.9 billion in the past year.[53]

3. Extortionate Hacking

Black's Law Dictionary defines extortion as "the act or practice of obtaining something or compelling some action by illegal means, as by force or coercion."[54] Combined with hacking, computers present a new twist on traditional extortion.[55]

48. *See* Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 245 n.41 (2003).

49. Sinrod & Reilly, *supra* note 33, at 194.

50. *See* Joris Evers, *Hacking for Dollars*, CNET NEWS, July 6, 2005, http://news.cnet.com/Hacking-for-dollars/2100-7349_3-5772238.html.

51. "Hacktivism," hacker (political) activism, has become a popular outlet for political dissent. Hacktivists launch politically motivated attacks by overloading e-mail or Internet servers with politically charged messages or crash servers to prove a political point. *See* Freeh, *supra* note 21; Sinrod & Reilly, *supra* note 33, at 183. An example of hacktivism was an attack in February 2000, when the now-infamous hacker known as "Mafiaboy" used commonly known techniques to completely disrupt network operations at eBay, Amazon.com, and CNN.com, as well as five other major commercial networks to protest the commercialization of the Internet. *See* Alexander Urbelis, *Toward a More Equitable Prosecution of Cybercrime: Concerning Hackers, Criminals, and the National Security*, 29 VT. L. REV. 975, 993 (2005). Another example is the U.K.-based Electrohippie Collective who used DDoS attacks as part of a "sit-in" to protest the World Trade Organization at their summit in Seattle. *See* Jelena Mirkovic & Peter Reiher, *A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms*, 34 COMPUTER COMM. REV. 39 (2004); Dorothy Denning, *Cyberwarriors: Activists and Terrorists Turn to Cyberspace*, HARV. INT. REV., Sept. 2001, at 70.

52. *See* Mudawi Mukhtar Elmusharaf, *Cyber Terorism: The New Kind of Terrorism*, COMPUTER CRIME RES. CENTER, Apr. 8, 2004, http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism.

53. LAWRENCE A. GORDON ET AL., COMPUTER SECURITY INST., CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 2006, at 15.

54. BLACK'S LAW DICTIONARY 623 (8th ed. 2004).

55. A self proclaimed manifesto of hackers is the following:

> Our mission is to help companies to protect their customers' data. There are many skilled hackers in our team. We can break almost any modern computer system, including online banks and big online shops. When we get access to such systems we notify their owners about it. Some companies are ready to cooperate and they get our help. We send them instructions about how to improve their systems and later we track the process of this improvement. These companies care about their customers.

Extortionist hackers infiltrate computer systems, and then demand a ransom by threatening further destruction or damage. Extortionate hacking can take the form of a hack, as against one computer, or a DDoS attack, where a user threatens to overwhelm a server unless a high ransom is paid.[56] The targets of such attacks are diverse.[57] Extortionists have levied threats against Michael Bloomberg, the founder of Bloomberg Financial L.P.;[58] business-to-business site Creditcards.com;[59] gambling Web sites prior to Super Bowl weekend;[60] and European financial sites.[61] Extortionate hacking attacks have forced targeted Web sites offline (and out of business) for weeks.[62] The security breaches have caused damaging losses of credibility as well as high costs of repair for online businesses.[63]

Additional consequences of extortionate hacking include concerns for national security. Experts assert that there is little doubt that international organized crime is involved in extortionate hacking, which has the potential to pose real and serious threats to national information security.[64]

> But some Internet sites don't want to cooperate. In this case we notify all their customers about existing security loopholes. We do it to protect people against further loss of personal information. This is our mission.

Bob Sullivan, *Inside a Net Extortion Ring*, MSNBC, June 20, 2006, http://www.msnbc.msn.com/id/3078571 (quoting no longer existing Web site supporting net-extortion ring).

56. *See, e.g.*, Steven J. Vaughan-Nichols, *SCO's MyDoom DDoS Hammering Begins*, EWEEK, Feb. 1, 2004, http://www.eweek.com/c/a/Linux-and-Open-Source/SCOs-MyDoom-DDoS-Hammering-Begins. The MyDoom virus was estimated to have infected hundreds of thousands of computers worldwide; the attack on SCO Group was the first large-scale attack that employed the zombie computers infected with MyDoom to overwhelm the company's webpage. *Id.*

57. One particularly successful extortionist-hacker, known as "Mr. Zilterio," has, by his own account, hacked into online companies and financial institutions, stolen data, and demanded extortion payments from over fifteen companies in the United States and Europe, nine of which he claims have paid him in excess of $150,000. Sullivan, *supra* note 55.

58. Oleg Zezov was arrested by the FBI for hacking into Bloomberg's computer system, then threatening that "the financial news service's reputation would be put at risk if he was not paid $200,000." John Leyden, *Bloomberg Extortion, Hacking Case Opens in New York*, REGISTER, Feb. 6, 2003, *available at* http://www.theregister.co.uk/2003/02/06/bloomberg_extortion_hacking_case_ opens. *See also* Press Release, U.S. Attorney for the S. Dist. of N.Y., Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System (Aug. 14, 2000), *available at* http://www.cybercrime.gov/bloomberg.htm.

59. *See* Steven Shankland, *Company Says Extortion Try Exposes Thousands of Card Numbers*, CNET NEWS, Jan. 2, 2002, http://www.news.com/2102-1017_3-249772.html.

60. Online gaming sites began receiving threats in October 2003 containing demands for money to prevent DDoS attacks that would shut down their Web site at key times, such as during the Super Bowl. Jack M. Germain, *Global Extortion: Online Gambling and Organized Hacking*, TECHNEWSWORLD, Mar. 23, 2004, http://www.technewsworld.com/story/33171.html.

61. *Id.*

62. *See id.*

63. *See* Shankland, *supra* note 59 (explaining that the breach of the Creditcards.com system threatened to expose fifty-five thousand credit card numbers).

64. *Id.*

4. Trade Secret Theft

"Trade secrets" are:

> all forms and types of financial, business, scientific, technical, economic, or engineering information . . . [that] the owner thereof has taken reasonable measures to keep . . . secret; and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by[] the public.[65]

Theft of a trade secret becomes a cyber crime when the secret is stolen, appropriated, taken, or carried away by use of computer or the Internet.[66] As the power of computer technology has grown in the past two decades, it has resulted in "increasingly more powerful means for theft and transfer of trade secret information."[67] For example, "an item of trade secret information (such as computer source code, a biochemical formula, or technical schematics) can be as valuable to a company as an entire factory was even several years ago. Computers now make it extremely easy to surreptitiously copy and transfer this valuable trade secret information."[68]

5. Access Device Fraud

Access device fraud is the theft of access devices, which generally are any

> card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.[69]

Access device fraud commonly refers to credit card theft or "skimming"; however, it also applies to theft of other access devices including computer passwords, personal identification numbers—or PINs, used to activate ATMs—long-distance access codes, and the computer

65. 18 U.S.C. § 1839(3) (2000).

66. 18 U.S.C. § 1832(a)(1)–(3) (2000).

67. R. Mark Halligan, The Economic Espionage Act of 1996: The Theft of Trade Secrets Is Now a Federal Crime, http://my.execpc.com/~mhallign/crime.html (last visited July 31, 2008). *See* National Cybercrime Conference: Bio: R. Mark Halligan, http://www.cybercrimeconference.org/bios/Halligan.html (last visited July 31, 2008) (providing credentials).

68. Halligan, *supra* note 67.

69. 18 U.S.C. § 1029(e)(1) (2000).

chips in cellular phones that track billing data.[70] Increasingly, theft of these devices is being treated as a cyber crime.[71]

6. Wiretap Violations

Federal law criminalizes the manufacture, possession, assembly, or sale of any device designed "for the purpose of the surreptitious interception of wire, oral, or electronic communications."[72] As provided by statute, "electronic communication" means any transfer of "signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce."[73] The growing use of computers has added new dimensions to wiretapping crimes. Courts have interpreted an interception of *any* electronic communication to amount to a wiretap.[74]

B. COMPUTER AS THE TOOL

New computer technology can be "used by some of the worst elements of our society: small-time criminals who can take on a whole new persona on the Internet; malcontents who can find like-minded hate groups; and scam artists who think they can escape detection in the anonymity of the Web."[75] Such criminals have been able to use computers as instruments to commit other crimes. Internet fraud is the most prevalent, and the most costly, of these crimes.[76] Internet fraud refers generally to any type of fraud scheme that uses components of the Internet—for example, chat rooms, e-mail, message boards, or Web sites—to "present fraudulent solicitations to

70. U.S. Secret Service: Financial Crimes Division, http://www.secretservice.gov/financial_crimes.shtml (last visited June 23, 2008).

71. *See* Press Release, U.S. Secret Service, Additional Indictments Announced in Ongoing Secret Service Network Intrusion Investigation (Aug. 5, 2008), *available at* http://www.ustreas.gov/usss/press/GPA15-08_CyberIndictments_Final.pdf.

72. 18 U.S.C. § 2512(1)(b) (2000).

73. 18 U.S.C. § 2510(12) (Supp. IV 2002). *See* United States. v. Herring, 993 F.2d 784, 787–88 (11th Cir. 1993).

74. *See* United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005).

75. Mueller, *supra* note 24.

76. Internet fraud has accounted for between $183.12 million and $2.6 billion in losses annually. INTERNET CRIME COMPLAINT CTR., IC3 2005 INTERNET CRIME REPORT 8, *available at* http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf [hereinafter IC3 REPORT]. *See* Bob Sullivan, *Online Fraud Costs $2.6 Billion This Year*, MSNBC, Nov. 11, 2004, http://www.msnbc.msn.com/id/6463545; Press Release, Computer Security Institute, Financial Losses Due to Internet Intrusions, Trade Secret Theft, and Other Cyber Crimes Soar (Mar. 12, 2001), *available at* http://www.cryptic.co.uk/Press_Documents/Press_Articles/2001-03-12_CSI.pdf (noting an approximately 40 percent increase from the amount of loss in 2000).

prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other [sic] connected with the scheme."[77] Internet fraud takes various forms.

1. Auction Fraud

Internet auction sites present an easy source of possible Internet fraud victims.[78] Online auction sites are immensely popular, and their popularity is only growing.[79] The largest, eBay, reported third quarter revenues of $1.449 billion in 2006, up 31 percent from 2005, and had 212 million registered users, up 26 percent.[80] However, the popularity of online auction sites also makes them a target for cyber criminals. Indeed, online auctions provide an ideal environment for Internet fraud due to the completely anonymous and virtual nature of the transaction.[81]

Types of Internet auction fraud include "fraud due to the misrepresentation of a product advertised for sale through an Internet auction site, the non-delivery of an item purchased through an Internet auction site or a non-payment for goods purchased through an Internet auction."[82] Cases of auction fraud often involve the use of a legitimate online auction site or retail site that purports to offer a high-value item or items, that, when purchased, either do not exist or are of substantially less value than advertised (that is, they are counterfeit or altered goods).[83]

77. Internet Fraud, U.S. Dep't of Justice, http://www.usdoj.gov/criminal/fraud/internet/ (last visited July 31, 2008).

78. Fed. Trade Comm'n, Internet Auctions: A Guide for Buyers and Sellers, http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec07.pdf (last visited July 31, 2008).

79. The total value of e-commerce transactions around the world reached around $3.8 trillion in 2003, and was projected to reach over $9 trillion in 2005, and around 18 percent of total global sales in 2006. Mohamed S. Wahab, *E-Commerce and Internet Auction Fraud: The E-Bay Community Model*, COMPUTER CRIME RES. CENTER, Apr. 29, 2004, http://www.crime-research.org/articles/Wahab1.

80. *Online Auction Fraud: Data Mining Software Fingers Both Perpetrators and Accomplices*, SCI. DAILY, Dec. 5, 2006, http://www.sciencedaily.com/releases/2006/12/061205143326.htm.

81. *See* Alex Tsow, Phishing with Consumer Electronics: Malicious Home Routers 5–6 (May, 22, 2006), http://www.cs.indiana.edu/~atsow/papers/MTW06-final.pdf.

82. Royal Can. Mounted Police, Online Auction Fraud, http://www.rcmp-grc.gc.ca/scams/online_fraud_e.htm (last visited July 31, 2008).

83. Internet Fraud, *supra* note 77. An example of a victim of such a crime is "Mark," who was the highest bidder on eBay for a Toshiba Protégé 2000 laptop computer. On August 10, 2002, Mark sent a cashiers check for approximately $1500 to the online seller; by September 1, Mark still had not seen the computer. *See* Ina Steiner, *eBay Auction Fraud Spawns Vigilantism Trend*, AUCTIONBYTES, Oct. 12, 2002, http://www.auctionbytes.com/cab/abn/y02/m10/i12/s01. Other Internet auction crimes defraud legitimate users by exploiting illegal strategies to mark up prices; "shill bidding," where fraudulent sellers or their partners, known as "shills," bid on sellers' items to drive up the price, and "bid shielding," when fraudulent buyers submit very high bids to discourage other bidders from competing for the same item, then retract their bids so that coconspirators can purchase the item at a

Internet auction fraud accounted for almost two-thirds of the 97,000 complaints referred to law enforcement agencies in 2005 by the Federal Internet Crime Complaint Center, and auction fraud accounts for the largest percentage of Internet fraud (62.7 percent).[84] The total dollar loss for Internet fraud was $183 million in 2005, up from $68 million in 2004.[85]

2. Spam

"Spam" is unsolicited bulk electronic mail, usually of a commercial nature.[86] While unsolicited and unwelcome letters clog up many e-mail inboxes, an unwanted e-mail is not necessarily spam. Spam refers to unsolicited, inappropriate, or irrelevant messages sent through e-mail systems, often on a mass scale and with a commercial purpose—such as to attract Internet users to Web sites offering pornography, "get rich quick" schemes, or fraudulent medical products.[87] Under the technical definition, an unsolicited bulk e-mail is spam if: "(1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; [and] (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be

lower price, are prevalent problems on Internet auction sites. *See* Susan Kuchinskas, *EBay Charged with Shilling*¸ INTERNETNEWS, Feb. 23, 2005, http://www.internetnews.com/ec-news/article.php/3485301; Joseph Pelliciotti, *Online Auctions Fertile Ground for Fraud*, TIME (Munster, Ill.), May 26, 2003, *available at* http://www.crime-research.org/news/2003/05/Mess2602.html. Other auction fraud crimes aim to draw the user off the legitimate site onto an unsecured site, the end goal of which is to trick consumers into sending money without delivering the item. *See* Jodie Kirshner, *Bitten Bidders*, U.S. NEWS & WORLD REP., June, 8, 2003, at 56. By going off-site, buyers lose any protections the original site may provide, such as insurance, feedback forms, or guarantees. *See*, *e.g.*, eBay Privacy Policy, http://pages.ebay.com/help/policies/privacy-policy.html (last visited Aug. 13, 2008). Examples of this type of crime are "bid siphoning," where bidders are lured off legitimate auction sites by offers of the "same" item at a lower price, and "second chance offers," where con artists offer losing bidders of a closed auction a second chance to purchase the item that they lost in the auction. *See* Pelliciotti, *supra* note 83.

84. IC3 REPORT, *supra* note 76, at 3. *See* JONATHAN RUSCH, U.S. DEP'T OF JUSTICE, THE RISING TIDE OF INTERNET FRAUD (2001), *available at* http://www.cybercrime.gov/usamay2001_1.htm.

85. Press Release, FBI, FBI Internet Crime Complaint Center Releases Stats (Apr. 6, 2006), *available at* http://www.fbi.gov/pressrel/pressrel06/internetcrimereport.htm.

86. BLACK'S LAW DICTIONARY 1430 (8th ed. 2004). The prevailing theory for the etymology of the word "spam" refers to a classic skit by Monty Python's Flying Circus. In the skit, a couple in a restaurant tries in vain to order something that does not contain Spam (the canned meat). As the waitress lists endless dishes, all of them containing increasing amounts of Spam, a group of Vikings in the corner begin to sing, "[s]pam spam spam spam . . ." until all useful information is drowned out. H. Kent Craig, The True Story of How Internet "Spam" Got Its Name, http://hkentcraig.com/HowInternetSpamGotItsName.html#pythonskit (last visited July 31, 2008).

87. *See* Lily Zhang, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301, 308 (2005).

sent."[88] Spam is widely condemned in the Internet community.[89]

Approximately 140 million Americans regularly use e-mail.[90] Spam accounts for half of all U.S. e-mail traffic, making it not only "a hair-pulling annoyance but also an increasing drain on corporate budgets and possibly a threat to the continued usefulness of the most successful tool of the computer age."[91] According to Ferris Research, a San Francisco-based consulting group, the cost of spam to U.S. organizations is at least $17 billion per year.[92] The annoyance cost of spam to individuals is incalculable as e-mail users are forced to spend precious time sorting through a sea of junk to find the few legitimate messages.[93]

While the deluge of spam continues, it is perhaps being outpaced by "spIM."[94] SpIM refers to the sending of unsolicited commercial messages through instant messaging programs.[95] In most respects spIM is similar to spam, and entails similar costs and dangers. Like spam, spIM utilizes the attention grabbing nature of online messaging systems to entice users to fall for fraudulent schemes.[96] However, unlike spam, spIMmers can use the commercial messages to embed malicious code that exploits vulnerabilities

88. The Spamhaus Project, The Definition of Spam, http://www.spamhaus.org/definition.html (last visited July 31, 2008).

89. The overwhelming presence of unwanted and often offensive e-mail "greatly interferes with the user's ability to sort out which e-mail messages are 'legitimate' and desired." Jay M. Zitter, Annotation, *Validity Construction, and Application of Federal and State Statutes Regulating Unsolicited E-mail or "Spam,"* 10 A.L.R. 6th 1, 1 (2006).

90. *See* CAN-SPAM ACT OF 2003, S. REP. NO. 108-102, at 2 (2003), *as reprinted in* 2004 U.S.C.C.A.N. 2348, 2349.

91. Roughly 40 percent of all e-mail was spam in 2003. Jonathan Krim, *Spam's Cost to Business Escalates*, WASH. POST, Mar. 13, 2003, at A1.

92. DAVID FERRIS, RICHI JENNINGS & CHRIS WILLIAMS, FERRIS RES., THE GLOBAL ECONOMIC IMPACT OF SPAM, 2005, at 6 (David Ferris ed., 2005). According to the Ferris Research study, the annual global cost of spam was $50 billion in 2005, $17 billion of which is attributable to the United States. *Id.* The loss is spread between lost productivity, the costs of replacement of powerful servers and increased bandwidth which companies are forced to buy, the lost time diverted for implementation, and the cost of providing help-desk support to annoyed users. *Id.* Spam has become so prevalent that Internet company Commtouch's research lab has created a spam cost calculator including inserts for number of employees, average annual salary, average daily e-mail per recipient, and average percentage of spam per e-mail recipient. *See* Commtouch, Spam Cost Calculator, http://www.commtouch.com/site/ResearchLab/Calculator.asp (last visited July 31, 2008).

93. Zitter, *supra* note 89, at 10.

94. *See* Celeste Biever, *Spam Being Rapidly Outpaced by 'Spim,'* NEW SCIENTIST, Mar. 26, 2004, http://space.newscientist.com/article/dn4822; Anita Hamilton, *You've Got Spim!*, TIME, Jan. 25, 2004, http://www.time.com/time/magazine/article/0,9171,582320,00.html.

95. *See* Eric Zorn, *R U Ready for a Plague of Instant Messages?*, CHI. TRIB., Aug. 5, 1999, at N1.

96. *Messaging Spam Heads for Your PC* (BBC Radio Five Live broadcast Aug. 23, 2004), *available at* http://news.bbc.co.uk/2/hi/technology/3581148.stm [hereinafter *Radio Broadcast*].

in the messaging program or to employ the computer as a "zombie" to launch malicious attacks on other computers.[97] SpIM presents particularly invidious pitfalls to the unsuspecting user, as messages "from friends" can contain links to annoying and harmful schemes and even "away messages" can contain virus-ridden code.[98]

SpIM is growing at an alarming rate. The number of spIM messages has reached the billions, and is projected to grow at a rate three times that of spam.[99] According to a survey by the Pew Internet & American Life Project, one in every two instant-messaging users in the United States has received some kind of spIM.[100] Experts warn that due to the "immediacy of instant messaging and its growing popularity with businesses and home users," spIM will likely be the next area of development for those looking to corrupt the security of the cyber environment.[101]

3. Phishing

The U.S. Department of Justice defines phishing as the "creation and use of e-mails and Web sites—designed to look like e-mails and Web sites of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames or passwords."[102] A phishing crime often begins with a "spoofed" e-mail that appears to be from a trusted source. The e-mail can contain a link taking the user to a webpage that is visually identical to a trusted source webpage;[103] there "phishers" entice users to enter their passwords, credit card, or other private information into the false web page, after which

97. Biever, *supra* note 94. If a user activates the code in the instant message, the spimmer can employ the unsuspecting user's buddy list to send messages to all of their contacts; this impersonation ability makes spIM particularly dangerous. *See Radio Broadcast*, *supra* note 96.

98. *See* AOL Instant Messenger Online Safety/Security FAQ, http://www.aim.com/help_faq/security/faq.adp#share (last visited July 31, 2008).

99. *See* Biever, *supra* note 94; Linda Stern, *Corporate Spim Is No LOL Matter*, NEWSWEEK, May 9, 2005, at 36.

100. EULYNN SHIU & AMANDA LENHART, PEW INTERNET & AM. LIFE PROJECT, HOW AMERICANS USE INSTANT MESSAGING 10 (2004), *available at* http://www.pewinternet.org/pdfs/PIP_Instantmessage_Report.pdf.

101. Will Sturgeon, *U.S. Makes First Arrest for Spim*, CNET NEWS, Feb. 21, 2005, http://www.news.com/U.S.+makes+first+arrest+for+spim/2100-7355_3-5584574.html. *See also* Peter Griffiths, *Internet Criminals to Step Up "Cyberwar" in 2007*, REUTERS, Dec. 12, 2006, http://news.soft32.com/internet-criminals-to-step-up-cyberwar-in-2007_3015.html.

102. BINATIONAL WORKING GROUP ON CROSS-BORDER MASS MKTG. FRAUD, REPORT ON PHISHING 3 (2006), http://www.usdoj.gov/opa/report_on_phishing.pdf.

103. *See* 151 CONG. REC. S1796, 1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

phishers loot the users' accounts or steal their identities.[104]

Original phishing schemes were easily detectible, as they were frequently laden with typographical, grammatical, and spelling errors, and contained entirely numerical hyperlinks that indicated the page to which they linked was not legitimate.[105] The e-mails were also often sent indiscriminately, reaching many users who never interacted with the business in question, making it easier for users to distinguish a phish from a legitimate e-mail. However, recent phishing schemes have grown more sophisticated. Phishing e-mails now tend to be grammatically correct[106] and targeted toward known customers of the impersonated business.[107] Phishers have also developed a technique known as "pharming" which masks the Uniform Resource Locator ("URL") of a fraudulent site as the URL of the real company's site.[108] Phishing crimes are becoming increasingly more dangerous as identity thieves crawl through networked cyberspace, picking up personal details to strengthen their "phish."[109] Data suggests that phishers now have a 5 percent success rate of tricking the unwary user into falling for the scheme,[110] whereas the response rate for regular spam is 0.01 percent.[111]

Phishing is a complex crime because it "almost always involves two separate acts of fraud. The phisher first 'steals' the identity of the business it is impersonating and then acquires the personal information of the unwitting customers who fall for the impersonation."[112] There are therefore two victims of a phishing scheme: the unsuspecting user who falls for the phish, and the business whose identity is stolen and copied.

104. *See* Jennifer Lynch, Note, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L. J. 259, 259 (2005); Editorial, *We're Just Phish to Them*, MILWAUKEE J. SENTINEL, Mar. 12, 2006, at A14.

105. *See* Jefferson Lankford, *The Phishing Line*, ARIZ. ATT'Y, May 2005, at 14.

106. *See* ANTI-PHISHING WORKING GROUP, EVOLUTION OF PHISHING ATTACKS 8–9 (2005), http://www.antiphishing.org/Evolution%20of%20Phishing%20Attacks.pdf.

107. *See* Lankford, *supra* note 105; Timothy L. O'Brien, *Gone Spear-Phishin'; For a New Breed of Hackers, This Time It's Personal*, N.Y. TIMES, Dec. 4, 2005, at A1 (describing a technique known as "spear fishing," which can be alarmingly specific and accurate).

108. *See generally* Lynch, *supra* note 104, at 269 (describing sophisticated techniques, including pharming, used by spammers).

109. Griffiths, *supra* note 101.

110. ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT (2005), http://www.antiphishing.org/reports/APWG_Phishing_Activity_Report-January2005.pdf (last visited Mar. 2007).

111. Laura Sullivan, *Internet "Phishing" Scams on the Rise*, L.A. TIMES, Mar. 22, 2004, at C2.

112. Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation Versus Technology*, 2005 DUKE L. & TECH. REV. 0006, ¶ 3, http://www.law.duke.edu/journals/dltr/articles/2005dltr0006.html.

This rapidly growing class of Internet fraud causes both short-term loss and long-term economic damage,[113] the costs of which will only increase as the number of new phishing scams continues to climb.[114] The biggest long-term effect is the loss of public trust in the Internet, which in turn undermines the integrity of e-commerce.[115] Overall, estimated losses caused by phishing are in the billions;[116] in terms of cost to consumers, estimates range from $500 million to $2.4 billion.[117]

4. Other Internet Fraud

Other types of Internet fraud include business opportunity "work at home" schemes,[118] which require individuals to pay money for the opportunity to earn money by working at home;[119] investment schemes;[120] and identity theft and fraud.[121]

III. CURRENT CYBER CRIME LAW

Before the widespread proliferation of computers in American life, the amount of property susceptible to criminal activity was, to some extent, limited by the constraints of the physical world; for example, a thief can

113. *See* 151 CONG. REC. S1796, 1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

114. Phishing attacks have increased by an average of 30 percent each month since July 2004. THE ANTI-PHISHING WORKING GROUP, *supra* note 110.

115. 151 CONG. REC. S1796, 1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

116. *Id.*

117. *Good News: "Phishing" Scams Net Only $500 Million*, CNET NEWS, Sept. 29, 2004, http://news.cnet.com/2102-1029_3-5388757.html (summarizing studies from Truste, Inc. and Gartner, Inc.).

118. *See* Rusch, *supra* note 84.

119. Internet Fraud, *supra* note 77.

120. *Id. See, e.g.*, CHRISTOPHER M.E. PAINTER, U.S. DEP'T OF JUSTICE, TRACING IN INTERNET FRAUD CASES: PAIRGAIN AND NEI WEBWORLD, (2005), *available at* http://www.usdoj.gov/criminal/cybercrime/usamay2001_3.htm; Press Release, SEC, Three Settle SEC Charges in NEI Webworld Internet Stock Manipulation Case; Two Sentenced to Prison in Related Criminal Prosecution (Jan. 23, 2001), *available at* http://www.sec.gov/litigation/litreleases/lr16867.htm. *See also* Rusch, *supra* note 84.

121. Although identity theft has become the fastest growing crime in America, it will not be discussed in great detail here, except in relation to phishing crimes. For more information on identity theft see *Fighting Identity Theft—the Role of FCRA: Hearing before the H. Subcomm. on Fin. Instits. and Consumer Credit*, 108th Cong. (2003) (statement of Rep. John B. Shadegg). *See also* SEAN B. HOAR, U.S. DEP'T OF JUSTICE IDENTITY THEFT: THE CRIME OF THE NEW MILLENNIUM (2001), *available at* http://www.cybercrime.gov/usamarch2001_3.htm (applying the statute). Identity theft "affects as many as 10 million Americans at a price tag of $55 billion to American businesses and individuals." Cassell Bryan-Low, *As Identity Theft Moves Online, Crime Rings Mimic Big Business*, WALL ST. J., July 13, 2005, at A1. Identity theft is particularly costly to individuals because, while banks typically compensate them for losses, victims still must spend time and money repairing "the havoc wreaked on their personal records and finances and often end up paying legal fees to do so." *Id.*

only carry so many television sets or rob so many houses before, inevitably, someone notices. However, as the public eagerly embraced computers in the 1990s, a new arena for criminal mischief and theft appeared, the dimensions of which had never before been imagined. As thieves were able to utilize modern technology to steal or damage extraordinary amounts of property,[122] Congress was forced to search for legislative solutions that would "prove suitable to the society of computer users that it foresees in the immediate future."[123]

Congress was presented with a number of options: rely on laws for physical property to prosecute computer-based crimes, rely on the states to prosecute, or pass federal statutes specifically targeting computer-based crime. Initially, Congress chose the first option, relying primarily on existing code sections.[124] Yet, as computer use expanded, legislators agreed that greater action was needed.[125] The unique problem and concomitant threat to public welfare created by the introduction of computers caused Congress to recognize that the "clear shift to a borderless, incorporeal environment and the increased risk that information will be stolen and transported in electronic form" would be impossible to address by relying on older laws, written to protect physical property.[126]

Over the past two decades, Congress has taken a piecemeal approach in addressing the ever-evolving cyber environment, passing a slate of new legislation to combat specific crimes and reworking current legislation to incorporate other crimes. This approach was intended to enable prosecutors and law enforcement to "swiftly trace a cyber attack back to its source and appropriately prosecute"[127] without having to continually parse and rework the entire U.S. Code.[128] Generally, the legislation was intended to permit prosecutors and legislators to garner a better understanding of the scope of cyber crime, and to derive more reliable statistics regarding cyber crime to "better measure existing harms, anticipate trends, and determine the need

122. *See* Griffith, *supra* note 4, at 454.

123. *Id.* at 455 (*citing* S. REP. No. 99-432, at 2–3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2479).

124. Prior to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Congress had relied on the mail and wire fraud statutes to combat computer crime. *See* Deborah F. Buckman, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. Fed. 101, 112 (2001).

125. *See* Griffith, *supra* note 4, at 471.

126. *Legislative Analysis*, *supra* note 27. *See* United States v. Brown, 925 F.2d 1301, 1307–09 (10th Cir. 1991) (highlighting the difficulty of prosecuting theft of intellectual property—namely source code—under current physical property sections).

127. Kyl Statement, *supra* note 18.

128. *Legislative Analysis*, *supra* note 27.

for further legislative reform."[129] This Note does not question Congress's approach, but offers additional ways to supplement the existing scheme.

As with all criminal law, the specifics of the crime determine which statutory section is applicable. Criminalizing measures for cyber crime can be arranged in roughly similar categories as to the crimes they prohibit: those statutes that are geared toward crimes targeting the computer and networks, and those geared toward using such systems as an instrumentality of a crime.

A. CRIMES AGAINST COMPUTERS AND NETWORKS

1. Hacking

The primary statute used to prosecute hacking crimes—including DDoS attacks and extortionate hacking—is 18 U.S.C. § 1030.[130] By prohibiting unauthorized access to computer systems, this statute enables prosecutors to pursue crimes that attack computers and networks and the information contained within them.

The current statute is the result of nearly twenty years of evolving responses to the cyber crime threat. The statute was first passed in 1984 as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ("1984 Act").[131] This Act prohibited computer-related activity in only a few very narrow areas. The 1984 Act made it a felony to knowingly access a computer without authorization or in excess of authorization to obtain federal government information, and a misdemeanor to access a computer without, or in excess of authorization to obtain financial records or in order to use, modify, destroy or disclose federal government information.[132] Although hailed as the first important step in fighting cyber crime, the lack of clarity in defining key terms, inability to react to changing technology, and failure to combat noninterstate computer crime ultimately doomed the success of the 1984 Act.[133]

Industry analysts and legislators at the time felt it was necessary to expand the 1984 Act to protect the growing number of private sector

129. *Id.*

130. 18 U.S.C. § 1030 (2000 & Supp. IV 2004).

131. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, ch. 21, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2000)).

132. *Id.*

133. *See* Griffith, *supra* note 4, at 466–73 (providing an indepth analysis of the 1984 Act and its failings).

computers used in interstate commerce. Congress attempted to address the shortcomings with the CFAA,[134] which eliminated ambiguous language, defined additional terms, restructured the offenses, and expanded the scope to include new and significant computer crimes.[135] The CFAA sought to increase the deterrent effect of the statute on cyber criminals by closing loopholes inadvertently created in the 1984 Act.[136]

Computer technology continued its rapid evolution and the CFAA was forced to evolve alongside it. In recognition of the increase of the prevalence of computers and networks in the United States and the attendant opportunities for computer crime, in 1994, Congress broadened the focus of the CFAA from the technical concept of unauthorized access to a computer system to a focus on the defendant's harmful intent and resulting harm.[137] Congress also reduced the threshold requirement to $1000 for jurisdiction over crimes of intentional access to a government computer.[138]

In 1996, the statute was substantially reorganized,[139] and again broadened by two main provisions: first, Congress relaxed the interstate threshold requirement to a "computer used in interstate commerce or communications,"[140] recognizing the inherently interstate nature of the

134. CFAA, sec. 2, § 1030(a)(1)–(3), (b), (e), 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2000)).

135. *See* Joseph B. Tomkins, Jr. & Frederick S. Ansell, *Computer Crime: Keeping Up with High Tech Criminals*, CRIM. JUST., Winter 1987, at 30, 32. Specifically, the CFAA raised the criminal intent standard to "intentionally" from "knowingly" for 18 U.S.C. §1030(a)(2); clarified what the 1984 Act means by "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" by replacing it with "exceeds authorized access"; removed redundant clauses that were covered by 18 U.S.C. §1030(a)(4); and refined the measurement mechanism for calculating fines under the act. CFAA, § 2(a)(1)–(b)(1),(c),(f)(1)–(7), 100 Stat 1213, 1213 (1986).

136. *See* Griffith, *supra* note 4, at 484.

137. *See* 139 CONG. REC. S16421-03 (daily ed. Nov. 19, 1993) (statement of Sen. Leahy). Prior to the 1994 amendment, amendments in 1989 and 1990 broadened the scope of the CFAA to include applicability to "institutions," not just "banks" in § 1030(e)(4), Financial Institutions Reform, Recovery, and Enforcement Act of 1989, Pub. L. No. 101-73, § 962(a)(5)(A)–(C), 103 Stat. 183, 502, and to include "commonwealth[s]" of the United States alongside "possession[s] or territory of the United States" in § 1030(e)(3). Crime Control Act of 1990, Pub. L. No. 101-647, § 1205(e), 104 Stat. 4789, 4831.

138. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001(b), 108 Stat. 1796, 2097–98.

139. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(2)(A)–(D), 110 Stat. 3488, 3492–93 (codified as amended at 18 U.S.C. §§ 1831–39 (2000)).

140. CFAA, 18 U.S.C. § 1030(a)(5) (Supp. IV 2004). Prior to this amendment, § 1030(e)(2)(A) read: "which is one of two or more computers use in committing the offense, not all of which are located in the same state." Economic Espionage Act § 201(4)(A)(iii). Congress also inserted a provision for crimes committed internationally, including in the Act "a computer located outside the United States

Internet (and perhaps foreseeing the future need not to limit the crime to only computer-to-computer transmissions); and second, Congress replaced the phrase "federal interest computer" with the broader phrase "protected computer"[141] to accommodate the growing legion of computers in the home and workplace.

Congress conceded the changing nature of computers and Internet technology; as the Senate Report on the 1996 amendments noted:

> [a]s intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime . . . . As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime.[142]

In its current form,[143] the CFAA addresses the "interstate transmission of threats directed against computers and computer networks" and applies to "any interstate or international transmission of threats against computers, computer networks, and their data and programs, whether the threat is received by mail, a telephone call, electronic mail, or through a computerized message service."[144]

The CFAA, § 1030(a)(5), is the primary tool used to investigate and

that is used in a manner that affects interstate or foreign commerce or communication of the United States." Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, § 814(d)(1), 115 Stat. 272, 384.

141. *See* Economic Espionage Act § 201(4)(A)(i); *Legislative Analysis*, *supra* note 27. *See also* Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d. 926 (E.D. Tex. 1999). Congress also substituted "*any nonpublic* computer of a department or agency" for "any computer of a department or agency." This change helped to better define the scope of this section. § 201(1)(A).

142. National Information Infrastructure Protection Act of 1995, S. REP. NO. 104-357, pt. II, at 5 (1996).

143. The CFAA was further amended in 2001. The 2001 amendments were largely formatting changes; however, a few important substantive changes were made as well. The definition of damages was changed to its current meaning from, "any impairment to the integrity or availability of data, a program, a system, or information." USA Patriot Act § 814(d)(3). The prior law required that the damages "cause loss aggregating at least $5,000 in value during any 1-year period," modify medical treatment "of one or more individuals," cause "physical injury to any person," or "threate[n] public health or safety." Economic Espionage Act § 201(2)(A)–(D). While the substantive text of the earlier Act has been carried over to the current Act in relation to § 1030(a)(4) and (a)(5), this change in 2001 eliminated the monetary minimum for unauthorized access to government computers and extortionate acts. In the 2001 amendment, Congress also refined the civil action provision of the CFAA, limiting damages to economic damages only, and creating a safe harbor for manufacturers in that "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware." USA Patriot Act § 814(e).

144. *Legislative Analysis*, *supra* note 27.

prosecute hacking crimes.[145] Subsection 1030(a)(5)(A)(i) applies to anyone who "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."[146] This section covers most hacking crimes. For example, a hacker who infiltrates a system and in some way damages the system or the data on it faces liability under this section of the criminal code. Under this subsection, a hacker faces dual liability in a DDoS attack (to both the "zombie" system and the targeted system) since the attacker causes the transmission of information, packets, and code with the intent to harm both systems.

Unintentional, unauthorized access is also covered. Section 1030(a)(5)(A)(ii) creates a felony for unauthorized access that "recklessly" causes damage to a protected computer.[147] This lower culpability standard is applicable to hacking crimes in which damage is caused inadvertently. If a prosecutor is still unable to make a case, § 1030(a)(5)(A)(iii),[148] which prohibits unauthorized access that negligently causes damage, can be used. Although it is hard to imagine an example of such negligence, without this provision, Congress would implicitly condone hacking into a computer or system so long as no damage occurred. Perhaps, in recognition of the importance of information on its own without economic damage, Congress found it necessary to include this provision. Activation of § 1030(a)(5)(i)–(iii) requires "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."[149]

Section 1030(a)(5) is similar to § 1030(a)(4), which criminalizes the access and intentionally fraudulent use of a protected computer.[150] Section 1030(a)(4) is also triggered only if the "conduct furthers the intended fraud and obtains anything of value" in excess of $5000.[151] This section is often employed to prosecute hacking crimes which involve the obtaining or destruction of some measurable thing.

Sections 1030(a)(4) and 1030(a)(5)(i)–(iii) both require a showing of

145. 18 U.S.C. § 1030(a)(5) (Supp. IV 2004).
146. *Id.* § 1030(a)(5)(A)(i).
147. *Id.* § 1030(a)(5)(A)(ii).
148. *Id.* § 1030(a)(5)(A)(iii).
149. *Id.* § 1030(a)(5)(B)(i).
150. *Id.* § 1030(a)(4)–(5) (2000 & Supp. IV 2004).
151. *Id.* § 1030(a)(4) (2000).

damages greater than $5000;[152] § 1030(a)(4) requires the value of the thing obtained in the hack be greater than $5000[153] and § 1030(a)(5) requires the "loss" be greater than $5000.[154] Although this damages requirement is important as an element, jurisdictional threshold, and sentencing factor,[155] prosecutors have found the $5000 loss requirement of § 1030(a)(5) to be both "difficult to establish and an impediment to investigation."[156]

The CFAA provides a broad definition for "damages" that leaves much ambiguous. The statutory definition is unclear, suggesting only damage that interferes with the integrity of a computer system.[157] The statute does provide specific examples of foreseeable damages, such as "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[158]

The ambiguous parameters of this element of a hacking crime have forced courts to further interpret the gray areas within damages and loss. Courts have found loss to refer to the costs that are the "natural and foreseeable result" of a violator's conduct, including monetary loss for system destruction, as well as expenses related to restoring data, and creating a better, more secure system.[159] Courts have not required a loss to be physical damages (in the traditional sense) in order to fall within the purview of the act;[160] even if no actual physical damage is caused to a data system, the $5000 threshold may be met if a cost is incurred as a result of a violation of the CFAA.[161] Examples of losses accepted by the courts to fall within the parameters of the CFAA are damage assessment and remedial

152. While the 2001 amendments to the CFAA allow for contemplation of intangible harms from unauthorized access to data systems, they still require fact finders to express the harms in economic terms that total $5000 while failing to suggest how an economic calculation should be conducted.

153. 18 U.S.C. § 1030(a)(4).

154. *Id.* § 1030(a)(5).

155. Damages are also a major factor in sentencing and are fundamental to restitution. Section 2B1.1 of the U.S. Sentencing Guidelines applies to violations of 18 U.S.C. § 1030; it has a base level offense of six, and dictates a two to thirty upward adjustment for loss. U.S. SENTENCING COMM'N, 2007 FEDERAL SENTENCING GUIDELINES MANUAL § 2B1.1(a)(2)–(b)(1).

156. *See* Sinrod & Reilly, *supra* note 33, at 200.

157. 18 U.S.C. § 1030(e)(8) (Supp. IV 2004).

158. *Id.* § 1030(e)(11).

159. *See* United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000).

160. 18 U.S.C. § 1030(e)(8)(A) (2000); 18 U.S.C. § 1030(g) (Supp. IV 2004). *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 (S.D.N.Y. 2001).

161. 18 U.S.C. § 1030(e)(8)(A). *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584 (1st Cir. 2001).

measures,[162] loss of business and goodwill,[163] and the expense of technicians' salaries paid to fix the problem.[164] However, courts have interpreted the CFAA to exclude as compensable loss the lost revenues,[165] travel costs,[166] and lost competitive advantage a business or individual suffers in the wake of a cyber attack.[167]

Extortionist hacking is often prosecuted under § 1030(a)(7), which prohibits "any communication containing any threat to cause damage to a protected computer" with the "intent to extort from any person any money or other thing of value" in interstate or foreign commerce.[168] Although the section requires the intent to extort some thing "of value," unlike § 1030(a)(4)–(5), the statute does not specify any threshold value.[169] Prosecutors often employ this statute in conjunction with the Hobbs Act[170] if the hacking attack contains a threat of "physical violence to any person or property,"[171] and with 18 U.S.C. § 875 if the intent to extort includes a threat to injure property or reputation.[172]

Hacking crimes where the target is the U.S. government often fall under § 1030(a)(1), which protects against intentional access to government computers in order to obtain confidential or classified information.[173] This section often works in conjunction with § 1030(a)(3), which concerns access that interferes with the use or the ability to use a

162. *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 526 (S.D.N.Y. 2004).

163. *See* Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 934–35 (9th Cir. 2004).

164. *See Middleton*, 231 F.3d at 1214 (finding that the hourly wage of bank employee can be included because it would have cost the bank a similar fee to hire an outside consultant); United States v. Sablan, 92 F.3d 865, 870 (9th Cir. 1996) (finding that inhouse employees' salaries can be included in calculation of loss even though they were not paid extra to fix the damages).

165. 18 U.S.C. § 1030(a)(5)(B)(i), (g) (Supp. IV 2004). *See* Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 472 (S.D.N.Y. 2004).

166. Nexans Wires S.A. v. Sark-USA, Inc., 166 F. App'x. 559, 563 (2d Cir. 2006). *See* 18 U.S.C. § 1030(e)(11).

167. *See* Civic Ctr. Motors, Ltd., v. Mason St. Import Cars, Ltd., 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005) (holding that damages here—a competitor gaining an advantage and the original business wasting its investment in the development and compilation of a database—stemming from unauthorized access to a business' computer database were not compensable).

168. 18 U.S.C. § 1030(a)(7).

169. *Id.*

170. Hobbs Act, 18 U.S.C. § 1951 (2000).

171. *See id.* § 1951(a).

172. *See* 18 U.S.C. § 875 (2000). The Interstate Nexus requirement is met by the inherently interstate nature of the Internet medium. *Id.* § 875(d). It is still unclear in both statutes whether "'property' includes the unimpaired operation of a computer or the unrestricted access to the data or programs stored in a computer and its peripheral equipment." *Legislative Analysis*, *supra* note 27.

173. 18 U.S.C. § 1030(a)(1) (2000).

government computer.[174] A prosecution under this section requires that a user "intentionally" access an exclusively government computer, but does not currently require any damages be alleged.[175]

The CFAA's application is not limited to hacking crimes. Section 1030(a)(2) is used to prosecute economic espionage.[176] This section prohibits intentional access and obtaining of information without, or in excess of, authorization from a financial institution, the federal government, or any "protected computer involved in interstate or foreign communications."[177] This section is primarily concerned with the protection of information, and can be used to prosecute theft of trade secrets.[178] The CFAA can also be used in prosecutions for access device fraud.[179] Although this section of the CFAA has limited application to hacking crimes, this section can be used in conjunction with § 1029 to prosecute access device theft.[180]

Criminal acts charged under the CFAA are punishable by up to twenty-years imprisonment or a fine, or both. The CFAA also provides a civil remedy.[181] Section 1030(g) allows "[a]ny person who suffers damage or loss by reason of a violation of this section" to bring a civil action against the violator for injunctive or equitable relief, including compensatory damages.[182] A viable civil action requires that the violative conduct have caused either an excess of $5000 in damages within a year, or one of the noneconomic damages set forth in § 1030(a)(5)(B)(i)–(v).[183] Standing in a civil action is not limited to the owner of an affected

174. *Id.* § 1030(a)(3).

175. *Id.* This was not always the case; the original 1984 Act *did* require damages of at least $1000 to allege the crime. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2000)).

176. 18 U.S.C. § 1030(a)(2).

177. *Id.* § 1030(a)(2)(c).

178. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (stating that in the context of a civil action "'[t]he premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions'" (citing S. REP. NO. 99-432, at 6 (1986))).

179. Section 1030(a)(6) prohibits knowingly trafficking, that is, to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of," 18 U.S.C. § 1029(e)(5), "any password or similar information through which a computer may be accessed without authorization" with the intent to defraud. 18 U.S.C. § 1030(a)(6).

180. *See* discussion *infra* Part III.A.4.

181. 18 U.S.C. § 1030(g) (Supp. IV 2004). *See* Fiber Sys. Int'l v. Roehrs, 470 F.3d 1150, 1156 (5th Cir. 2006).

182. 18 U.S.C. § 1030(g).

183. *Id.* ("Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.").

computer; the CFAA provides a cause of action against any person who intentionally accesses a computer and information.[184] If that information belongs to a person other than the one who owns the computer, that third party has standing to bring a claim.[185]

A bill to expand coverage of the CFAA is currently pending in Congress.[186] This bill would extend the jurisdiction of the Act to cover not only computers "used in" interstate commerce but also those "affecting" computers used in interstate commerce; it would also eliminate the requirement of involving interstate commerce for protected computers.[187] The proposed bill would also broaden the protected elements under § 1030(a)(2) and create a crime of "conspiracy" to commit a cyber crime.[188] The bill was referred to the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee in March of 2007, and as of July 2008 remains in committee.[189]

2. DDoS Attacks

DDoS attacks are generally prosecuted under the CFAA. The CFAA is well suited for the prosecution of DDoS attacks since these sorts of attacks include unauthorized or excessive access to another computer. Prosecutions under this statute are still subject to the $5000 threshold requirement for damages; however, in a DDoS attack these damages are often easier to allege than in a single hacking crime. For example, a man recently pled guilty to waging a DDoS attack against eBay.[190] From July through August 2003, Anthony Scott Clark accumulated approximately twenty thousand "zombie computers" by using a worm program that took advantage of computer vulnerability in the Windows Operating System.[191] When instructed to do so, the "zombies" launched DDoS attacks focused on the nameserver for eBay.com at computers or computer networks connected to the Internet. As a result, the DDoS attack critically impaired the infected

184. *Id.*

185. 18 U.S.C. § 1030(a)(2)(C), (g) (2000 & Supp. IV 2004). *See* Theofel v. Farley-Jones, 359 F.3d 1066, 1078 (9th Cir. 2004).

186. H.R. 836, 110th Cong. (2007).

187. *Id.* § 3.

188. *Id.* §§ 2, 6.

189. *See* Status Report, H.R. 836, 110th Cong., http://www.thomas.gov (search "Bill Number" for "H.R. 836"; then follow "Bill Summary & Status" hyperlink).

190. *See* Press Release, U.S. Attorney's Office, Man Pleads Guilty to Infecting Thousands of Computers Using Worm Program then Launching them in Denial of Service Attacks (Dec. 28, 2005), *available at* http://www.cybercrime.gov/clarkPlea.htm [hereinafter Man Pleads Guilty].

191. *Id.* The "zombies" were directed to a password-protected Internet Relay Chat server, where they connected, logged in, and waited for instructions. *Id.*

computers and eBay.com.[192] Clark pled guilty to 18 U.S.C. § 1030(a)(5)(A)(i) and (a)(5)(B)(i), and faces up to ten years in prison.[193] Because his attack was aimed toward shutting down eBay, a sizeable target, a case for $5000 in damages could be made relatively easily. If the target was a smaller site or personal network, the damages may not be quite as easily alleged.

3. Theft of Trade Secrets

The Economic Espionage Act of 1996 makes theft or misappropriation of trade secrets a federal crime.[194] The Act prohibits the wrongful copying or otherwise controlling of trade secrets with the intent to "benefit any foreign government, foreign instrumentality or foreign agent,"[195] or to benefit economically "anyone other than the owner thereof."[196] "Trade secret[s]" include "all types of financial, business, scientific, technical, economic, or engineering information, whether tangible or intangible, and regardless of the means by which the information is stored, compiled, or memorialized."[197]

Prior to the 1996 Act, the criminal sanctions for trade-secret misappropriation were found under existing statutes;[198] in reality, regulation of economic espionage was left principally to state legislatures

192. *Id.*

193. *Id.*

194. Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39 (2000).

195. *Id.* § 1831(a)(1)–(2).

196. *Id.* § 1832(a)(1)–(2).

197. H.R. REP. NO. 104-788, at 3 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 4021, 4022. For proprietary information to be a trade secret: (1) the owner of the information must "have taken reasonable measures to keep such information secret," and (2) "the information derives independent economic value, actual or potential, from not being generally known" to the public, and "not being readily ascertainable" through legal means. *Id.* at 2.

198. Prior to the passage of this law, federal authorities relied principally on the Interstate Transportation of Stolen Property Act (ITSPA), 18 U.S.C. § 2314 (2000), which was passed in the 1930s in an effort to prevent criminals from moving stolen property across state lines to evade local and state law enforcement. H.R. REP. NO. 104-788, at 6. ITSPA relates to physical property—"goods, wares, or merchandise." 18 U.S.C. § 2314. However, this provision was difficult to apply to Internet property because it is intangible "intellectual" property that is not by its nature transported from place to place. 18 U.S.C. § 2314; H.R. REP. NO. 104-788, at 4–5. Courts too have been reluctant to extend this statute to nonphysical property, believing the physical property of "goods, wares or merchandise" to be a limitation "imposed by the statute itself, and [it] must be observed." United States v. Brown, 925 F.2d 1301, 1308–09 (10th Cir. 1991). Given the limitations of the ITSPA, the government has used other statutes to prosecute trade secret theft, which have proved somewhat limited in their use. *See* H.R. REP. NO. 104-788, at 6. For example, charging a crime under the mail or wire fraud statute requires proof that the mails, or wire radio, or television technology, respectively, were use to commit the crime; this can present an obstacle in some cases. *Id.*

who passed separate and largely inconsistent laws.[199] While many states had rarely used civil remedies, only a handful of states had any criminal laws regarding economic espionage, and of those who did, most created misdemeanor violations that, as a result, received little attention from state prosecutors.[200]

In 1996, Congress recognized two competing trends: on one hand, the proliferation of computers made intangible assets—the intellectual property embodied by the computer systems and software and the information available via the computer and networks—incredibly valuable.[201] The increasing prevalence of computers in the home and business made intangible assets vital to the prosperity of companies. It was expected that "[a]s the nation move[d] into the high-technology, information age, the value of these intangible assets [would] only continue to grow."[202] Indeed, whole new businesses, such as Google, have been created from purely intellectual property associated with the Internet and are now worth hundreds of billions of dollars. On the other hand, the growth of personal computers made these important assets vastly easier to misappropriate. As computers spread in society and the computer technology for the creation and storage of information advanced, so too did the methods for "rapid and surreptitious duplications of the information."[203] Thus, ironically, "the very conditions that [made] this proprietary information so much more valuable [made] it easier to steal."[204]

The changing way in which intangible assets were created and stored, as well as the gaps in federal law and the inability of states to cover the ground, "underscore[d] the importance of developing a systematic approach to the problem of economic espionage."[205] Section 1030(a)(2), which prohibits intentional access and obtaining of information without, or in excess of, authorization from a financial institution, the federal government or any "protected computer involved in interstate or foreign communications," can also be used, alone or in tandem with the Economic Espionage Act, to prosecute the theft of trade secrets when the access to a

199. *See* Arnold B. Silverman, *The Theft of Trade Secrets Is a Federal Crime*, JOM, July 2008, at 63.

200. H.R. REP. NO. 104-788, at 6.

201. *Id.* at 4–5.

202. *Id.* at 4.

203. *Id.* at 5. Intangible, intellectual, assets are particularly good targets for theft for a number of reasons: (1) they cost a great deal of money to develop independently; (2) they are immensely valuable; and (3) theft of such assets is not bound by physical limitations. *Id.*

204. *Id.* at 4–5.

205. *Id.* at 7.

protected computer yields confidential proprietary information.[206]

4. Access Device Fraud

The primary statute tailored to access device fraud is 18 U.S.C. § 1029.[207] This statute makes it illegal to "knowingly and with intent to defraud" produce, use, or traffic "in one or more counterfeit access devices," or traffic in or use "one or more unauthorized access devices during any one-year period," if by such conduct the thief "obtains anything of value aggregating $1,000 or more during that period."[208]

This statute was first enacted in 1984 in response to the growing importance of credit cards and other access devices, and in recognition of increasingly sophisticated criminal activity in this area.[209] The 1984 statute was designed to "close the loopholes of already existing legislation"—the Truth in Lending Act[210] and the Electronic Funds Transfer Act[211]—which it did by allowing the aggregation of loss. Section 1029 is somewhat of a "consequential" statute; it does not criminalize the hack itself, but rather criminalizes the subsequent use of the fruits of the hack.[212]

The current statute still primarily criminalizes theft of credit and debit card information and related identity theft; however, as this type of criminal behavior migrates to the cyber world, this statute is increasingly used, often in conjunction with 18 U.S.C. § 1030(a)(6), to protect against the theft of online access devices such as passwords and other online information.[213]

206. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, THEFT OF COMMERCIAL TRADE SECRETS—18 U.S.C. §§ 1831-1839, at 173–74 (2004), http://www.usdoj.gov/criminal/cybercrime/ipmanual/04ipma.pdf

207. 18 U.S.C. § 1029 (2000).

208. *Id.* § 1029(a)(1)–(2).

209. H.R. REP. No. 98-130, at 1–4 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3689–90.

210. Truth in Lending Act, 15 U.S.C. §§ 1601–67 (2000).

211. Electronic Funds Transfer Act, 15 U.S.C. § 1693 (2000). *See* United States v. Ryan, 894 F.2d 355, 357 (10th Cir. 1990). These statutes prohibited "fraudulent use of credit cards and debit instruments"; however, they were limited by the common requirement of $1000 worth of activity on each instrument within one year. *Id.* Industry representatives testified that "organized groups generally stay just under this amount but use many different counterfeit or stolen cards or debit instruments." *Id.* (quoting H. REP. NO. 98-894, at 5 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3691).

212. *See* 18 U.S.C. § 1029(a)(2).

213. *See* CHARLES DOYLE, CONG. RESEARCH SERV., CYBERCRIME: A SKETCH OF 18 U.S.C. 1030 AND RELATED FEDERAL CRIMINAL LAWS 4–5 (2008), http://fpc.state.gov/documents/organization/103707.pdf.

5. Wiretapping

The original Federal Wiretap Act was enacted in 1968 as part of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) "in an effort to better articulate a balance between the privacy rights of individuals and the legitimate needs of law enforcement."[214] This Act covered only the intentional interception of wire and oral communications.[215] As other modes of communication, such as mobile phones, cordless phones, and data services grew in popularity in the mid-1980s, Congress amended the original Act with the Electronic Communications and Privacy Act of 1986 ("ECPA") to include electronic communications within the original intended protections of the Federal Wiretap Act.[216]

Title I of the ECPA defines electronic communications as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[217] The ECPA prohibits the intentional and attempted interception of electronic communications,[218] as well as the use of illegally obtained electronic communications.[219]

Title II of the ECPA aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications.[220] Specifically, Title II provides that anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided; or . . . intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system

214. Shana K. Rahavy, *The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home*, 88 J. OF HIGH TECH. L. 87, 87–88 (2003). *See* Omnibus Crime Control and Safe Streets Act of 1968, S. REP. NO. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2113–15 (current version at 18 U.S.C. § 2511(1) (2000)).

215. S. REP. NO. 90-1097.

216. 18 U.S.C. § 2510 (2000).

217. *Id.* § 2510(12).

218. 18 U.S.C. § 2511(1)(a) (2000). *See* Thomas R. Greenberg, *E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219 (1994). The wiretapping provision was added to the code in 1968 in response to Supreme Court decisions *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United State*s, 389 U.S. 347 (1967), which found the Fourth Amendment did apply to searches and seizures of conversations and protected all conversations of an individual as to which he had a reasonable expectation of privacy. *See* SENATE COMM. TO STUDY GOV'T OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, FINAL REPORT, BOOK II(c) (1976).

219. 18 U.S.C. § 2511(1)(b)–(d).

220. *See* Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000).

shall be punished."[221]

The ECPA often works in conjunction with the Federal Wiretap Act,[222] to prosecute computer-related electronic communication violations. The joint effect of these two statutes has allowed prosecutors the flexibility necessary to adapt to changing technology. For example, prosecutors brought a case under the Federal Wiretap Act involving a hardware device known as a keystroke logger, a device that is attached to a computer-keyboard cable to record keystrokes.[223] This case, the first in the nation of this sort, contained an indictment for endeavoring to intercept electronic communications when the perpetrator placed the keystroke logger on his employer's computer.[224] This case was dismissed on the basis that the interception of keystrokes between the keyboard and the central processing unit ("CPU") did not meet the "interstate or foreign commerce" clause in the Federal Wiretap Act.[225] However, the decision does not speak to devices that intercept communications between the CPU and the Internet. The charging of this crime is perhaps an early demonstration of the next frontier of electronic wiretapping.[226]

The USA Patriot Act of 2001 anticipated the changing nature of wiretapping, and updated the wiretap statute in two ways: first, by adding felony violations of the computer hacking statute to the list of predicate offenses for the interception of communications;[227] and second, by changing the way in which the Federal Wiretap Act and the ECPA apply to stored voice communications, allowing federal agents to obtain protected communications under the less demanding procedures of the ECPA rather that the more demanding wiretap order required by § 2516.[228] These

221. 18 U.S.C. § 2701(a) (2000).

222. 18 U.S.C.A. § 2516 (West 2008).

223. Press Release, U.S. Att'y for the Cent. Dist. of Cal., Orange County Man Indicted on Wiretapping Charges for Installing Spy Hardware on Employer's Computer (Mar. 23, 2004), *available at* http://www.cybercrime.gov/roppIndict.htm.

224. *Id.*

225. Kevin Poulsen, *Judge Dismisses Keylogger Case*, SECURITYFOCUS, Nov. 19, 2004, http://www.securityfocus.com/news/9978.

226. The dismissal of Ropp's case in the Ninth Circuit came on the heels of a controversial First Circuit decision that differentiated between e-mails on a computer and e-mail sent over a network, and decided that in the case of the former, conduct transgressing on the privacy of the e-mail does not constitute a wiretap. United States v. Councilman, 373 F.3d. 197, 203–04 (1st Cir. 2004). That decision has since been overturned, leaving unclear the future of the Federal Wiretap Act. *See* United States v. Councilman, 418 F.3d. 67, 77–78 (1st Cir. 2005) (en banc).

227. USA Patriot Act of 2001, Pub. L. No. 107-56, § 202, 115 Stat. 272, 278. *See* 18 U.S.C. § 2516(1)(c) (Supp. IV 2004).

228. § 202; Mark Sherman, Federal Judicial Center, *Cyber Crime and Cyber Terrorism*, CLOSE-UP (Fed. Judicial Ctr., Washington, D.C.), Apr. 2002, at 1–2, *available at*

amendments continue to create flexibility, allowing the statutes to adjust to evolving computer and electronic technology.

B. COMPUTER AS THE INSTRUMENTALITY

1. Auction Fraud

Although no specific Internet fraud statute currently exists, Internet fraud is largely prosecuted under mail fraud and wire fraud statutes. The federal mail fraud statute prohibits "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises" to utilize the U.S. Postal Service to in any way further the fraud.[229] The federal wire fraud statute, enacted in 1952, contains nearly identical language to the federal mail fraud statute, and criminalizes fraudulent schemes that make use of interstate television, radio, or wire communications.[230] Both statutes have been applied to "cover not only the full range of consumer frauds, stock frauds, land frauds, bank frauds, insurance frauds, and commodity frauds, but [also] . . . such areas as blackmail, counterfeiting, election fraud and bribery."[231] Frequently the mail and wire fraud statutes have "represented the sole instrument of justice that could be wielded against the ever-innovative practitioners of deceit" in areas in which legislators have been slow to follow the technological advancement.[232]

The federal mail fraud statute is in many ways the preeminent cyber crime statute for federal prosecutors. Recent applications of the mail fraud statute reflect an evolving view of the statute as a substantive provision to combat all fraud, not just mail fraud. This is not a new trend; in the 1970s, federal prosecutors began using the mail fraud statute to attack political corruption at the federal, state, and local level.[233] Prosecutors proceeded under the theory that governmental officials who received kickbacks or other gratuities in connection with their offices engaged in a scheme to defraud the citizenry.[234] Congress supported this interpretation, and as part

http://www.fjc.gov/public/pdf.nsf/lookup/snocyb02.pdf/$file/snocyb02.pdf.

229. 18 U.S.C. § 1341 (2000).

230. *Id.* § 1343.

231. Laura A. Eilers & Harvey B. Silikovitz, *Mail and Wire Fraud*, 31 AM. CRIM. L. REV. 703, 703–04 (1994) (quoting Jed. S. Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771, 772 (1980)).

232. *Id.* (quoting Rakoff, *supra* note 231, at 772).

233. *See* Daniel J. Hurson, *Limiting the Federal Mail Fraud Statute—A Legislative Approach*, 20 AM. CRIM. L. REV. 423, 429–30 (1983).

234. *See* Michael C. Bennett, Note, Borre v. United States*: An Improper Interpretation of*

of the Anti-Drug Abuse Act of 1988,[235] added § 1346 to Title 18. This provision states in its entirety: "[f]or the purposes of this chapter, the term 'scheme or artifice to defraud' includes a scheme or artifice to deprive another of the intangible right of honest services."[236]

Prosecutors have used the mail and wire fraud statutes "to combat con artists who prey on individuals through sophisticated programs."[237] As fraud quickly transitions to the Internet, the application of the federal mail and wire fraud statutes to Internet fraud, including auction frauds, is the next logical step. Since online purchases in auctions generally involve the transmission of some thing or good through the mail or wires, these statutes are adaptable to Internet auction fraud.[238] When a legitimate purchaser is defrauded of some good after an online purchase, the online fraudster can be held criminally liable under the wire and mail fraud statutes.[239] Use of the mails or wires need not be an essential element of the scheme; rather, the statute is satisfied if the mailings are incident to an essential aspect of the scheme.[240] The broad applicability of the statute derives at least some flexibility from the low intent requirement of a wire or mail fraud crime. The perpetrator of such a fraud is required only to have acted "with knowledge that the use of the mails will follow in the ordinary course of business, or where he could reasonably foresee that use of the mails would result. It is not necessary to prove the accused . . . actually intended the mail to be used."[241]

Property Rights, 42 DEPAUL L. REV. 1499, 1508 n.70 (1993).

235. Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, 102 Stat. 4181.

236. 18 U.S.C. § 1346 (2000).

237. Peter J. Henning, *Maybe It Should Just Be Called Federal Fraud: The Changing Nature of the Mail Fraud Statute*, 36 B.C. L. REV. 435, 469 (1995).

238. This may not always be the case. As the virtual world gains popularity (9.4 million people belong to one of 32 virtual worlds currently) purchases made over the Internet may not in the future ever leave the Internet. Even now "castles" in "Scotland" and American Apparel "tee-shirts" can be purchased on the Internet to remain on the Internet. *See* American Apparel's Second Life Press Center, http://www.americanapparal.net/presscenter/secondlife (last visited July 31, 2008) (virtual store discontinued). However, as long as the wires are used at some point in the transaction, perhaps to transfer money from a real bank to an online exchange, there will likely be some plausible argument for applicability of the mail and wire fraud statutes when an online purchase fails to deliver. For an interesting discussion of the myriad issues presented by the virtual world, see Viktor Mayer-Schönberger & John Crowley, *Napster's Second Life?: The Regulatory Challenges of Virtual Worlds*, 100 NW. U. L. REV. 1775 (2006).

239. This is either because the good did not arrive or arrived in a substantially different form than was promised, if that good was sent by the U.S. Postal Service, or for that matter, FedEx, UPS, or DHL, or over a wire. *See* United States v. Sharpe, 438 F.3d 1257, 1259, 1263 (11th Cir. 2006) (use of FedEx); United States v. Curry, 461 F.3d 452, 456 (4th Cir. 2006) (use of UPS); United States v. Silvestri, 409 F.3d 1311, 1320 (11th Cir. 2005) (use of DHL).

240. *See* Schmuck v. United States., 489 U.S. 705, 710–11 (1989).

241. United States v. Figueroa, 832 F.2d 691, 696–97 (1st Cir. 1987) (citing United States v.

2. Spam

The CAN-SPAM Act was signed into law in December 2003.[242] Prior to the passage of the Act, the regulation of spam was left primarily to state legislatures. States enacted a variety of idiosyncratic measures to stem the spam problem.[243] However, the sheer volume of spam overwhelmed states' abilities to regulate. In 2003, the volume of spam was threatening to overwhelm "not only the average consumer's in-box, but also the network systems of ISPs, businesses, universities, and other organizations."[244] In response, Congress removed the burden of spam from state legislatures[245] and passed the CAN-SPAM Act in order to:

> (i) prohibit senders of electronic mail (e-mail) for primarily commercial advertisement or promotional purposes from deceiving intended recipients or Internet service providers as to the source or subject matter of their e-mail messages; (ii) require such e-mail senders to give recipients an opportunity to decline to receive future commercial e-mail from them and to honor such requests; . . . and (iv) prohibit businesses from knowingly promoting, or permitting the promotion of, their trade or business through e-mail transmitted with false or misleading sender or routing information.[246]

As a result, this law—the first federal statute to address the increasing volume of unsolicited commercial e-mails—criminalized the use of spam as a mass marketing tool and broadened the scope of what is prosecutable. The Act prohibits the intentional sending of spam from a protected computer without authorization;[247] the use of a protected computer to send spam with the intent to deceive recipients of its origin;[248]

Contenti, 735 F.2d 628, 631 (1st Cir. 1984)). *But see* United States v. Smith, 934 F.2d 270, 272–73 (11th Cir. 1991) (holding that a defendant cannot be convicted based on mailing between insurance company's offices to approve his payment draft where it was not reasonably foreseeable to defendant that company would mail draft).

242. CAN-SPAM Act of 2003, 15 U.S.C. §§ 7701–13 (Supp. IV 2004).

243. *See* Zitter, *supra* note 89, at 1.

244. CAN-SPAM ACT OF 2003, S. REP. NO. 108-102, at 2 (2003), *as reprinted in* 2004 U.S.C.C.A.N. 2348, 2359. Internet providers were becoming completely overburdened by the volume of spam. In 2003 America Online blocked approximately 80 percent of its inbound e-mails as spam, Microsoft blocked 2.4 billion spam messages *per day*, and Earthlink reported a 500 percent increase in spam in the previous eighteen months. *Id.* at 2–3.

245. The federal law now preempts most state legislation other than those regulating deceptive practices. *See* Gordon v. Impulse Mktg. Group, Inc., 375 F. Supp. 2d 1040, 1045–46 (E.D. Wash. 2005).

246. S. REP. NO. 108-102, at 1.

247. 15 U.S.C. § 7704(b)(3).

248. *Id.* § 7704(a)(1)(C).

the sending of spam with materially false headings;[249] and the false representation of origin in a spam message.[250]

The Act defines spam as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."[251] The term "electronic mail message" means, "a message sent to a unique electronic mail address."[252] An "electronic mail address" is "a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox . . . and a reference to an Internet domain . . . whether or not displayed, to which an electronic mail message can be sent or delivered."[253] This definition likely limits the application of the CAN-SPAM Act to e-mail communications.

Prosecution under this section carries up to a five-year jail sentence, a fine, or both.[254] The CAN-SPAM Act is often used in conjunction with the Hobbs Act[255] and the CFAA[256] if the spam crime includes the intent to extort or to cause damage to a protected computer. SpIM, the new frontier of spam crimes, is probably not included in the definitions of the CAN-SPAM Act, and there has been limited success under the CFAA to prosecute this emerging crime.[257]

3. Phishing

There is no specific statute criminalizing phishing. Currently phishing crimes are charged under a variety of statutes, including the CFAA, the federal wire fraud statute, the CAN-SPAM Act, and federal trademark law.[258]

Phishing is a crime best examined by its component parts. The

249. *Id.* § 7704(a)(2).
250. *Id.* § 7704(a)(1).
251. *Id.* § 7702(2)(A).
252. *Id.* § 7702(6).
253. *Id.* § 7702(5).
254. 18 U.S.C. § 1037(b)(1)–(3) (Supp. IV 2004).
255. Hobbs Act, 18 U.S.C. § 1951 (2000).
256. CFAA, 18 U.S.C. § 1030 (2000).
257. *See* Press Release, U.S. Att'y for the Cent. Dist. of Cal., New York Teen Pleads Guilty to Making Extortion Threats Against Internet Company (Mar. 22, 2005), *available at* http://www.usdoj.gov/criminal/cybercrime/grecoPlea.htm [hereinafter New York Teen Pleads] (discussing eventual guilty plea by Greco to a violation of the CFAA under § 1030(a)(7), extortionate hacking).
258. Occasionally phishing crimes are also charged under the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961–68 (2000), and the access device fraud statute, 18 U.S.C. § 1029 (2000).

spoofed e-mail that sparks a phishing scam can be prosecuted under the CAN-SPAM Act. The e-mail, a commercial electronic mail message, "the primary purpose of which is the commercial advertisement or promotion of a commercial product or service,"[259] fits squarely within the definition of mass mailings prohibited by the act. The overall scheme of fraud that occurs in inducing unsuspecting users to enter personal information to a false Web site is generally prosecuted under the federal wire fraud statute, which prohibits the perpetration of a fraud over the use of wires.[260] Any fraud that gives a phisher impermissible access to a protected computer by stealing a password can also be prosecuted under the CFAA. The copied Web site or falsified e-mail may be prosecuted under trademark law prohibiting unlawful infringement on trademarked symbols or other materials if there is intentional trafficking in that trademark.[261]

Two phishing cases have recently been charged using a combination of these statutes. The most recent case involved a sophisticated phishing scam of spoofed e-mails from America Online's billing department that prompted users to enter their personal and financial information onto a phished site.[262] The perpetrator was charged and convicted under the CAN-SPAM Act—the first prosecution under this act—and faced a maximum 101-year jail sentence, although he was later sentenced only to 70 months.[263] A similar scheme, using spoofed e-mails from America Online and Paypal's billing departments, prompted users to update their billing information on the threat of cancellation of their accounts.[264] The perpetrator of this scheme amassed nearly $50,000 from unsuspecting victims of his phishing scheme.[265] He was charged and convicted under two counts of the access device fraud statute and sentenced to four years in prison for orchestrating a "scheme to defraud consumers of personal financial information via spam e-mail."[266] The disparate charges and disparity in sentencing perhaps reflects the chaotic nature of phishing

259. 15 U.S.C. § 7702(2)(A) (Supp. IV 2004).

260. 18 U.S.C. § 1343 (2000).

261. *See id.* § 2320(a).

262. Sharon Gaudin, *Phisher Convicted, Faces 101 Years in Prison*, INFORMATIONWEEK, Jan. 17, 2007, http://www.informationweek.com/shared/printableArticle.jhtml?articleID=196901446.

263. *See* Sharon Gaudin, *California Man Gets 6-Year Sentence for Phishing*, INFORMATIONWEEK, June 12, 2007, http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=199903450.

264. Press Release, U.S. Dep't of Justice, Fraudster Sentenced to Nearly Four Years in Prison in Internet ePhishing Case (May 18, 2004), *available at* http://www.usdoj.gov/criminal/cybercrime/hillSent.htm.

265. *Id.*

266. *Id.*

prosecutions demanded by the absence of a specialized statute for phishing schemes.

States have also taken an active role in addressing phishing crimes. In January 2005, Virginia added phishing to its Computer Crimes Act, categorizing the use of a computer to obtain personal information "through the use of material artifice, trickery or deception" as a felony.[267] New Mexico and New York have enacted similar statutes.[268] Washington has criminalized even attempted phishing.[269] In California, the Anti-Phishing Act of 2005 makes it "unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business."[270] However, the California statue does not create a criminal provision for phishing.

IV. ARE THERE ANY GAPS?

Given the changing nature of the Internet and cyber crime, it seems reasonable to test whether the existing statutory framework of the U.S. Code provides adequate prosecutorial tools. There appear to be certain areas of the Code that contain "gaps" in coverage, allowing cyber crimes to evolve beyond the applicability of the statutes. Specifically, this Note identifies three important gaps in the existing criminal code: the difficulty of meeting the $5000 minimum requirement of 18 U.S.C. § 1030 (a)(5), the definitional element that limits the CAN-SPAM Act's applicability to spIM, and the lack of a specialized phishing statute. Each gap will be examined in turn.

267. Va. Code Ann. § 18.2-152.5:1 (West 2005). *See AOL Sues Over Identity Thefts, Uses New Law*, REUTERS, Feb. 27, 2006, http://today.reuters.com/news/articlebusiness.aspx?type=telecomm&storyID=nN27331008&from=business; Larry Greenemeier, *States Tell Phishers to Cut Bait or Else*, INFORMATIONWEEK, Apr. 13, 2005, http://www.informationweek.com/news/management/showArticle.jhtml?articleID=160702186.

268. *See* N.M. Stat. Ann. § 30-16-24.1 (West 2005); Assemb. 8025-B, 2005 Assemb., Reg. Session (N.Y. 2005). *See also* Press Release, N.Y. State Senate Republican Campaign Comm., Senate Passes Four Identity Theft Bills (June 21, 2005), *available at* http://www.nysenategop.com/Committee/News/NewsStory.asp?t=co&id=7.

269. Washington criminalizes both the sending of spoofed e-mails and the creation of fraudulent Web sites, even lacking consumer fraud by either action. *See* Wash. Rev. Code Ann. §§ 19.190.010–19.190.110 (West 2005).

270. Anti-Phishing Act of 2005, Cal. Bus. & Prof. Code §§ 22948–48.3 (West). *See also* Press Release, Cal. Dep't of Consumer Affairs, New Laws Will Help Protect Against Identity Theft (Oct. 7, 2005), *available at* http://www.dca.ca.gov/publications/press_releases/2005/1007_idtheft.shtml.

A. 18 U.S.C. § 1030 (a)(5)

The existence of the $5000 damages threshold in 18 U.S.C. § 1030(a)(5) creates a gap that allows some hacking crimes to continue unchecked. Prosecutors must allege damages of over $5000 as a jurisdictional matter and as an element of the crime in order to invoke § 1030(a)(5). This section, along with § 1030(a)(4), is the primary tool used in the prosecution of hacking crimes against personal and business computers, yet § 1030(a)(5) is also the *only* section of the CFAA that contains a minimum loss threshold.[271] By contrast, hacking crimes against government computers require no minimum loss,[272] and threats to hack into a protected computer, while requiring the intent to extort something of value, do not require any monetary threshold to prosecute the crime.[273]

The $5000 threshold requirement to prosecute hacking is unique when compared to analogous crimes in the physical world. Hacking, at its root, is theft and destruction. Similar crimes such as the sale and transportation of stolen vehicles,[274] the sale and transportation of livestock,[275] and the crime of counterfeiting labels,[276] do not require any monetary threshold in damages to allege the crime.[277] Indeed, Wesley L. Hsu, Assistant U.S. Attorney, Deputy Chief of the Cyber and Intellectual Property Crimes Section in Los Angeles, believes the $5000 threshold requirement of the CFAA is the only crime with an element defined by the victim's response after the completion of the defendant's criminal acts.[278]

The lack of a monetary threshold in certain computer and physical crime statutes makes the crimes easier to prosecute and broadens the scope of the statutes. As computers spread and cyber crime evolves, society is confronted by many hacking crimes that fall within the stated congressional intent to protect individuals "from harm caused by the improper disclosure

271. Section 1030(a)(4) requires the hacked object have value of over $5000, which is much easier to allege and define than the requirement for "loss." 18 U.S.C. § 1030(a)(4) (2000).

272. *Id.* § 1030(a)(1)–(2).

273. *Id.* § 1030(a)(7).

274. *Id.* §§ 2312–13.

275. *Id.* §§ 2316–17.

276. *Id.* § 2318.

277. This is not to overstate the case. Some physical crime statutes *do* require a monetary threshold. For example, 18 U.S.C. § 2314, which criminalizes the transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting, requires that the goods transported amount to more than $5000. *Id.*

278. Interview with Wesley L. Hsu, U.S. Att'y, Deputy Chief of the Cyber and Intellectual Prop. Crimes Section, in L.A., Cal. (Mar. 20. 2007) (on file with author). For this Note, Hsu expressed his personal opinions. Hsu's personal opinions do not reflect the opinions of the United States Attorney's Office or the Department of Justice.

or use of personal information,"[279] yet arguably are outside the scope of the CFAA due to the $5000 threshold. For example, illegal access by computer to medical records from a hospital or an executive's work produced in a sensitive merger negotiation would likely not meet the required monetary threshold since the viewing of sensitive information does not necessarily cause tangible damages. However, notwithstanding the inability to demonstrate immediate economic loss, it is clear that unauthorized access to such confidential information is damaging and can cause immediate and long-term damage in terms of security, emotional well-being, and reputation.

Various changes in the CFAA since its original enactment seem to reflect congressional recognition of the scope of the crime extending beyond what was initially envisioned in the mid-1980s. It is important to note that in the early 1980s, when the CFAA was first enacted, the federal government used twice the number of computers the public used.[280] As a result, most hacking crimes occurred on government computers, as those were the largest group and the ones most vulnerable to attack. It made sense then that crimes against government computers were the main target of the act, and no threshold damages were required to prosecute.[281]

The number of personal computers now far exceeds the computers employed in government service. As a result, Congress has shifted the focus of the CFAA away from the exclusive protection of government computers. For example, in 1996, Congress replaced the phrase "federal interest computer" to "protected computer" to broaden the group of computers protected by the act.[282] Congress has also shifted away from the technical concept of unauthorized access to a computer system to a focus on the defendant's harmful intent.[283] It appears that in these actions Congress has recognized the substantial threat, both tangible and intangible, posed to private and business computers by cyber criminals.

279. Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, 60 Fed. Reg. 4362-01, 4363 (Jan. 20, 1995) [hereinafter Privacy and National Information].

280. *See* CFAA, S. REP. NO. 99-432, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2479; 132 CONG. REC. H3277 (daily ed. June 3, 1986) (statement of Rep. Nelson). *See also* Exec. Order No. 12845, 58 Fed. Reg. 21887 (Apr. 21, 1993) ("[T]he Federal Government is the largest purchaser of computer equipment in the world.").

281. In 1994, as hacking crimes were increasing in frequency, Congress reduced the threshold damages requirement for hacks against government computers. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 929001(6), 108 Stat. 1796, 2097–98.

282. Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(4)(A)(i), 110 Stat. 3488, 34993 (codified as amended at 18 U.S.C. § 1831–39 (2000)).

283. *See* 139 CONG. REC. S16421-03 (daily ed. Nov. 19, 1993).

However, Congress has yet to address the vestigial $5000 threshold that hinders the prosecution of many hacking crimes. This is problematic on both a pragmatic and theoretical level. The damages threshold is the most difficult element to prove beyond a reasonable doubt and the easiest element to defend against.[284] It is inherently difficult to calculate the cost of a cyber attack given both the murky parameters of the definition of "loss," and the inherent difficulty for an attacked organization to know the scope and extent of an attack at the time of the attack. Later in court, defendants can pick apart measures taken at the time to cast doubt as to whether the threshold is met and can suggest that a victim's panic at the time of the attack implies overspending on remedial measures. Since jurors are generally not as familiar with computer security and the costs of remedying and preventing cyber attacks as they are with physical security, they are not adequately prepared to assess damages in the wake of a cyber attack. Consequently, the $5000 minimum threshold creates an unreasonably high barrier to successful federal prosecution.

In effect, Congress has created a dual-threshold test for federal jurisdiction: in order to prosecute, a hacking crime must meet the requirement of $5000 in loss or it must reach a special government interest. For example, if information was viewed and no physical damages wrought by criminal hacking into U.S. military records,[285] NASA computers,[286] and private tax return data stored on IRS computers,[287] these hacks would not fall within the scope of the CFAA if measured only by the loss threshold. However, as measured by access to a protected computer of federal interest, hacking into these sources falls within the scope of the CFAA. This dual threshold creates a wide gap for hacks that meet neither threshold, but still fall within the area Congress intended to protect by the act.

B. SPIM

The CAN-SPAM Act is the first federal step taken to address the increasing volume of spam beleaguering e-mail users, yet its application is

284. *See* Freeh, *supra* note 21. For a discussion on the difficulties of proving loss see *infra* Part V.A.

285. *See, e.g.*, *Teens Tapped Computers of U.S. Military*, CHI. TRIB., Nov. 21, 1991, at C3.

286. *See, e.g.*, Press Release, U.S. Attorney's Office for the Cent. Dist. of Cal., Romanian Charged with Hacking into Government Computers, Causing Nearly $1.5 Million in Losses (Nov. 30, 2006), *available at* http://oig.nasa.gov/press/pr2007-C.pdf.

287. *See* Robert D. Hershey, Jr., *I.R.S. Staff is Cited in Snoopings*, N.Y. TIMES, July 19, 1994, at D1.

limited. As the nature of communication over the Internet evolves and moves toward the instantaneous conversational ability of instant messaging,[288] a possible gap in the statutory coverage appears: the CAN-SPAM Act probably does not apply to spIM.

The Act defines prohibited spam as "any electronic mail message" with a commercial purpose.[289] An electronic mail message is in turn "a message sent to a unique electronic mail address"[290] which refers to an Internet domain name to which e-mail messages can be sent or delivered.[291] The definition of spam in this Act likely limits its coverage to e-mail communications, precluding other spam-like media such as instant messaging which do not have domain names associated with the messaging address.

SpIM is a rapidly growing problem. Experts warn that spIM is growing at three times the rate of spam.[292] In many ways, it is also more dangerous, as enticing a user to click on a link embedded in an IM is often easier than it is via e-mail.[293] Despite its dangers, the use of spIM is difficult to prosecute under the current statutory provisions. The first prosecution for spIM began in February 2005.[294] According to the criminal complaint, Anthony Greco, an eighteen-year-old New Yorker, created thousands of accounts on the Internet messaging service MySpace.com and used the accounts to send over 1.5 million spam messages to unsuspecting MySpace users.[295] Greco then threatened to share his methods for spamming if MySpace did not assign him an exclusive marketing deal that would legitimize the messages he sent over the service.[296] Although he was charged under the CAN-SPAM Act, Greco pled guilty to a violation of the CFAA, § 1030(a)(7), extortionate hacking.[297] A case under the CAN-SPAM Act would undoubtedly be difficult; by its defining terms, the CAN-SPAM Act requires a criminal act of spam be sent to a domain name.[298]

288. *See* Biever, *supra* note 94.
289. 15 U.S.C. § 7702(2)(A) (Supp. IV 2004).
290. *Id.* § 7702(6).
291. *Id.* § 7702(5).
292. *See* Biever, *supra* note 94.
293. *Id.*
294. *See* Press Release, U.S. Attorney for the Cent. Dist. of Cal., New York Spammer Arrested for Making Threats Against Internet Messaging Company and Sending More Than 1.5 Million Spam Messages (Feb. 17, 2005), *available at* http://www.usdoj.gov/criminal/cybercrime/grecoArrest.htm [hereinafter New York Spammer Arrested].
295. *Id.*
296. *Id.*
297. *See* New York Teen Pleads, *supra* note 257; Sturgeon, *supra* note 101.
298. 15 U.S.C. § 7704(a)(1)(A) (Supp. IV 2004).

MySpace and other messaging services, such as America Online's AIM and Microsoft's MSN Messenger, do not link a domain name to their instant messaging services. And although the sentence was sealed,[299] Greco most likely served significantly less time, if any at all, under his plea bargain to extortionate threats. All three of the offenses he was charged with—violation of CAN-SPAM Act, extortionate threats, and damaging a protected computer—carried a maximum possible penalty of eighteen years in federal prison.[300]

The Greco case is unlikely to be the last prosecution for spIM on the Internet. Indeed, prosecutors in the case warn this is just the "tip of the iceberg. This could be a new wave as online communities start up."[301] The gap in the CAN-SPAM Act that limits its applicability to e-mail messaging only is certain to become a problem as the rate of spIM increases over the coming years.

C. PHISHING

Each act of phishing involves two separate victims: the targeted user who responds to a phish, and the company whose identity and Web sites are "spoofed" to create the phish.[302] Generally, prosecutors are able to use the CFAA, the Racketeer Influenced and Corrupt Organizations Act ("RICO"),[303] the federal wire and mail fraud statutes,[304] the access device fraud statute,[305] and the CAN-SPAM Act, among others, to prosecute most elements of a phishing scheme affecting an unsuspecting user. Indeed, identity theft, fraud, and hacking against the user are well-established precedent in the cyber crime lexicon. However, existing statutes are not necessarily applicable to all aspects of the phishing scheme.

In particular, prosecutors have difficulty applying existing statutes to the spoofing of a Web site. In a phishing scheme, an e-mail or Web site is created to look similar to or the same as that of a real business or source. Since these creations are done without any access to another computer, the copying cannot be prosecuted as a "hack" as defined by the CFAA.[306] Even

299. *Spammer Gets Likely Prison Sentence*, FOXNEWS.COM, Oct. 18, 2005, http://www.foxnews.com/story/0,2933,172629,00.html.

300. *See* New York Spammer, *supra* note 294.

301. Sturgeon, *supra* note 101 (quoting Asst. U.S. Att'y Brian Hoffstadt).

302. *See* Stevenson, *supra* note 112, at ¶ 3.

303. *See* 18 U.S.C. §§ 1961–68 (2000).

304. *Id.* §§ 1341, 1343.

305. *Id.* § 1029.

306. There is no definition of "access" provided by the CFAA. In 1977, Senator Ribicoff proposed an important and visionary bill, the Federal Computer Systems Protection Act, which never got out of

if a spoof of a Web site could be considered "access," the difficulty of proving tangible damages as a result of the copying would terminally impair the crime's ability to meet the monetary threshold of the CFAA.[307] A prosecution under the federal wire or mail statutes may work but is not a perfect fit. These statutes presume the existence of an identifiable piece of property;[308] in the case of a spoofed Web site, "identifying a property interest and then concluding that it was taken can require considerable creativity."[309] A spoofed Web site or e-mail is not an access device, and the access device fraud statute criminalizes the use of the fruits of the hack, not the hack itself,[310] and would therefore not be applicable. If an e-mail or spoofed Web site copies and traffics in a trademarked symbol, the phisher could be prosecuted under federal trademark law, which criminalizes the intentional trafficking of counterfeit goods or services;[311] however, this is an odd fit to suggest a spoof of a Web site is an "attempt" to offer the victim services. Lastly, while the e-mail promulgating the link to the Web site is spam within the technical definition, the spoofed Web site is not.[312]

Because no specialized phishing statute exists, the crime of spoofing a Web site has been difficult to prosecute. The spoofed company that loses consumer confidence and perhaps real profits is often left without a legal redress; the cyber criminal who spoofed its Web site is often beyond the reach of prosecutors.

committee. PENDER M. MCCARTER, AM. FEDERATION OF INFO. PROCESSING SOC'Y, AFIPS WASHINGTON REPORT 7 (1977). In the bill he defined "access" as means "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network." *Id.* Without more current federal guidance courts have taken many approaches to define the term. Some courts look to a physical definition, suggesting a user "accesses" a computer when the user sends a command to that computer instructing it to complete a task. *See* United States v. Morris, 928 F.2d 504, 510–11 (2d Cir. 1991). Other courts rely on virtual standard, such that access occurs when a user makes a virtual entrance onto a computer, such as by using a password. *See* Trulock v. Freeh, 275 F.3d 391, 409 (4th Cir. 2001). None of these definitions would include the copying of a webpage or e-mail as prohibited access.

307. 18 U.S.C. § 1030(a)(5)(B)(i) (2000).

308. *Id.* §§ 1341, 1343.

309. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1610 (2003). The difficulty in proving harm is also troublesome to an argument under these statutes; even if a property interest were found, it would be difficult to demonstrate how a spoof actually deprives the rightful owner of that property: thus,

> courts tended to reach results-oriented outcomes. When computer misuse caused harm to a victim in some way, courts generally concluded that property had in fact been taken and held the defendants liable. When no appreciable harm resulted, courts tended to find that no property was taken and hold that the defendants had committed no crime.

Id. at 1611.

310. 18 U.S.C. § 1029 (2000).

311. *Id.* § 2320.

312. *See id.* § 1037 (Supp. IV 2004).

V. WHAT SHOULD BE DONE?

Although it is clear that some gaps exist in the federal criminal laws against cyber crime, it is less clear what remedial measures, if any, should be taken. It is first necessary that reconciliation be made between the benefits to be achieved by closing such gaps and the administrative and procedural costs potentially to be incurred.

Any suggestion to expand federal jurisdiction by extending the scope of criminalized acts automatically prompts fears of an overreaching federal government. These sorts of fears are not unique. In the mid-1990s, Congress's expansion of federal criminal jurisdiction to violent street crimes prompted a similar federalization debate.[313] Critics foresaw the expansion of federal criminal legislation to entail "dire consequences for federalism and for the federal criminal justice system,"[314] fearing that the expansion of jurisdiction would flood federal courts, impeding their ability to function.[315] Scholars worried that decisionmaking would be shifted away from the most "directly accountable levels of government" and that prosecutors, emboldened by the new federal authority, would charge and pursue every case no matter how minor.[316]

This fear has not disappeared in the decade since the last major debate over the expansion of the federal government's role in the prosecution of crime. However, a number of things have changed since the mid-1990s. First, a broad and expansive reading of the Commerce Clause has substantially expanded federal criminal jurisdiction. In 1995, the Supreme Court found the Commerce Clause to delegate three broad categories of activities for Congress to regulate: the use of the "channels of interstate commerce," "the instrumentalities of interstate commerce," and "those activities that substantially affect interstate commerce."[317] Much of the expanded federal criminal jurisdiction has derived from the statement that a "federal cause of action is in pursuance of Congress's power to regulate interstate commerce."[318] Correspondingly, the regulation of cyber crime falls within Congress's constitutional power. Because of the inherently interstate, and indeed global, nature of the medium, Congress's ability to

313. Harry Litman & Mark D. Greenberg, *Dual Prosecutions: A Model for Concurrent Federal Jurisdiction*, 543 ANNALS AM. ACAD. OF POL. & SOC. SCI., 72, 73 (1996).

314. *Id.* at 74.

315. *See* Sanford H. Kadish, Comment, *The Folly of Overfederalization*, 46 HASTINGS L.J. 1247, 1249 (1995).

316. Litman & Greenberg, *supra* note 313, at 74.

317. United States v. Lopez, 514 U.S. 549, 558–59 (1995).

318. United States v. Morrison, 529 U.S. 598, 613 (2000).

regulate criminal activity on the Internet falls within the jurisdiction under both the channels and instrumentality prongs of the *United States v. Lopez* jurisdictional query.[319]

Second, the world has changed; computers are now present in two-thirds of American houses, and nearly 100 percent of Americans between the ages of twelve and eighteen use the Internet on a daily basis.[320] As the reach of the Internet has expanded to all corners of the country, and indeed the world, a practical analysis suggests that federal jurisdiction over cyber crime is the most effective and efficient approach.

Prosecution of cyber crime requires detailed technical knowledge and understanding of computing and networked technologies, in addition to a mastery of the complexities of cyber law. The federal government has already introduced mechanisms for the investigation and prosecution of cyber crime. For example, in the San Francisco area, which is home to many technology companies, the U.S. Attorney's office established a unit exclusively to prosecute computer and intellectual property crimes. Robert Mueller (as the former U.S. Attorney for the Northern District of California) saw "a necessity to staff that unit with individuals who were both talented prosecutors and who understood and could work with the technology . . . [with] computer crimes cases, or hacking and denial of service cases, or the intellectual property cases . . . ."[321] The federal government has made it a priority to hire specialists, engineers, and scientists, who have a "bedrock experience so that they start with a profound understanding of the computer world."[322] The FBI has established regional computer forensics labs in several cities so that the "interchange of ideas" can occur between these FBI initiatives and other branches of federal and state government enabling federal prosecutors "to go into a court room and testify with expertise and credibility."[323]

The federal government has also taken steps to improve its ability to track and fight cyber crimes on a global scale in recognition of the Internet's capacity to weave communications through service providers in different states or countries.[324] Crimes committed remotely from anywhere

319. *See* James K. Robinson, Remarks at the Internet Computer Crime Conf.: Internet as the Scene of the Crime (May 29–31, 2000) (transcript available at http://www.cybercrime.gov/roboslo.htm). Arguably, although more attenuated, the use of the Internet is an activity "that substantially affects interstate commerce." *Morrison*, 529 U.S. at 609.

320. Levy, *supra* note 13.

321. Mueller, *supra* note 24.

322. *Id.*

323. *Id.*

324. Robinson, *supra* note 319. Modern cyber crimes are not simple point A to point B

in the world can end up on American computers.[325] As a result, even crimes that seem local in nature might require international assistance and cooperation. This demands federal involvement. To this end, the FBI has created Cyber Action Teams, groups of approximately twenty-five people including agents, computer forensic experts and specialists in computer code, to tackle computer crime issues,[326] and has deployed them in fifty-six offices around the world, including Iraq and China, to deal with computer intrusions.[327]

Certainly, some states also have created powerful cyber crime task force units. For example, the California High Technology Crimes Task Force, comprised of prior existing state-funded regional task forces, is "big enough and sophisticated enough to undertake the necessary enforcement measures: long-term surveillance and intelligence gathering, especially on organized criminal groups; undercover purchases; use of confidential informants; reverse stings; storefront operations; and other techniques suited to preventing crime, not just reacting to it."[328] California is perhaps a unique case due to the concentration of high-tech and information technology companies in the state;[329] most states have not devoted the same amount of resources to cyber crime prevention.[330] Whereas the

transactions; even if one computer infects another computer from twenty feet away, the infection could be routed through providers in New York, Marrakesh, and Rome before accessing the victim's computer. *See id.*

325. This includes almost every type of computer related crime, from "violent crime, terrorism, and drug-trafficking, to the distribution of child pornography and stolen intellectual property, and attacks on e-commerce merchants." *Id.*

326. Bryan-Low, *supra* note 16.

327. *Id.*

328. OHLHAUSEN RESEARCH, INC., CAL. HIGH TECH TASK FORCE COMM., COMBATING HIGH-TECH CRIME IN CALIFORNIA: THE TASK FORCE APPROACH 19 (1997) [hereinafter HIGH TECH TASK FORCE].

329. It is important to note that,

> [t]he high-technology industry is a vital part of California's economy, employing some three-quarters of a million Californians . . . . The industry produces over half of the state's total export sales, and its electronics sector alone employs more Californians than any other manufacturing sector in the state.
>
> But high tech is under serious attack.

HIGH TECH TASK FORCE, *supra* note 328, at iii.

330. Only fifteen states were up to federal standards by 2003. LEE M. ZEICHNER & ROBERT ALMOSD, STATE IMPLEMENTATION OF FEDERAL CYBER-SECURITY REQUIREMENTS 4 (2003). However, some states have taken sizeable steps. North Carolina directed $15.2 million from its reserve savings account to combat cyber crimes. *See* Press Release, N.C. Crime Control & Pub. Safety, North Carolina's Terrorism Preparations Well Underway as One-year Anniversay Approaches (Sept. 9, 2002), *available at* http://www.nccrimecontrol.org/newsrels/em/2002/terrorismpreparations.html. And Louisiana hired defense contractors to install programs protecting computers in all of its critical state agencies. *See* John McMillan, *State Has More Tools for Terrorism Response*, ADVOCATE (Baton Rouge, La.), Sept. 7, 2002.

federal infrastructure and training mechanisms are already in place, the costs of improvements in technology and training necessary to upgrade states' cyber prosecution abilities would be quite high. As a result, a federal approach is the most efficient, and likely the most effective, approach to cyber crime regulation.

Both constitutionally and pragmatically, the regulation of cyber crimes is best left to federal legislators and law enforcement. This Note now looks to three specific remedies that Congress should undertake to update the criminal code against the evolving cyber threat.

A. 18 U.S.C. § 1030

It is first important to understand the history of the CFAA before considering steps to reduce or eliminate the $5000 threshold. Similar to a diversity-lawsuit threshold, the monetary minimum in the CFAA was imposed so as to include only "serious" violations in the realm of prosecutorial fodder, which is consistent with Congress's general intent to limit federal jurisdiction to "cases of substantial computer crimes."[331] Senator Laxalt, one of the CFAA's sponsors, explained that the monetary threshold was meant, "first, to distinguish between alterations that should fairly be treated as misdemeanors and those that should be felonies; and second, to limit federal jurisdiction to the felonious alterations. Setting a specific loss value is one way to achieve this end."[332]

However, just as the courts face an awkward problem applying the amount-in-controversy requirement for diversity jurisdiction, especially in cases involving intangible damages such as emotional distress or loss of goodwill, the monetary threshold of the CFAA causes a real and substantial problem due to the difficulties of pleading $5000 in damages. Prosecutors are fond of using the example of a jimmied lock. If a burglar picks the lock to a back door and breaks into a house, it is clear that the minimal cost of replacing the lock is incidental to the burglary and necessary to remedy the damages caused. But, what if the owner of the house replaced the lock with a $200 deadbolt? What if the owner replaces the lock with a high-tech alarm system for $10,000? The parameters of loss caused by the burglary are unclear in this situation.

331. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp 2d 497, 522 (S.D.N.Y. 2001).

332. 132 CONG. REC. S4072 (daily ed. Apr. 10, 1986) (statement of Sen. Laxalt). *See* 132 CONG. REC. S14453-02 (daily ed. Oct. 1, 1986) (statement of Sen. Tribble) ("This bill will assert Federal jurisdiction over computer crimes only in those cases in which there is a compelling Federal interest. This reflects my belief and the Judiciary Committee's belief that the States can and should handle most such crimes, and that Federal jurisdiction in this area should be asserted narrowly.").

The same is true for cyber crimes. Cyber attacks do not usually leave detailed tracks and specific markers or instructions about how to remedy problems. Victims of a cyber attack—businesses or individuals—must assume the worst-case scenario to ascertain the nature of the damage potentially suffered, including theft of information, corruption of databases and operating systems, and creation of worms and trapdoors to facilitate future attacks. Often this requires restoring an environment to a prior period and then undertaking a painstaking process of testing and experimentation to determine the nature of the attack and the damage it caused. Unlike repairing the physical damage from a jimmied lock, restoration of the integrity of a computing and networking environment often requires tedious incremental steps of trial and error. This can lead to high failure rates and huge bills until confidence in the remedy is achieved.

Costs of this process include both the direct costs of time and services required to restore the environment and the indirect costs imposed upon the users who must change their day-to-day routines to prevent future attacks. Under the current statutory scheme, a judge or jury is forced to piece together a complex set of steps to determine how much of the represented remedial costs should count toward the loss threshold. Courts have determined that the monetary loss for system destruction, as well as expenses related to restoring data, and creating a better, more secure system, are consistent with the threshold requirement.[333] However, it is unclear what that includes. A jury is left to decide whether the "expenses relating to creating a better . . . system" are reasonable;[334] for example, whether loss should include a basic patch and repair job or whether protection for the system against future attacks with expensive firewalls should be included in the loss threshold. Juries are not as familiar with the workings and costs of computer and Internet security procedures as they are with locks and alarm systems, making it especially difficult for them to assess accurately the legitimacy of postattack measures. According to prosecutors, "whereas professionals in the field understand that emergency computer services will cost hundreds of dollars per hour, to a common juror that rate 'may' seem absurd. Defendants can exploit jurors' inexperience with this sort of crime to attack the 'reasonableness' of the services rendered."[335]

333. *See* United States v. Middleton, 231 F.3d 1207, 1212 (9th Cir. 2000).

334. *See id.* at 1213 (denying defendant's request of an instruction stating that "[d]amage does not include expenses relating to creating a better or making a more secure system").

335. Interview with Wesley L. Hsu, *supra* note 278. This problem is particularly acute where services are rendered by inhouse employees; "defendants can suggest that in these cases the business does not actually experience any loss because the employees would receive a salary whether or not an

The problem is compounded by the fact that it is almost impossible to have accurate records of the true total costs of a cyber attack, since it will often involve both direct and indirect costs. First, it is a great challenge for a victim to reconstruct the events following an attack to create a precise cost analysis. If a business is attacked, it will work as quickly as it can to restore the integrity of its information lest it lose valuable profits or risk its relationships with customers, employees, vendors, lenders, and shareholders. As anyone who has ever struggled with a computer problem knows, it is hard, after all is said and done, to reconstruct which keystroke or series of keystrokes, ultimately fixed the problem. Second, the actual costs—measured in time sheets, programming, invoices, and the like—are generally tabulated after the event. It is easy for defendants to point to this unfortunate reality to engage in a lively session of "Monday morning quarterbacking." It is very easy to say, after the exigency of the attack has passed, that certain measures were unreasonable.

The gap created by the damages threshold presents a dangerous loophole for the future of cyber-crime prosecution. In a substantial proportion of hacking crimes, the criminally culpable conduct is conceded, but the damages are contested. The prevalence of this situation is likely to grow in the coming years as information becomes more accessible over the Internet. Criminal law relies on the deterrence effect of its statutory provisions; elimination of the $5000 threshold would substantially improve the deterrent effect and thereby close the gap it unintentionally created.[336]

The difficulties in proving the loss threshold and the systematic inequity in proving back up the costs associated with an attack suggest that the $5000 minimum threshold should be eliminated altogether. Although a lower threshold would lower the pleading burden, any sort of statutory definition—be it $5000, $50, or $500,000—diminishes the impact of the actual criminal conduct. It is important to keep in mind that,

> [t]he risk of harm to individuals or to the public safety posed by breaking into numerous systems and obtaining root access, with the ability to destroy the confidentiality or accuracy of crucial—perhaps lifesaving information—is very real and very serious even if provable monetary damages never approach the $5,000 mark.[337]

Indeed, the monetary threshold has "nothing to do with the mens rea or actus reus of the crime."[338] It thus seems valid to question "why it should

attack occurs." *Id.*

336. *See* Yang & Hoffstadt, *supra* note 14, at 213.

337. Freeh, *supra* note 21.

338. Interview with Wesley L. Hsu, *supra* note 278.

matter how the victim responded" when a defendant committed the crime.[339] Elimination of the threshold would not render the statute overbroad, as the protections built in to the CFAA and the dual threshold test implicit in the Act would still limit prosecution to only the "serious" cases.

In the creation of the CFAA, Congress appreciated the delicate balance between efficient prosecutions and the need to protect privacy and property rights.[340] As a result, Congress built certain protections against federal prosecution into the CFAA. For example, in order to fall within the scope of the statute, a user must access a computer either without authorization or in excess of authorization;[341] a user with authorization to use a computer, even if he causes damage, cannot be prosecuted under this Act. Moreover, a user must not merely access computers and view data, but must actually do something with the data;[342] mere onlookers for curiosity's sake cannot be prosecuted.[343] Additionally, courts have carved out an exception for a "permissible purpose"; even if a user, without authorization, accesses data and causes damage, if there is a permissible purpose there can be no prosecution under the CFAA.[344] On a pragmatic

339. *Id.*

340. The question of how much control is appropriate has dominated debate since the passage of the 1984 Act. Representative William Nelson postured that the conflict between the need for legislation and the need for protection of rights posed by the introduction of computers in broad society was analogous to the conflicts posed by gun legislation; "[c]omputers may not commit crimes," he stated,

> any more than guns commit crimes. But we have to be realistic—there are people who will commit crimes with guns if they are readily available, and there are people who will commit crimes with computers as they become ubiquitous in our society. . . . [We cannot] address the problem of crime by banning either.

132 CONG. REC. H3277 (daily ed. June 3, 1986) (statement of Rep. Nelson). And with great foresight he added "Americans may not now be as attached to their computers as they are to their guns, but I suspect they will be inseparable before too long." *Id.*

341. *See* Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495 (D. Md. 2005).

342. *See* 18 U.S.C. § 1030(a)(4) (2000); United States v. Ivanov, 175 F. Supp. 2d 367, 371 (D. Conn. 2001).

343. *See* United States v. Czubinski, 106 F.3d 1069, 1076–77 (1st Cir. 1997) (stating that although IRS employee unquestionably exceeded authorization while browsing a confidential taxpayer file, because he did not obtain anything of value or use the information in any way, his conviction for wire fraud and computer fraud was reversed). However, the value of the precedent of this case is slight because the holding centers mostly around wire fraud. *See* P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 508–09 (3d Cir. 2005) (holding that former employees accessing employers' computer system is not illegal absent any evidence of what was viewed or taken).

344. *See* 18 U.SC. § 1030(a)(2)(A); LeBlanc v. Allstate Ins. Co., No. Civ.A. 99-2724, 2000 WL 825683 (E.D. La. June 22, 2000) (holding that an insurance company is not prohibited from obtaining credit reports on its insurees in connection with insurance claims investigations); Edge v. Prof'l Claims Bureau Inc., 64 F. Supp. 2d 115, 118 (E.D.N.Y. 1999) (holding a debt collection agency did not violate the CFAA when accessing a debt guarantor's credit report on a computer because it was for a

level, "Hsu believes that the elimination of the threshold would not result in prosecutions where no true federal interest lies because prosecutors must exercise daily discretion regarding the use of investigative and prosecutorial resources."[345] Consequently, strong protections against overeager prosecutors would still exist even absent the $5000 minimum threshold.

Congress intended that the CFAA would protect individuals "from harm caused by the improper disclosure or use of personal information."[346] It created essentially two thresholds for federal prosecution to this end: the $5000 minimum and the special federal interest. Eliminating the $5000 minimum is consistent with this rubric. Within a modern interpretation of the Commerce Clause, all Internet crime involves a channel of interstate commerce; this in itself is a special federal interest.[347] Therefore, the Commerce Clause provides that federal jurisdiction should be triggered by the inherently interstate nature of the act without the need to rely on a monetary threshold. Federal prosecution under the power of the Commerce Clause demands there be a federal interest at stake; protection of the safety and security of the Internet is certainly in the federal interest.

The $5000 threshold is overly burdensome to that end. When dealing with information, the litmus test for federal jurisdiction of monetary amount does not accurately distinguish important from unimportant information,[348] and therefore renders the statute fatally underinclusive. In the same way, Congress has amended and created statutory provisions to adapt to changes in the cyber environment in the past,[349] Congress should remedy the flaw in the cyber criminal code by eliminating the $5000 threshold requirement.

Elimination of the threshold minimum would also provide a single point of reference to prosecutors,[350] which in turn, would give better understanding of the scope of the problem. Congress intended the CFAA to

"permissible purpose").

345. Interview with Wesley L. Hsu, *supra* note 278.

346. Privacy and National Information, *supra* note 279, at 4363.

347. Where a regulated activity has an effect on interstate commerce the government must show that effect is substantial to trigger Commerce Clause jurisdiction. This is not the case for channels of interstate commerce; the effect on the channel is enough in itself to justify federal regulation. *See* United States v. Lopez, 514 U.S. 549, 558–59 (1995).

348. *Legislative Analysis*, *supra* note 27.

349. For example, Congress eliminated the $1000 threshold for hacking crimes on government computers in 1994 and created the Economic Espionage Act in 1996 to respond to the changing nature of information technology. *See* discussion *supra* Parts III.A.1, III.A.3.

350. *See* Privacy and National Information, *supra* note 279; discussion *supra* Parts III.A.1, III.A.3.

allow prosecutors to "swiftly trace a cyber attack back to its source and appropriately prosecute"[351] without the need to continually parse the criminal code.[352] In order for law enforcement and federal agencies to prevent crime in the future, they require a comprehensive database that compiles accurate data regarding cyber attacks;[353] efficient prosecutions under one statute would effectively allow the creation of a reliable database. Partnerships between prosecutors, law enforcement, and industry facilitated by federal intervention help "develop early awareness of, and a coordinated, proactive response to, the [cyber] crime problem. The cyber crime problem is constantly changing, requiring law enforcement to develop a flexible and dynamically evolving approach as well."[354] Consequently, elimination of the threshold provides tools not only to fight cyber crime currently, but also to predict and improve the tools for fighting cyber crime in the future.

In 1996, Congressman Leahy declared that "Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime."[355] Over the past two decades, Congress has met that goal by amending the CFAA to reflect the current state of cyber crime. In 2008, the state of cyber crime has again changed. As computers continue to evolve in their methods of creation and storage of valuable information, Congress must again modernize the criminal provisions to protect this irreplaceable commodity.

B. SPIM

Instant messaging services are rapidly increasing in popularity and crimes using them are following close behind. Nearly half of all Internet users use some form of instant messaging.[356] Among teenagers that number is much higher; "instant messaging has become the digital communication backbone of teens' daily lives."[357] According to the Pew Report, 75 percent

351. *See* Kyl Statement, *supra* note 18.

352. *Legislative Analysis*, *supra* note 27.

353. Mueller, *supra* note 24.

354. *The FBI's Cyber Division: Hearing on H.R. 2517 Before the Subcomm. on Cts., the Internet, and Intellectual Property*, 108th Cong. (2003) (statement of Jana D. Monroe, Assistant Dir., FBI Cyber Div.).

355. S. REP. NO. 104-357, pt. II, at 5 (1996).

356. SHIU & LENHART, *supra* note 100, at 3 (noting that 42 percent of Internet users—more than 53 million American adults—report using instant messaging at least once).

357. AMANDA LENHART, MAY MADDEN & PAUL HITLIN, PEW INTERNET & AM. LIFE PROJECT, TEENS AND TECHNOLOGY iii (2005), *available at* http://www.pewinternet.org/pdfs/

of online teenagers, or approximately two-thirds of *all* American teenagers, use an instant messenger every day.[358] Instant messengers are not only used for conversation; but also, among teenagers, 50 percent have used an instant messenger to send a link to an article or clip, 45 percent have sent a photo or document, and 35 percent have sent music or a media file.[359]

The percentage of adults who have ever used instant messaging is lower—42 percent—but, of those "53 million American adults, 12 [percent]" still use an instant messenger on a daily basis.[360] One of the fastest growth areas for instant messaging is the workplace.[361] The Radicati Group, a technology market research firm, "determined that seventy percent of businesses have employees who use instant messaging, and half of them use public providers in which the message bypasses the company's own security, archiving, auditing, encryption and logging features."[362]

The growing prevalence of instant messaging in the home and workplace creates vast opportunities for spammers to target the unwary instant messenger. Ironically, the federal and industry focus on spam, "has painted e-mail spammers into a corner like never before and incited them to find other ways to try and reach our membership online," according to Nicholas Graham, a spokesperson for America Online.[363]

Because many instant messengers do not have a domain name associated with the program, many spIM crimes cannot be prosecuted under the CAN-SPAM Act. It is difficult to fill the gap left by the CAN-SPAM Act with existing legislation due to the difficulty of proving the crime with these statutes. Instant messaging occurs in real time, meaning it is instantaneous, unlike e-mail which can sit on a server for any length of time before delivery. One way to investigate and track spIM would be to monitor instant messages to catch an act of spIM; this would require the real-time message to be captured while it is being transmitted. This would violate the Federal Wiretap Act and would hinder the ability to implement a broad-scale monitoring system. SpIM could be proved circumstantially

PIP_Teens_Tech_July2005web.pdf.

358. *Id.*

359. *Id.*

360. SHIU & LENHART, *supra* note 100, at 3.

361. *See generally*, Tom Van Riper, *Text-message Generation Entering Workplace*, MSNBC, Aug. 30, 2006, http://www.msnbc.msn.com/id/14576541 (describing the increased entry of text-messaging employees into the workplace).

362. Katherine Flanagan, *Instant Message: Legal Problems Are Ahead as Popularity Increases*, HOUSTON BUS. J., Nov. 7, 2003, *available at* http://houston.bizjournals.com/houston/stores/2003/11/10/focus15.html.

363. Jenifer Saranow, *Angry Over Spam? Get Set for Spim*, WALL ST. J., Dec. 31, 2003, at D5.

through the messaging service's records or through screen captures of the spIM itself, yet no existing statute is an easy fit for this crime. For example, the mail and wire fraud statutes, the general catchall provisions for cyber crime, may be difficult to apply because the danger of spIM can be the overwhelming annoyance to the user and the taxation to the server; this does not necessarily constitute a fraud or conspiracy to commit a fraud. Similarly, the CFAA is not applicable to all spIM; without a protected computer, the current CFAA is not applicable to this crime.

The demographics of instant message users require that spIM be taken seriously. Teenagers and children, prolific instant messenger users, are easy targets for spIMmers. Businesses also present new and appealing venues to spIMers as gaining access to a business's network opens new sources of information and avenues of attack.

SpIM is a serious problem and will continue to be so unless there is some way to effectively prosecute and deter this crime. Because current statutes are unable to fill the gap in the CAN-SPAM Act, it should be revised to include spIM. The best solution is the elimination of the domain name requirement of an electronic communication. This revision would not unjustifiably broaden the scope of the CAN-SPAM Act or permit prosecutorial overzealousness. This would also eliminate the need to create a new statute. The CAN-SPAM Act can adequately reach the elements of a spIM crime provided its definition allows it to reach instant messaging. Technology has advanced to a point where the government is now forced to respond to a crime rather than prepare for its attack in the future. SpIM is here now, and its inclusion in the CAN-SPAM Act is a necessary step to arm prosecutors and investigators with the essential tools to fight back.

C. PHISHING PROVISION

Phishing is a difficult crime to prosecute. Most prosecutions can only take place *after* someone has been defrauded. The average spoofed Web site is online for less than six days, leaving criminals "plenty of time to cover their tracks" before a prosecution is even considered.[364] Although quick to come and go, the effects of phishing cannot be ignored; the mere threats of these attacks undermine consumer confidence in the Internet, which harms e-commerce and secure transactions.[365]

Currently, many phishing crimes are prosecuted under wire fraud

364. 151 CONG. REC. S1796, 1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

365. *See id.*

statutes. However, this is in some ways an inefficient method because it does not reach all elements of the phishing crime. State measures are also not sufficiently broad. The jurisdictional roadblocks set by the interstate nature of phishing crimes limits a state's ability to pursue and prosecute the crime.[366] Phishing presents a "new enough territory" to merit specificity in the law without fear of duplicating laws that prohibit fraud and identity theft.[367]

In 2005, Senators Patrick Leahy, Ken Salazar, and Charles Schumer proposed the Anti-Phishing Act of 2005, which addressed the crimes of phishing and "pharming."[368] As of April 2008, this proposal has yet to receive a hearing. The proposed law would impose a fine or imprisonment or both for a person who "creates or procures the creation of a website or domain name that represents itself as a legitimate online business, without the authority or approval of the registered owner of [such] business; and (2) uses that website or domain name to [solicit] means of identification" from any person.[369] In addition, the proposed law would impose a fine or imprisonment for a person who knowingly with the intent to engage in an activity consisting of fraud or identity theft under Federal or State law sends an electronic mail message that: "(1) falsely represents itself as being sent by a legitimate online business;" (2) includes an Internet location tool referring or linking users to an online location of the World Wide Web that falsely purports to belong to or be associated with a legitimate online business; and (3) solicits means of identification from the recipient.[370]

The proposed legislation does not contain a monetary threshold as a jurisdictional requirement or as an element of the crime because phishing crimes have two victims: the consumer and the spoofed company. While the consumer's damages are more easily alleged, "the reputational damages that a business incurs as the result of a phishing scam are often much more difficult to quantify."[371] A monetary threshold would unnecessarily limit the class of victims.

This proposed law would close the gap and protect the integrity of the

366. *See* discussion *supra* Part II.B.3.

367. *See We're Just Phish to Them*, *supra* note 104.

368. S. 472, 109th Cong. (2005). "Pharming" is a crime that attacks Web browsers and the Internet's addressing system such that a user could type in a desired Web site in a web browser and be directed to a phony site with the same result of clicking on a phony link in a phishing attack. 151 CONG. REC. S1796, 1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

369. S. 472 § 1351(a).

370. S. 472 § 1351(b).

371. Stevenson, *supra* note 112, ¶ 6 (citing Karen Greenstein, *Defending Your Brand from E-mail Spoofs—Powerpoint Slides*, 784 PLI/PAT 271, at 279–80 (2004)).

Internet by providing a mechanism to charge a phisher for spoofing a Web site. The proposed legislation would criminalize the sham Web sites that are the true scene of both phishing and pharming crimes.[372] Moreover, a specialized statute would strengthen investigators' and prosecutors' abilities to protect Internet users in two ways. First, a specialized statute will allow agents to act quickly to investigate a phishing crime immediately after a Web site has been spoofed, instead of being forced to wait until a fraud has been committed under the wire and mail fraud statutes. Second, the specialized statute will allow for coordination of the investigation between state and federal branches of government, facilitating a faster and more efficient response to phishing schemes.

This proposal generated support, but little action, since its introduction in 2005, and died in committee.[373] In February 2008, Senator Olympia Snow introduced the Anti-Phishing Consumer Protection Act of 2008. This bill aims to prohibit the "collection of identifying information of individuals by false, fraudulent, or deceptive means through the Internet[] . . . to provide the Federal Trade Commission the necessary authority to enforce such prohibition, and for other purposes."[374] This bill was referred to the Congressional Committee on Commerce, Science, and Transportation in February 2008, where it still remains as of July 2008.[375]

Prosecutors' inability to efficiently address this damaging and prevalent crime costs the U.S. economy billions of dollars each year.[376] Perhaps more damaging is the door it opens to the future of identity theft. Ideally, cyber law must anticipate the next step in cyber crime rather than lag behind the curve, and this legislation is a necessary step.

VI. CONCLUSION

The evolving cyber environment impacts all aspects of our society and economy and presents a complex set of challenges for lawmakers. The Internet is constantly shape shifting,[377] and it is impossible to foresee the

372. 151 CONG. REC. S1796, 1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

373. *See* Status Report, S. 472, 109th Cong., http://www.thomas.gov (search "Bill Number" for "S. 472"; then follow "Bill Summary & Status" hyperlink).

374. Anti-Phishing Consumer Protection Act of 2008, S. 2661, 110th Cong. (2008).

375. *See* Status Report, S. 2661, 110th Cong., http://www.thomas.gov (search "Bill Number" for "S. 2661"; then follow "Bill Summary & Status" hyperlink).

376. Total amount of loss is estimated at various levels from $150 million to $1.2 billion each year. RANDALL JACKSON, GEORGE MASON UNIV. SCHOOL OF LAW, K-12 EDUCATION AND CRITICAL INFRASTRUCTURE (2005), http://cipp.gmu.edu/research/K-12EducationCI.php.

377. New opportunities for cyber crime present themselves all the time; instant messaging, mobile phones, and online communities are likely the foreseeable next victims of cyber crime. *See* Voight,

nature and scope of all of the opportunities now and in the future for cyber criminals. Lawmakers at every level of government will need to watch and study the nature of our interactions with and via computers and networks adapting laws to deal with the most pressing risks as they become apparent. Cyber crime's potential for enormous cost to the U.S. economy, society, and national defense demands that Congress undertake constant vigilance and make every effort to develop feasible solutions to new problems. The elimination of the $5000 threshold requirement in the CFAA, and the addition to the U.S. Code of provisions for spIM and phishing are appropriate steps that should be taken now to equip federal prosecutors and law enforcement with additional tools necessary to stem crime in today's cyber world.

supra note 16.