PRIVATE ENFORCEMENT OF CYBERCRIME ON THE ELECTRONIC FRONTIER

MICHAEL L. RUSTAD*

Prior technological advances—the automobile, the telegraph, and the telephones, for example—have brought dramatic improvement for society, but have also created new opportunities for wrongdoing. The same is true of the Internet, which provides unparalleled opportunities for socially beneficial endeavors. . . . By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts.

—President's Working Group of Unlawful Conduct on the Internet[1]

INTRODUCTION

It seems as if everyone is talking about crime on the Internet. With a click of the mouse, hackers have brought "top Web sites like Yahoo, eBay, Amazon, E-Trade and Buy.com to their knees."[2] A wave of cyberattacks have disrupted Internet services, destroyed trade secrets, defaced corporate websites, and infected computers worldwide.[3] A former chemistry graduate student found a security flaw in a commercial website and demanded ransom payments to keep quiet about it.[4] Hackers on the borderless

* Michael Rustad, Ph.D., J.D., LL.M. is the Thomas F. Lambert Jr. Professor of Law and Director of the High Technology Law Program at Suffolk University Law School in Boston. I would like to thank Suffolk University Law School students Shannon Knight, Ron Kaplan, Jessica Natale, Anne-Marie Panone, William Stigler and Anna Zubova for their considerable help with this piece. Anna Zubova cite checked the article and also provided valuable research on federal criminal law statutes and cybercrime in Eastern Europe. I would also like to thank my wife Chryss Knowles for her editorial work. Julie Ross, Esquire, of the Massachusetts Attorney General's Computer Crime Unit made important contributions as well. Anita Sharma, Esquire, provided useful editorial suggestions as well. I would also like to thank Carolyn Ko, Executive Editor of the *Southern California Interdisciplinary Law Journal* for her editorial suggestions.

[1] U.S. DEP'T OF JUSTICE, THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET: A REPORT OF THE PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (Mar. 2000).

[2] Scott Rosenberg, *The Net Scare*, Salon, *at* http://www.salon.com/tech/col/rose/2000/02/10/web_attacks/index.html (Feb.. 10, 2000).

[3] Hacking is broadly defined as "the act of penetrating computer systems to gain knowledge about the system and how it works." Revelation Loa-Ash, *The Ultimate Beginner's Guide to Hacking and Phreaking*, ProAc Maniac Club, *at* http://www.proac.com/crack/hack/files/starthak.txt (Aug. 4, 1996). The motives to "hack" into computer systems are diverse. Ethical hackers, in contrast to dark-side hackers or cybercriminals, hack into networks in order learn about computer security. *See, e.g.*, Legion of Ethical Hacking, *A Hacking Group with Ethics*, *at* http://www.geocities.com/SiliconValley/Circuit/2644/LEH/ (last visited Jan. 24, 2002).

[4] Brian McWilliams, *Alleged E-Commerce Extortionist to Plead Not Guilty*, NEWSBYTES, *at* http://www.newsbytes.com/news/01/166714.html (June 11, 2001).

Internet have obtained unauthorized access into computer systems to rob banks, infringe copyrights, commit fraud, distribute child pornography, and plan terrorist attacks.[5] Spoofing,[6] piggybacking,[7] wire-tapping, data diddling,[8] viruses,[9] salami-type,[10] e-mail flood attacks,[11] and password sniffing[12] are all information-age crimes rarely prosecuted because there are relatively few high-tech crime units capable of investigating these offenses.

On any given day, a sampling from newspaper and trade publications reports of cybercrime convictions confirms that there is a cybercrime wave threatening our information-age economy: *Former Cisco Employee Pleads Guilty to Exceeding Authorized Access to Obtain Information from Cisco's Computer Systems*;[13] *New York City Computer Security Expert Convicted by Jury of Computer Hacking and Electronic Eavesdropping*;[14] *Employee of*

---

[5] U.S. DEP'T OF JUSTICE, FREQUENTLY ASKED QUESTIONS AND ANSWERS ABOUT THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (Dec. 1, 2000).

[6] "IP spoofing is when an attacker compromises the routing packets to direct a file or transmission to a different destination." Ken Brandt, *Cracker Exploits: Battle Plans*, SECURITY, *at* http://www.infosecuritymag.com/articles/march01/features4_battle_plans.shtml (Mar. 2001).

[7] The "Back Orifice" program created by the Cult of the Dead Cow hackers piggybacks on another program to enter into a computer system. Akweli Parker, *The Electronic Threat: Welcome to the High-Tech World of Corporate Spying Where an Alarm Clock Might Really Be a Video Surveillance Camera. Is Your Company Safe from Snoopers, or Does It Need a Wake-up Call?*, VIRGINIAN-PILOT, Jan. 18, 1999, at D1.

[8] Data diddling is the practice by employees and other knowledgeable insiders of altering or manipulating data, credit limits, or other financial information for financial gain. *See* Michael Becket, *Cybercops on Computer Beat with Computers Increasingly Being Used for Crime, the National High-Tech Crime Unit Has Been Formed with Pounds 25m to Build an 80-strong Team*, DAILY TELEGRAPH, April 23, 2001, at 31. *See also* M.E. Kabay, *INFOSEC '99: The Year in Review*, INFO. SECURITY, Dec. 1999, at 25 (reporting case of twin Chinese brothers sentenced to death for data diddling scheme which resulted in fraudulent transfer of funds).

[9] A virus is "[a] program or piece of code that is loaded without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade." *Virus*, Webopedia, http://www.webopedia.com/TERM/v/virus.html (last modified Oct. 18, 2001).
A macro virus is defined as:

> A type of computer virus encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages. These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.
>
> According to some estimates, 75% of all viruses today are macro viruses. Once a macro virus gets onto your machine, it can embed itself in all future documents you create with the application."

Macro virus, Webopedia, http://webopedia.internet.com/TERM/M/macro_virus.html (last modified Oct. 17, 2001).

[10] Salami attack is defined as a "series of minor computer crimes—slices of a larger crime—that are difficult to detect and trace." *The Tech Word Spy*, Logophilia, *at* http://www.logophilia.com/TechWordSpy/index.html (last visited Nov. 16, 1999).

[11] "'Mail-flood attacks' occur when so much [e-]mail is sent to a target that the transfer agent is overwhelmed, causing other communication programs to destabilize and crash the system." Brandt, *supra* note 6.

[12] Password sniffing involves using password sniffing programs to monitor and record the name and password of network users as they log in and impersonating the authorized users to access restricted documents. *Crime on the Internet*, Jones Telecommunications & Multimedia Encyclopedia, *at* http://www.digitalcentury.com/encyclo/update/crime.html (last visited Aug. 8, 2001).

[13] Press Release, U.S. Dep't of Justice, Former Cisco Employee Pleads Guilty to Exceeding Authorized Access to Obtain Information from Cisco's Computer Systems, *available at*, http://www.cybercrime.gov/MorchPlea.html (Mar. 21, 2001) [hereinafter Cisco Press Release].

[14] Press Release, U.S. Dep't of Justice, New York City Computer Security Expert Convicted by Jury of Computer Hacking and Electronic Eavesdropping, *available at*, http://www.cybercrime.gov/OQUENDOconvict.htm (Mar. 7, 2001).

Oklahoma ISP Pleads Guilty to Unauthorized Access Charge;[15] *'Global Hell' Hacker Sentenced to 26 Months Imprisonment*;[16] *Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System*;[17] *Darkside Hacker Sentenced to 21 Months in Prison*;[18] *Former Computer Network Administrator Guilty of Unleashing $10 Million Programming 'Timebomb;'*[19] and *Creator of 'Melissa' Computer Virus Pleads Guilty in New Jersey to State and Federal Charges*.[20]

Computer crime can be classified by the type of harm, the geographic location, the target, and the perpetrator,.[21] The harm caused by computer intrusion may consist of financial loss, invasion of privacy, information theft, destruction of trade secrets, meltdown of computer hard drives, or even threats to public health or security.[22] Computer intrusions originate both in the United States and in offshore havens, and target both private and public institutions. Private attacks inclu1ude attacks on corporate websites or computer networks, such as the recent intrusions by ex-employees into the GTE [23] and Cisco corporate computers.[24] The vast majority of computer intrusion cases prosecuted by the U.S. Department of Justice involve attacks on government computer networks. Public, or government, intrusions include intrusions into NASA Jet Propulsion Lab[25] and U.S. Postal Service computers,[26] and a hack attack on American and Israeli computers.[27] The perpetrators of computer intrusions may be bored juveniles, disgruntled employees, corporate spies, or organized crime networks. Many computer intrusions, however, are undetected and undetectable due to the failure of private and public cybercrime enforcement.

---

[15] Press Release, U.S. Dep't of Justice, Brian K. West, Employee of Oklahoma ISP, Pleads Guilty to Unauthorized Access Charge Under 18 U.S.C. § 1030(a)(2)(e), *available at* http://www.cybercrime.gov/WestPlea.htm (Sept. 24, 2001).

[16] Press Release, U.S. Dep't of Justice, "Global Hell" Hacker Sentenced to 26 Months Imprisonment, *available at* http://www.cybercrime.gov/gregorysen.htm (Sept. 6, 2000).

[17] U.S. Dep't of Justice, Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System, *available at* http://www.cybercrime.gov/bloomberg.htm (Aug. 14, 2000).

[18] Press Release, U.S. Dep't of Justice, "Darkside Hacker" Sentenced to 21 Months in Prison, *at* http://www.cybercrime.gov/miffle2.htm (Jul. 24, 2000).

[19] Press Release, U.S. Dep't of Justice, Former Computer Network Administrator Guilty of Unleashing $10 Million Programming "Timebomb," *available at* http://www.cybercrime.gov/njtime.htm (May 9, 2000).

[20] Press Release, U.S. Dep't of Justice, Creator of "Melissa" Computer Virus Pleads Guilty to State and Federal Charges, *available at* http://www.cybercrime.gov/melissa.htm (Dec. 9, 1999).

[21] U.S. Dep't of Justice, Computer Crime and Intellectual Property Section, *Computer Intrusion Cases*, *at* http://www.cybercrime.gov/cccases.html (last visited Nov. 16, 2001).

[22] This typology is based upon a classification of computer intrusion cases compiled by the United States Department of Justice. *Id.*

[23] Press Release, U.S. Dep't of Justice, Ex-GTE Employee Pleads Guilty to Intentionally Damaging Protected GTE Computers, *available at* http://www.cybercrime.gov/VentimigliaPlea.htm (Mar. 20, 2001).

[24] Cisco Press Release, *supra* note 13.

[25] Press Release, U.S. Dep't of Justice, Hacker Pleads Guilty in New York City to Hacking into Two NASA Jet Propulsion Lab Computers Located in Pasadena, California, *available at* http://www.cybercrime.gov/rolex.htm (Dec. 1, 2000).

[26] Press Release, U.S. Dep't of Justice, Texas Man Is Indicted for Unlawfully Accessing Computers of U.S. Postal Service, State of Texas, and Canadian Department of Defense, *available at* http://www.cybercrime.gov/Vahacker.htm (Oct. 12, 2000).

[27] Press Release, U.S. Dep't of Justice, Israeli Citizen Arrested in Israel for Hacking U.S. and Israeli Government Computers, *available at* http://www.cybercrime.gov/ehudpr.htm (Mar. 18, 1998).

Cybercrime statutes, sentencing guidelines, and probation guidelines need to address rapidly evolving forms of nonutilitarian cybercrimes—the Internet's equivalent to juvenile delinquency. One issue is whether sentencing guidelines should be adjusted upward for nonutilitarian hackers who cause serious societal harm.[28] A downward departure from an otherwise applicable guideline range could be provided for nonutilitarian intrusions by young hackers who do not interrupt businesses or cause any substantial economic loss. Young delinquent hackers, or "script kiddies," are chiefly motivated by thrill seeking, rather than any of Merton's modes of adaptation.[29] Another form of cybercrime, the defacing of corporate websites, is a form of resistance against globalization and corporate hegemony.

Law enforcement resources in cyberspace cannot keep pace with sophisticated cybercrime subcultures in anonymous offshore havens.[30] As soon as Internet-related criminal statutes are drafted, cybercriminals employ new software tools to attack computer systems. The expanded use of private "cybercops" and "private attorneys general," whose efforts in prosecuting a private suit for an individual client or class of clients also benefits the public,[31] will have to fill the enforcement gap in preventing and punishing wrongdoing on the electronic frontiers.

This Article argues that tort remedies[32] will have the potential to fill the enforcement gap in cyberspace, especially where law enforcement agencies have not addressed high-tech issues. Tort remedies are more flexible than criminal law and can be updated more easily to adapt to cyberspace. Tort law carries no death penalty and cannot incarcerate a defendant. Instead, it offers the remedy of punitive damages—civil punishment in the form of monetary damages proportional to the wealth of the defendant. Tort remedies adapted to Internet wrongdoing will play an increasingly important role in punishing and deterring fraud, hacking, and other wrongdoing on the Internet.

---

[28] *See, e.g.*, U.S. SENTENCING COMM'N, FEDERAL SENTENCING GUIDELINES MANUAL § 4A1.3 (2000) (providing for an upward departure where "reliable information indicates that the criminal history category does not adequately reflect the seriousness of the defendant's criminal conduct or the likelihood that the defendant will commit other crimes").

[29] For instance, "Mafiaboy," a sixteen-year-old from Montreal, Canada, shut down a number of corporate sites, including CNN. Judy Monchuk, *Business Battling Hacktivists, Cyber Security Big Item for Those Wary of Next Mafiaboy*, LONDON FREE PRESS, Feb. 16, 2001, at D3.

[30] Lack of resources prevents states from prosecuting the theft of trade secrets on the Internet. "As of 1996, at least twenty-four states had criminal statutes directed at the theft of trade secrets . . . . Yet the states often lacked sufficient resources to pursue espionage prosecutions." United States v. Hsu, 155 F.3d 189, 195 (3d Cir. 1998) (quoting James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 186 (1997)).

[31] Associated Indus. v. Ickes, 134 F.2d 694, 704 (2d Cir. 1943). "[A]ny person, official or not, . . . [who] institute[s] a proceeding . . . even if the sole purpose is to vindicate the public interest. Such persons, so authorized, are, so to speak, private Attorney Generals [*sic*]." *Id.*

[32] Torts are civil wrongs that arise from breaches of duty. William Prosser begins his classic treatise on torts with the statement that "[a] really satisfactory definition of tort has yet to be found." WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 1 (3d ed. 1964). An actor is civilly liable for tort damages if his or her conduct: (a) was intended to cause harm; (b) was negligent; or (c) created extrahazardous risks to others. FOWLER V. HARPER, A TREATISE ON THE LAW OF TORTS: A PRELIMINARY TREATISE ON CIVIL LIABILITY FOR HARMS TO LEGALLY PROTECTED INTERESTS § 7 (1st ed. 1933).

Part I of this Article begins with a criminological perspective on cybercrime, and develops a typology of hacking and other closely related cybercrimes drawn from sociological theory and case studies.[33] Section A of Part I is a socio-legal study of the sources of cybercrime extending the work of American sociologist Robert Merton to cyberspace. I argue that new categories of cybercrime are emerging that are not easily categorized by Merton's criminological theory. In this Section, I explain why criminal law will continue to lag behind the dramatic expansion of cybercrime. Section B of Part I examines the reasons why criminal law is an inadequate institution of social control against cybercrime. Part II of this Article argues for a greater role for private 'cybercops' to punish and control cybercrime to close the enforcement gap created by changing cybercrime subcultures.

I. THE TROUBLE WITH CRIMINAL LAW IN CYBERSPACE

Change comes so fast these days that the reaction of the average person recalls the depressive who takes some time off work and heads for the beach. A couple of days later his psychiatrist gets a postcard from him. The message on the card reads: "Having a wonderful time. Why?"

—James Burke, The Knowledge Web[34]

A. ROBERT MERTON'S THEORY OF DEVIANT BEHAVIOR

Émile Durkheim, a founding father of sociology, explained crime as a function of social change in his 1893 book, *The Division of Labor in Society*.[35] Durkheim's concept of anomie is the opposite of "the attachment to social groups" and the "spirit of discipline."[36] In Durkheim's 1897 work, *Suicide*, he argues that inactive or disrupted group life creates "unregulated individuals with 'insatiable appetites' and 'fevered imaginations.'"[37] Durkheim was the first to explain suicide as a sociological phenomenon. In *The Division of Labor in Society*,[38] Durkheim argues that societies may be broadly classified into two types, mechanical solidarity and organic solidarity.[39] Mechanical solidarity is the division of labor common in pre-

---

[33] Cybercrime may be divided into many categories, including the illegal use of cryptography, stock manipulation, offshore scams, e-mail threats, computer viruses, forged e-mail postings, illegal copying of software, and cyber-terrorism. Daniel P. Schafer, Comment, *Canada's Approach to Jurisdiction over Cybertorts:* Braintech v. Kostiuk, 23 FORDHAM INT'L L.J. 1186, 1233 (2000) (noting that cybercrimes include credit card fraud, unauthorized access to computer systems, child pornography, software piracy, and cyberstalking, but the definition is continually evolving). Part I of this article draws largely upon examples from computer hacking and information security crimes. The typology developed applies to many other forms of Internet-related wrongdoing. *Id.*

[34] JAMES BURKE, THE KNOWLEDGE WEB: FROM ELECTRONIC AGENTS TO STONEHENGE AND BACK—AND OTHER JOURNEYS THROUGH KNOWLEDGE 11 (1999).

[35] ÉMILE DURKHEIM, THE DIVISION OF LABOR IN SOCIETY (George Simpson trans., The Free Press 1964) (1893).

[36] Stephen R. Marks, *Durkheim's Theory of Anomie*, 80 AM. J. SOCIOLOGY 329, 329 (1974).

[37] *Id.* at 331.

[38] DURKHEIM, *supra* note 35.

[39] Stan Stojkovic, Book Review, 75 J. CRIM. L. & CRIMINOLOGY 1426, 1426–28 (1984) (reviewing STEVEN LUKES & ANDREW SCULL, DURKHEIM AND THE LAW (1983)) (describing Durkheim's theory of

industrial societies with homogenous dwelling in small villages.[40] In contrast, organic solidarity is the division of labor common in industrialized or urban societies with a manufacturing base.[41]

In the mechanical solidarity of pre-industrial societies, criminal law punishes offenses against the "collective conscience."[42] Durkheim defined the collective conscience as "[t]he totality of beliefs and sentiments common to average citizens of the same society [that] form a determinate system which has its own life."[43] The collective sentiments to which crime corresponds, therefore, must singularize themselves from others by some distinctive property—they must have a certain average intensity. Not only are these sentiments engraved on all consciences, but they are strongly engraved.[44] Because crime offends the collective conscience, an infraction attacks the entire social fabric. In Durkheim's words, "Everybody is attacked; consequently everybody opposes the attack."[45]

Durkheim argued that the collective conscience becomes progressively weaker with the advent of urbanization and industrialization.[46] With the advent of organic solidarity, members of society no longer have a collective conscience. Individuals become isolated in specialized tasks, and source of solidarity becomes the division of labor.[47] Occupational activity "tends to detach the individual from the social group to which we belong."[48] In Durkheim's words, the worker "no longer feels the idea of a common work being done by those who work side by side with him."[49]

Durkheim's sociology of law explained the essence of crime as functional and as arising from the division of labor. Government and its institutions develop with the division of labor.[50] In a society based upon mechanical solidarity, repressive law was the emblematic form of punishment:[51] "Crime . . . consists in an offense to collective sentiments."[52] Durkheim explained that promiscuous intercourse was an offense to the collective sentiments because it threatened the family as a social institution.[53] He argued that the repressive nature of criminal law correlated positively with the threat to society based upon mechanical solidarity.[54] His famous aphorism was: "We must not say that an action shocks the common conscience because it is criminal, rather that it is criminal because it shocks

---

law as progressing from mechanical to organic solidarity and the development of law from repressive to restitutionary form).

[40] DURKHEIM, *supra* note 35, at 77–110.
[41] *Id.* at 111–132.
[42] *Id.* at 79–80.
[43] *Id.* at 79.
[44] *Id.* at 102.
[45] *Id.*
[46] *Id.* at 283.
[47] *Id.*
[48] *Id.* at 361.
[49] *Id.* at 357. Durkheim's study of the division of labor shaped the development of structural-functionalism in sociology.
[50] *Id.* at 359.
[51] *Id.* at 70.
[52] *Id.* at 71.
[53] *Id.* at 77.
[54] *Id.* at 72.

the common conscience. We do not reprove it because it is a crime, but it is a crime because we reprove it."[55] He argued that the division of labor produced anomie: "In effect, when competition places isolated and estranged individuals, in opposition, it can only separate them more."[56] During the transition to an industrial society, anomic breakdowns occur. In the developed industrial society, the division of labor would evolve into a new source of social cohesion.[57] Durkheim argued that crime in an industrial society is linked to the division of labor where the remedies are expanded to include restitution, as well as repression.[58]

Durkheim described crime as a dysfunctional consequence of the deregulation of norms or a state of anomie.[59] Anomie, or normlessness, was likely to be the greatest when societies were undergoing social and technological change.[60] Durkheim theorized that "disruptions presumably reduce the individuals' sense of belongingness, resulting in anomie at a personal level."[61] He blamed anomie on the disintegration of social norms that occurs due to changes in social institutions caused by transformation of the economic base.[62]

Robert Merton updated Durkheim's theory of anomie to explain the rootlessness and social dislocation caused by the Great Depression, which left many without the means to fulfill American goals of success. Merton theorized that anomie was a function of the clash between socially approved goals and the restricted means to obtain them.[63] Merton argued that the American "cultural emphasis on monetary accumulation of monetary success" created a social strain manifested in the strong association between crime and poverty.[64] Merton hypothesized that when vertical mobility was limited, there would be a greater incidence of organized crime such as Al Capone's "amoral intelligence."[65] Merton's typology hypothesizes that individuals seek out one of five modes of adaptation: Conformity, Innovation, Ritualism, Retreatism, and Rebellion.[66]

This Section uses Merton's anomie theory as a starting point for studying criminal intent in cyberspace. The sociological term "subcultures" refers to "groups that share many elements of the dominant culture but maintain their own distinctive customs, values, norms and

---

[55] *Id.* at 81.
[56] *Id.* at 275.
[57] *Id.* at 395.
[58] *Id.* at 69.
[59] ÉMILE DURKHEIM, THE ELEMENTARY FORMS OF THE RELIGIOUS LIFE (Joseph Ward Swain trans., Macmillan Co. 1947) (1915).
[60] *See* Mark Abrahamson, *Sudden Wealth, Gratification, and Attainment: Durkheim's Anomie of Affluence Reconsidered*, 45 AM. SOC. REV. 49, 49 (1980) (describing "Durkheim's theory of how individuals are integrated into society" and how social change produces a state of anomie).
[61] *Id.* (citing sociologist Leo Srole's study of anomie).
[62] *Id.*
[63] Robert M. Merton, *Social Structure and Anomie*, 3 AM. SOC. REV. 672, 673, 676–81 (1938).
[64] *Id.* at 681.
[65] *Id.*
[66] Merton, *supra* note 63, at 676.

lifestyles."[67] Sociologists use the concept of subculture to refer to religious groups, new immigrants, and groups "based on age, wealth, sexual preference, education, and occupation."[68] The Internet, like the Industrial Revolution, has transformed every aspect of our social life, including subcultures of crime.

Merton's theory of blocked mobility,[69] that those with little formal education and limited economic resources are more likely to turn to a life of crime, cannot explain early hackers who were the products of the "anomie of affluence"[70] with ample means to attain American goals of success. The history of hacking provides insight into the motives of Internet-related computer offenses. The first generation of hackers comprised the children of the affluent and most educated segments of American society. Early hackers were largely curious young computer science students, creative computer programmers who later became professors of computer science, software developers, network administrators, and creative entrepreneurs such as Bill Gates, who launched the personal computer revolution.[71] Among the first hackers were MIT students who accessed computers without authorization to satisfy intellectual curiosity.[72] Dorothy Denning's empirical study of people referring to themselves as hackers concluded that hackers were a diffuse group with complex values.[73] Her interviews with hackers confirmed that many were ethical, in the sense that they were motivated primarily by the desire to further understand computer systems, security, and networks, rather than by the desire to use computers to commit financial crimes.[74]

Ethical hacking culture has devolved into dark-side hacking, organized crime, and computer addiction, to name a few subcultures. FBI Director Louis Freeh acknowledged that his agency has witnessed "a range of computer crimes ranging from simple hacking by juveniles to sophisticated

---

[67] WILLIAM E. THOMPSON & JOSEPH V. HICKEY, AN INTRODUCTION TO SOCIOLOGY: SOCIETY IN FOCUS 81 (1994).

[68] *Id.*

[69] Merton, *supra* note 63, at 681.

[70] Abramson, *supra* note 60, at 50. Merton noted the anomie of affluence "that can result when 'Fortune smiles.'" *Id.* (citing ROBERT MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 188 (1957)).

[71] John Markhoff, *The Tale of the Tape from the Days When It Was Still Micro Soft*, N.Y. TIMES, September 18, 2001 at C1.

[72] Mark Tamminga, *Technology in Practice; E-Definitions: The Hacker Chronicles*, 21 LAW PRAC. MGMT. 20 (2001); Doug Bedell, *Spreading the GNUs: Free Software Movement Pioneer Hacked over Sloppy Use of Computer Terms*, DALLAS MORNING NEWS, Jan. 11, 2001, at 2F.

[73] Dorothy E. Denning, *Concerning Hackers Who Break into Computer Systems*, Computer Professionals for Social Responsibility, *at* http://www.cpsr.org/cpsr/privacy/crime/denning.hackers.html (last visited Aug. 8, 2001).

[74] *Id.* A hacker was traditionally defined as: "[a] person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most other computer users, who prefer to learn only the minimum necessary. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations." *The New Hacker's Dictionary*, Logophilia, *at* http://www.logophilia.com/jargon/jargon_toc.html (last visited Nov. 15, 2001). A hacker was traditionally defined as: "[a] person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most other computer users, who prefer to learn only the minimum necessary. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations." *Id.*

intrusions . . . by foreign powers, and everything in between."[75] Organized criminal subcultures have long hacked into computer systems to disguise drug deals originating in Colombia and other Latin American countries, as well as in the Middle East.[76] The criminalization of hacking has also extended to the illegal access that was a form of intellectual curiosity in the 1960s and 1970s.[77] The hacking culture of the 1960s has morphed into diverse subcultures of creepy website crawlers, such as "crackers"[78] and other career criminals.

Applying Merton's theory to today's cybercriminal subcultures may be helpful in customizing cybercrime sentencing statutes and guidelines. The existing literature on computer hackers confirms that there is a rich diversity of subcultures, ranging from ethical hackers to organized crime networks and cultural radicals.[79] Today, criminologists agree that hackers constitute diverse subcultures with diverse cultural values, norms, and practices.[80] Paul Taylor, an English criminologist, argues that hacking must be seen as a product of "conflict and contestation between various social groups."[81] Taylor argues that "computer *cognoscenti* are split into two camps: those who either come from or are prepared to co-operate with the computer underground and those to whom the computer underground is an anathema."[82]

Robert Merton stated that everyone has their own adjustment to societal goals and the means to attain them. Table 1, below, summarizes Merton's ideal social adjustments and whether their attainment involves socially approved means and ends. In the remainder of this Section, Merton's typology serves as the starting point for a discussion of cybercrime subcultures, including those who engage in "electronic civil disobedience."

---

[75] *Cybercrime: Before the S. Comm. on Appropriations, Subcomm. for the Dep'ts of Commerce, Justice, State, the Judiciary and Related Agencies*, (Feb. 16, 2000) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress00/cyber021600.htm (Feb. 16, 2000).

[76] Michael Alexander, *Business Foots Hackers' Bill*, COMPUTERWORLD, Dec. 11, 1989, at 1.

[77] Mark Tamminga, *Technology in Practice*, 27 LAW PRAC. MGMT. 20 (2001).

[78] A cracker is generally defined as a "hacker with criminal intent." 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, 192 (2000).

[79] *See generally* Steve Silberman, *Beck Sliced, Diced by Culture Hackers*, WiredNews, *at* http://www.wired.com/news/culture/0.1284.10436.00.html (Feb. 20, 1998) (reporting how a coalition of art academics and pranksters "recycled" musical works protected by copyright law).

[80] *Id.*

[81] PAUL A. TAYLOR, HACKERS: CRIME IN THE DIGITAL SUBLIME, at xi (1999).

[82] *Id.*

Table 1. Robert Merton's Ideal Types of Cultural Means & Ends [83]

Ideal Type of Social Adjustment	Approved Means	Approved Ends
Conformity	+	+
Innovation	-	+
Ritualism	+	-
Retreatism	-	-
Rebellion	+/-	+/-

1. *Websurfers As Conformists*

Conformity occurs when individuals adopt socially-approved goals using socially-approved means. The vast majority of the hundreds of millions of Internet users are "conformists" in Merton's sense because they use the Internet largely for legitimate purposes. Internet conformity includes the use of the Internet to communicate, educate, consult professionals, shop for gifts, and connect with family, friends, and associates. If a majority of Internet users were not conformers, then the e-business world would not be possible. For example, the online selling of goods and services depends on most shoppers using the Internet in an appropriate manner. The first computer hackers used computer intrusions in a socially beneficial way—as a practicum to understand how the system worked. In the early 1960s and 1970s, hacking was the functional equivalent of an advanced course of study for many computer science students.

2. *Innovation: Hacking for Profit*

Some website users use the Internet as an instrument to commit crimes. The dictionary defines "innovation" as the act of introducing "a new device or process created by study and experimentation."[84] Merton defined innovation as a social accommodation by individuals who have "assimilated the cultural emphasis on success without equally internalizing the morally prescribed norms governing means for its attainment."[85] Merton's innovators accept social success goals, but lack the legitimate means to attain them. His ideal innovators were social deviants who employed illicit means to attain financial success.[86] Innovators account for the vast majority of criminals using the Internet as an instrument for illicit

[83] Adapted from Merton. Merton, *supra* note 63.
[84] Dictionary.com, *at* http://www.dictionary.com (last visited Jul. 26 2001).
[85] Merton, *supra* note 63, at 678.
[86] The term "ideal type" is a conceptual device rather than a moral good. The concept of the "ideal type" is a sociological concept used to describe social phenomena. I use the analytical construct of ideal types to describe diverse cybercriminal subcultures extending Merton's modes of adaptation to Internet deviance.

financial gain.[87] Finding the conventional door to success blocked, the innovator uses illegitimate means to attain wealth. The interesting empirical question is why there are relatively few cybercriminals, given the great opportunities for illicit gains on the Internet.

The HBO series "*The Sopranos*" is a fictional account of a contemporary New Jersey crime family that used illicit means to attain the American dream. During the Great Depression, Al Capone and John Dillinger were innovators, as were Bugsy Siegel and the organized crime figures who developed Las Vegas into America's gambling and prostitution capital in the 1950s. Finding the front door to American financial success blocked, organized criminals achieved financial success by entering the mainstream illegally through the back door. Similarly, dark-side innovators use illegitimate means to attain easy riches through hacking.[88] Computer "innovators" flourish where legal institutions are unable to effectively detect cybercrime. Many computer crime statutes focus on deterring the misuse of computers for illicit financial gain.[89]

The law enforcement community has uncovered many Internet crimes originating in Eastern European countries. A twenty-six-year-old Russian programmer was the first defendant to be prosecuted for violation of the 1998 Digital Millennium Copyright Act ("DMCA").[90] He was arrested in July 2001 in Las Vegas, shortly after he finished addressing a major hacker convention.[91] The arrest resulted from a complaint by Adobe Systems to federal law enforcement authorities that the program the hacker wrote violated the DMCA's anti-circumvention and anti-trafficking provisions.[92] Adobe then backed off from its stance that the programmer should not be released on bail, partially as the result of pressure from its own employees,

---

[87] Further empirical study is necessary to verify this hypothesis.

[88] A "dark-side hacker" is a criminal or malicious hacker, also known as a cracker. *The New Hacker's Dictionary*, Logophilia, *at* http://www.logophilia.com/jargon/jargon_toc.html (last visited Jul. 26, 2001). The term "dark-side hacker" was inspired by George Lucas's character, Darth Vader, who was "seduced by the dark side of the Force." *Id.* The implication that hackers form a sort of elite force of Jedi Knights is part of the cultural lore and ideology of hackers. *Id.*

[89] *See, e.g.*, Jeff Nemerofsky, *The Crime of "Interruption of Computer Services to Authorized Users": Have You Ever Heard of It?*, 6 RICH. J.L. & TECH. 23 (2000) (arguing that federal computer crime legislation was directed to financial crimes involving the loss of property as opposed to damages such as denial of service); Charles Victor Lang, Note, *Stolen Bytes: Business Can Bite Back*, 1986 COLUM. BUS. L. REV. 251, 262 (1986) (noting that the Computer and Abuse Act made a criminal's commercial benefit an essential element of the crime). *See also* Gary Spencer, *Computer Tampering Law Interpreted; Court of Appeals Sustains Conviction; Defines 1986 Law As Having Wide Scope*, N.Y. L.J., Feb. 16, 1994, at 1 (noting that the New York legislature's purpose in enacting state computer law was to protect against larceny and fraud versus hacking or computer intrusions).

[90] *Case Advances Despite Pressure*, THE RECORDER, Jul. 24, 2001, at 1. Chapter Twelve of the DMCA, entitled "Copyright and Management Systems," proscribes the circumvention of copyright protection systems. 17 U.S.C. § 1201(a) (2000) (defining the circumvention of a technological measure as "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological protection measure without the authority of the copyright owner"). The DMCA makes it a crime to create or sell technologies that circumvent copyright protection. *Id.*

[91] *Case Advances Despite Pressure*, *supra* note 90.

[92] 17 U.S.C. § 1201.

customers, authors, publishers, and numerous supporters of Internet free speech.[93]

The Russian Republics have been a popular venue for innovative cyberscams involving credit card numbers stolen from websites.[94] A Russian national was arrested earlier this year in Connecticut for penetrating corporate computer networks, stealing credit card numbers, and threatening to harm company computers.[95] Organized hacker groups in the Ukraine gained access to e-commerce computer systems by stealing credit card information.[96] Russia's online population has doubled since 1999 to include an estimated four million Internet users.[97] There is little empirical data concerning the incidence of Internet crime in "have not" nations of the world's online population.[98] Organized cybercriminals in less-developed countries might constitute a significant segment of online fraud, computer crime, and cybersex offenses in cyberspace.[99]

One reason for the high rate of cybercrime in former Soviet bloc countries is that organized criminal groups are becoming more sophisticated, engaging in complex economic fraud, cybertheft, and money laundering.[100] The original wave of organized crime in Eastern Europe was largely composed of violent gangs.[101] Today, white-collar cybercriminals threaten all Internet users. Another reason that cybercrime flourishes in less-developed countries is the lack of an effective law enforcement presence. Eastern European countries do not belong to the European Union and do not typically cooperate with Interpol or other law enforcement entities. Because these countries are not members of the European Union, there is less pressure for them to enact laws to investigate and prosecute cybercrime.[102]

---

[93] Scott Harris, *Russian Programmer Is Released—But Not Free*, INDUSTRY STANDARD.COM, Aug. 6, 2001, LEXIS, News Group Files.

[94] Press Release, Christine Winter, Scams Are Thriving in World of E-Business, SUN-SENTINEL, Feb. 4, 2001, at 1; U.S. Dep't of Justice, *NIPC Advisory 01-003*, *available at* http://www.cybercrime.gov/NIPCpr.htm (Mar. 8, 2001).

[95] Press Release, U.S. Dep't of Justice, Russian National Arrested and Indicted in Connecticut for Penetrating United States Corporate Computer Networks, Stealing Credit Card Numbers, and Extorting the Companies by Threatening to Damage Their Computers, *available at* http://www.cybercrime.gov/ivanovIndict.htm (May 7, 2001).

[96] *See* U.S. Dep't of Justice, *supra* note 94 (noting that "several hacker groups from Eastern Europe, specifically Russia and the Ukraine, have penetrated U.S. e-commerce computer systems by exploiting vulnerabilities" in Microsoft software).

[97] Michael Pastore, *Russia's Online Population*, Cyberatlas, *at* http://www.cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_284191,00.html (July 20, 2001).

[98] The world's online population is now extending to less-developed countries. The United States has thirty-nine percent of the Internet users worldwide with 165.2 million users. China, however, now has 22.5 million users. Michael Pastore, *The World's Online Population*, CyberAtlas, *at* http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html (Oct. 26, 2001).

[99] *See, e.g.*, *Crimes on the Internet on the Rise in Russia*, NEWS BULL., Aug. 23, 2001, LEXIS, News Group File. *See also* Margaret Coker, *Russia Producing Talented Hackers*, PALM BEACH POST, Apr. 15, 2001, at 7A (discussing hackers in Russia and the former Soviet republics); *Justice and Home Affairs: Europol Work Programme for 2002*, EUROPEAN REP., June 30, 2001, LEXIS, News Group File (describing the expansion of Internet crime enforcement to curb crimes originating in Eastern Europe).

[100] *Countries Posing 'Extreme Risk' Are on the Rise, Says Control Risks Group: RiskMap 2001 Forecasts Business Climate*, Business Wire, *at* http://www.businesswire.com (Nov. 2, 2000).

[101] Michael Hedges, *Russian Mobsters Pose Damaging Potential*, SCRIPPS HOWARD NEWS SERVICE, Jan. 18, 2001, LEXIS, News Group File.

[102] *See A Difficult Fight to Wage*, DESERT NEWS, July 27, 2001, at A10.

a. Innovation As Electronic Robbery

Cybercriminal innovators use the Internet as an instrument to commit crime. Thus, the innovator's primary motivation is economic gain, not intellectual curiosity.[103] For example, in December of 2000, an unknown hacker broke into the Creditcards.com website to steal confidential credit card information.[104] "Phone phreaks" hack into telephone systems to unscramble cellular telephone codes.[105] Operators of pornographic websites offer "free tours" of sites while making unauthorized charges against the visitor's credit cards.[106]

The Computer Security Institute's ("CSI") *CSI/FBI Computer Crime and Security Survey* found that financial losses due to computer breaches totaled $265.6 million,[107] double the amount for 1998.[108] These hundreds of millions of dollars in losses fall into two categories: the actual financial gain by cyber-criminal innovators and the cost of hiring information security experts to help companies recover from an intrusion or a virus.

b. Corporate Espionage As Illicit Innovation

Some hackers steal source codes from companies by entering corporate networks remotely: "With a simple e-mail, hackers can easily gain access to a company's crown jewels."[109] Corporate espionage targets known vulnerabilities in systems, allowing remote authors of queries to take unauthorized actions in corporate networks. Microsoft and AOL have both been victimized by such corporate espionage.[110] For example, Microsoft reported an attack involving web server file request parsing.[111] This "vulnerability could allow a malicious user to run system commands on a web server."[112] "The FBI reports that intellectual property losses from foreign and domestic espionage may have exceeded $300 billion in 1997."[113]

---

[103] The ideology of ethical hackers is that their main goal is to learn about computers, telephones, or communities. Hacking is portrayed as a form of continuing education by breaking into networks. The Legion of the Apocalypse, for example, states that their "main goal is to show the public what hacking and phreaking is all about and to reveal confidential information to the hacking/phreaking community so that we can learn more about computers, telephones, electronics etc." Revelation Loa-Ash, *supra* note 3.

[104] Dick Kelsey, *Creditcards.com Hacked, Data Exposed*, Newsbytes, *at* http://www.infowar.com/hacker/hacker_2000.shtml (Dec. 13, 2000).

[105] Michael Myer, *Stop! Cyberthief!*, NEWSWEEK, Feb. 6, 1995, at 36.

[106] *See* FTC v. Crescent Publ'g Group, 121 F. Supp. 2d 311 (S.D.N.Y. 2001) (enjoining unauthorized charges by operators of pornographic web sites).

[107] COMPUTER SEC. INST., 2001 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY (2001), *available at* http://www.gocsi.com/prelea/000321.html.

[108] David Hughes, *Hackers Help Insurers Lead the Way: Risk Management Fundamentals in Cyberspace*, 14 ANDREWS DEL. CORP. LITIG. REP. 12 (2000).

[109] *Id.* (quoting Adam Penenberg, coauthor of *Spooked: Espionage in Corporate America* (2000)).

[110] Jon Swartz & Kevin McCoy, *Corporate Networks Vulnerable, Pros Say*, USA TODAY, *available at* http://www.usatoday.com/life/cyber/tech/cti734.htm (Oct. 30, 2000).

[111] NAT'L INFRASTRUCTURE PROT. CTR., UPDATE TO NIPC ADVISORY 00-060 "E-COMMERCE VULNERABILITIES" (Mar. 8, 2001).

[112] *Id.*

[113] Curtis E. A. Karnow, *Computer Network Risks: Security Breaches and Liability Issues*, COMPUTER L. STRATEGIST, Feb. 1999, at 1.

c. Innovation by the "Enemy Within"

One of the greatest threats to the security of client computers is not the hacker, but the enemy within: trusted company employees, ex-employees, consultants, or other insiders familiar with the computer network.[114] Insiders commit computer crimes to steal money or trade secrets. A study by KPMG Investigation and Security, Inc. concluded that the most significant threat to electronic data comes from "disgruntled employees with intimate knowledge of a company's highly sensitive intellectual property, trade secrets, computer software, business, financial and customer information, and even DOS prevention programs."[115] For example, an ex-employee of a New Jersey engineering firm used his password to destroy data, software, and other intellectual property "worth nearly $11 million."[116] Recently, an ex-GTE employee pleaded guilty to intentionally damaging protected GTE computers.[117]

One IBM advertisement used the fear that a company will lose its trade secrets and valuable proprietary information to sell its information security software.[118] The advertisement, designed to spur sales of IBM's Internet security products and consulting services,

> feature[d] two 20-something hackers who have infiltrated a computer network containing confidential executive compensation information. The young woman hacker observes that the other company vice presidents would be surprised to know what one of the other vice presidents made. Her accomplice says: "They know. I just sent an e-mail to everyone in the company.[119]

---

[114] Chris Bucholtz, *New Security Tools Fight Inside Enemies—Protecting Your Customer's Networks from the Most Dangerous Threat of All—Their Employees*, VARBUSINESS, Sept. 17, 2001, at 49. *See also* Pimm Fox, *Layoffs Can Also Harm the Corporate Net*, COMPUTERWORLD, Sept. 3, 2001, at 22 (discussing potential security threats resulting from former employees); Karen A. Forcht, Daphne Thomas, & Karen Wigginton, *Computer Crime: Assessing the Lawyer's Perspective*, 8 J. BUS. ETHICS 243, 243–46 (1989); David Neal, *Security Threats Begin at Home, Warns KPMG Study*, ZDNet UK, *at* http://www.zdnet.co.uk.news/2001/14/ns-22143.html (Aug. 9, 2001). *See, e.g.*, Xenia Ley Parker, *Understanding Risk*, INTERNAL AUDITOR, Feb. 2001, at 61 (arguing that insiders are the biggest security threat to an organization, accounting for "somewhere between seventy and eight-five percent of security incidents").

[115] Mark A. Rush & Lucas G. Paglia, *Preventing, Investigating and Prosecuting Computer Attacks and E-Commerce Crimes: Public or Private Initiatives and Other Federal Reserves*, 18 COMPUTER & ONLINE INDUS. LITIG. RPTR. 16 (2001).

[116] Parker, *supra* note 7 at 61.

[117] U.S. Dep't of Justice, *supra* note 23.

[118] Heather Led, *Tom Talleur*, E-BUSINESS ADVISOR, Feb. 2001, LEXIS, News Group File. *See also* Peter Delevett, *California-Based DVD Trade Group Wins Injunction*, SAN JOSE MERCURY NEWS, Jan. 22, 2000, LEXIS, News Group File (discussing the impact of injunctions against posting of proprietary information for trade secret protections and free speech rights).

[119] MICHAEL L. RUSTAD & CYRUS DAFTARY, E-BUSINESS LEGAL HANDBOOK 151–52 (2001) (referencing the IBM advertisement). Hackers now have a negative connotation. The term "hacker" was first coined at MIT in the 1960s meaning that the person was a computer virtuoso. Wade Rousch, *Hackers: Taking a Byte Out of Computer Crime*, TECH. REV., Apr. 1995, at 32, 34. A hacker was someone who could design innovative ways around difficult problems. *See id.*

3. *Ritualism: The Microserf Subculture*

Merton's third category of subcultures is ritualists who lower their expectations, living a life without purpose or long-term goals.[120] Ritualists reject goals of success, but conform to socially acceptable means. The classic example of a ritualist is the minimum-wage worker who has little prospect for long-term success. An adult working for a fast food restaurant or cleaning service is an example of a ritualistic mode of adaptation. The computer industry deskills many jobs in order to pay workers less money, making what was once highly skilled work mind-numbingly routine.

Douglas Coupland's novel *Microserfs* is a fictional account of computer professionals or "techno-geeks" who become absorbed in their work as programmers but never manage to fulfill their goals of success.[121] The term "microserf" refers to hackers who have been co-opted into using their hacker skills for commercial computing.[122] Like Merton's ritualist, the microserfs work for low salaries without the prospects of long-term financial success. The microserf plods on at a low-level computer job, despite falling short of American goals of success. A microserf, therefore, is a computer ritualist whose job can only be characterized as a de-skilled occupation with relatively little autonomy. The increased outsourcing of computer services to less-developed countries will result in a new class of microserfs in those countries.

4. *Retreatism: Hacking As an Addiction*

Merton hypothesizes that retreatists, those who reject goals and means, are the least common subculture.[123] In Merton's day, retreatists were social pariahs such as beats, drug addicts, tramps, and chronic drunkards. For today's cyber-retreatists, computers and the Internet are a form of addiction. *The Hacker Manifesto*,[124] a classic article written by a computer hacker, uses the language of an addict to describe his relationship with computer systems:

> I made a discovery today. I found a computer. Wait a second, this is cool. . . .
>
> . . . .
>
> And then it happened . . . a door opened to a world . . . rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought . . . a board is found. "This is it . . . this is where I belong . . ."
>
> . . . .

---

[120] Merton, *supra* note 63, at 673–74.

[121] Heather Mallick, *Microsoft's Techno-Geek Breaks Free*, jam! SHOWBIZ, *at* http://www.chl.ca/JamBooksReviewsM/microserfs_coupland.html (July 16, 1995).

[122] TAYLOR, *supra* note 81, at 23 (noting that microserfs are a new group of hackers co-opted by the computer industry. The term "microserfs" was first coined in Douglas Coupland's novel, *Microserfs*. *Id.*

[123] Merton, *supra* note 63, at 677.

[124] The Mentor, *The Hacker Manifesto, at* http://www.iit.edu/~beberg/manifesto.html (Jan. 8, 1986).

I am a hacker, and this is my manifesto.[125]

Retreatists who break into corporate computer networks are primarily motivated by thrill-seeking, rather than economic gain.[126] "'Recreational hackers' break into computer networks for the thrill of the challenge or for bragging rights in the hacking community."[127] A fifteen-year-old Connecticut juvenile was charged with hacking into the U.S. Air Force computer system that tracks the positions of Air Force airplanes worldwide.[128] He was also charged with breaking into the U.S. Department of Transportation computers at the Volpe Center in Cambridge, Massachusetts and causing $66,000 in economic losses.[129] Another nineteen-year-old hacker from a small Welsh village stole 23,000 credit card numbers, one of which belonged to Bill Gates.[130] The prankster used Gates' credit card to order him a case of Viagra.[131] He justified his actions by explaining that he wished to demonstrate that Internet shopping sites were so vulnerable that it was possible "to teach your grandma" to invade them.[132] A seventeen-year-old Canadian teenager using the name, "Mafiaboy," was sentenced to eight months in a youth detention center for launching denial of service ("DoS") attacks that temporarily disabled websites such as Amazon.com, "CNN.com, Yahoo.com, Ebay.com, and the Web home of computer maker Dell."[133] A Massachusetts teenager caused a regional airport to be shut down by disrupting telephone service when he hacked into the facility's computer system.[134]

Many of the cybercriminals who release computer viruses may also be classified as electronic retreatists, because the authors of viruses, like other computer abusers, are motivated by the thrill of outwitting law enforcement authorities worldwide. A computer virus is a piece of programming code inserted into other programming that causes some unexpected and, for the victim, undesirable event.[135] A virus is programmed to propagate automatically *ad infinitum*.[136] Many viruses masquerade as useful programs. "Trojan horses" received their name from the Trojan horse delivered to the gates of the city of Troy as an ersatz peace offering in Homer's *The Iliad*.[137] When the Trojans brought the horse inside the city

---

[125] *Id*.

[126] *Attrition Defacement Statistics*, Attrition.org, *at* http://www.attrition.org/mirror/attrition/stats.html (last visited, Jan. 2, 2001).

[127] Sinrod & Reilly, *supra* note 78, at 185.

[128] Linda Rosencrance, *Teen Charged with Jacking into Air Force System*, Infowar.com, *at* http://www.infowar.com/hacker/01/hack_042501b_j.shtml (Apr. 25, 2001).

[129] *Id*.

[130] Simon De Bruxelles, *Teenage Hacker Faces Jail over Bill Gates Stunt*, Infowar.com, *at* http://www.infowar.com/hacker/01/hack_042501a_j.shtml (Apr. 21, 2001).

[131] *Id*.

[132] *Id*.

[133] Steven Bonisteel, *Mafiaboy Gets Eight Months for DDos Attacks*, Newsbytes, *at* http://www.newsbytes.com/news/01/170029.html (Sept. 12, 2001).

[134] *Prepared Testimony Before the S. Judiciary Comm.* (May 25, 2000) (statement of James Robinson, Assistant Att'y Gen., Criminal Div. Dep't of Justice).

[135] *What Is a Virus*, Whatis.com, *at* http://whatis.com.htm (last visited Nov. 16, 2001).

[136] *See* United States v. Morris, 928 F.2d 504, 505 n.1 (2d Cir. 1991).

[137] *Trojan Horse*, Webopedia, *at* http://www.webopedia.com/TERM/T/Trojan_horse.html (last modified June 20, 2001).

walls, Greek soldiers appeared from horse's belly and captured Troy. Similarly, a Trojan horse virus is an apparently harmless computer code that masquerades as antiviral software. In reality, it introduces viruses into the target's computer system. A group calling itself "The Cult of the Dead Cow" was the source of *Back Orifice*, the most infamous of the Trojan horses.[138] *Back Orifice* invades computer systems through a benign program, such as an animated greeting card attachment. After the user executes the program, *Back Orifice* copies itself onto the host computer's hard drive.[139]

New viruses appear online each month. Cyberspace criminals introduce destructive codes into computer systems, thereby, usurping control of the system and reading or recording confidential information.[140] For example, the Chinese *Code Red* worm infected 12,000 Web servers in July of 2001 alone, and a second wave emerged in August of 2001.[141] *Code Red* infected computer systems by gaining control over them and permitting the defacing of websites.[142] Electronic mail attachments were used to transmit the virus known as *Chernobyl*, a self-spreading program that infected servers running Microsoft Windows 95 and 98, which had known security vulnerabilities.[143] It is unknown and possibly unknowable who created these viruses or what their motivations were.

The *Melissa* virus of March 1999 infected 1.2 million computers, including one in five businesses, causing $80 million in damages worldwide.[144] Federal prosecutors reached a plea agreement with David Smith, the author of the *Melissa* virus, after he was charged with violating the Computer Fraud and Abuse Act.[145]

5. *Rebellion As "Electronic Civil Disobedience"*

Rebellion is Merton's fifth type of subculture in which societal goals and means are rejected in favor of alternative goals and means.[146] The computer hackers who developed the computer program called "DeCSS," which circumvents the protection system for digital versatile disks ("DVDs") containing motion pictures, refer to their hacking as a form of "electronic civil disobedience."[147]

---

[138] Parker, *supra* note 7. The Cult of the Dead Cow is an example of a hacktivist subculture. *See Cult of the Dead Cow*, Paramedia, *at* http://www.cultdeadow.com (last visited Sept. 6, 2001).

[139] *The Back Orifice "Backdoor" Program*, *at* http://www.nwinternet.com/~pchelp/bo/bo.html (last modified Nov. 4, 1999).

[140] *See, e.g.*, *id.* (noting that "[w]ith Back Orifice installed, absolutely . . . [no] information is safe from loss and/or prying eyes").

[141] Robert Lemos, '*Code Red' Worm Claims 12,000 Servers*, ZDNet UK News, *at* http://news.zdnet.co.uk/story/0,,t269-s2091572,00.html (July 19, 2001); *CERT/CC Incident Notes*, Cert Coordination Center, *at* http://www.cert.org/incident_notes (last visited Oct. 10, 2001).

[142] *Id.*

[143] Keith Bowers & Iolande Bloxsom, *CIH 'Chernobyl' Set to Detonate*, techtv, *at* http://www.techtv.com/cybercrime/viruses/story/0,23008,2246676,00.html (Apr. 23, 1999).

[144] U.S. Dep't of Justice, Computer Crime and Intellectual Prop. Section, *The Melissa Virus*, *at* http://www.usdoj.gov/criminal/cybercrime/compcrime.html (last visited Aug. 13, 2001).

[145] *Id.*

[146] Merton, *supra* note 63, at 677–78.

[147] Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 303 (S.D.N.Y. 2000).

The countercultural radicals of the late 1960s, like today's electronic radicals, eschewed dominant culture, positing alternative values, norms, and institutions. Countercultural radicals rejected traditional nuclear families and experimented with alternative extended family groups with communal lifestyles. Similarly, "hacktivism" is a form of political activism against globalism and corporate control of the Internet.[148] Criminologist Paul Taylor observes that hactivists typically target powerful corporations by posting political messages on their websites.[149]

In one instance, anticorporate collectives defaced company websites "with a range of electronic weapons, from viruses to e-mail bombs, which crash websites by bombarding them with thousands of protest messages."[150] The Swiss hactivist Virtual Monkeywrench described the computer intrusion as hacking for a cause against the "well-oiled running of the corporate machine."[151] Hactivists also broke into the World Trade Organization's computer system during an online press conference of the World Economic Forum.[152] During their highly publicized attack, they downloaded the phone numbers and addresses of 1,400 business and political leaders, including personal information about Bill Gates.[153] Italian hactivists, protesting the increased role of government on the Internet, launched a protest attack against an Italian online share dealing website in April of 2001.[154] Recently, hacktivism has been extended to politically motivated viruses. For example, a virus similar to the *Kournkova* strain was released along with "a message attacking Israeli security forces and calling for an end to violence in the Middle East."[155]

Other hactivists reject societal ideas of intellectual property.[156] Cultural radicals challenge the legitimacy of copyright law in favor of a

---

[148] Stuart Millar, *For Hackers, Read Political Heroes of Cyberspace*, GUARDIAN, Mar. 8, 2001, at 4.

[149] *Id*.

[150] *Id*.

[151] Aorife White, *Hackers Adopt Political Causes to Legitimate Their Targets*, NETWORK NEWS, Feb. 21, 2001, at 18.

[152] *See Hacktivists Motto: Oppose a Policy? Hack the System*, ECON. TIMES, Feb. 9, 2001, LEXIS, News Group File.

[153] White, *supra* note 151.

[154] *Cyberdigest*, JANE'S INTELLIGENCE REV., Mar. 23, 2001, LEXIS, Market & Industry File.

[155] *Id*.

[156] A hacker group was recently sued by the entertainment industry for publishing computer codes to crack DVDs. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000). The hackers devised a computer program called DeCSS that circumvented the devices that used encryption software to protect motion pictures from being copied. *Reimerdes* was the first case filed to enjoin websites from distributing software that permitted the unauthorized copying of movies. In *Reimerdes*, the court ruled that the motion picture studios were entitled to injunctive and declaratory relief against the hackers that posted DeCSS and electronically linked their site to others that posted DeCSS. *Id.* at 346–47. The court rejected the defendants' claim that the Digital Millennium Copyright Act's prohibition of anticircumvention devices did not violate the First Amendment of the United States Constitution. *Id. See also* Ariana Eunjung Cha, *From Teen Hackers to Job Hunters*, WASH. POST, Apr. 17, 2001, at E1. In March of 2001, computer programmers released code designed to "unscramble CSS, the content-scrambling system designed to prevent unauthorized copying of DVDs." *Hack Job*, SCI. AM., May 2001, at 20. The debate over DVD encryption technology pits the entertainment industry against programmers who contest expanded definitions of intellectual property. There is a similar cultural war over Napster, the popular MP3 swapping service. Napster was enjoined by a preliminary injunction ordered by a federal district court judge. A&M Records, Inc. v. Napster, 114 F. Supp. 2d 896, 927 & n.32 (N.D. Cal. 2000). The Ninth Circuit upheld the district court order granting a motion enjoining Napster from loading, transmitting, and distributing sound recordings on the Internet.

countercultural value that "information should be free."[157] One on-line journal, *2600: The Hacker Quarterly*,[158] posts articles on how to "steal an Internet domain name, access other people's e-mail, intercept cellular phone calls, and break into computer systems at Costco stores and Federal Express."[159] The journal claims the protection of copyright law on its online materials, while challenging the extension of copyright protection to DVDs and other digital products. The 2600.com website posted the source and object code for DeCSS,[160] and was later enjoined from posting these codes and from electronically linking their site to other sites posting them because doing so was determined to be a violation of the DMCA.[161] The court rejected the hacker's argument that the DMCA, as applied to computer programs, or code, violates the First Amendment.[162]

The *2600* hacker network recently joined forces with punk rock and free speech activists to challenge overreaching definitions of intellectual property.[163] The *2600* hackers also produced a documentary film about the "Free Kevin" campaign, challenging the federal computer crime prosecution of hacker, Kevin Mitnick.[164] Mitnick was charged with breaking into computer networks and stealing credit card numbers. He was sentenced to another twenty-two months for using cloned cellular telephones and violating the terms of his release for an earlier computer fraud conviction.[165] Mitnick challenged probation restrictions as violating his First Amendment rights, a defense rejected by the Ninth Circuit U.S. Court of Appeals.[166]

Law enforcement officials and prosecutors would likely view hackivists' political ideologies as self-serving rationalizations. Criminals in the "brick and mortar" world frequently rationalize the harm caused by their activities. Cybercrime ideologies are often sophisticated rationalizations for socially destructive acts. Criminologists Gresham Sykes and David Matza identified five types of rationalization: denial of responsibility, denial of injury, denial of the victim, condemnation of the

---

A&M Records, Inc. v. Napster, 239 F.3d 1004, 1029–30 (9th Cir. 2001). The Ninth Circuit found that the trial court did not err in finding that Napster had no fair use defense against claims of contributory and vicarious copyright infringement. *Id.* at 1013–28.

[157] Gary D. Robson, *Am I a Hacker?*, *at* http://www.robson.org/gary/writing/hacker.html (Apr. 1997) (restating the hacker ethic as having the value that "information should be free").

[158] Eric Corley is the founding editor of *2600: The Hacker Quarterly*. *Reimerdes*, 111 F. Supp. 2d at 308. The name "2600" was chosen in honor of phone phreaks' use of the 2600 hertz tone to gain unauthorized access to telephone networks. *Id.*

[159] *Id.*

[160] The Control Scramble System ("CSS") is an encryption based copy protection system for DVDS developed by the motion picture companies. *Id.* at 308. DeCSS is a "software utility or computer program, that enables users to break the CSS copy protection system and hence to view DVDS on unlicensed players and make digital copies." *Id.*

[161] *Reimerdes*, 111 F. Supp. 2d at 304.

[162] *Id.*

[163] Jello Biafra of *The Dead Kennedys* punk rock group gave the keynote speech at a 2600 H2K meeting on July 15, 2000. *Info on H2K2*, H2K, Hackers on Planet Earth, *at* http://www.hope.net (last visited Nov. 16, 2001).

[164] *See id.*

[165] Jack McCarthy, *Hacker Mitnick Could Be Released By Early 2000*, INFOWORLD DAILY NEWS, Aug. 10, 1999, LEXIS, News Group File.

[166] United States v. Mitnick, 1998 WL255343 (9th Cir. May 20, 1998) (unpublished opinion).

condemners, and appeal to higher loyalties.[167] Many rationalization techniques appear in the literature of cultural radical hacking groups such as the *Legion of Doom* or *2600*. Hackers use the rhetoric of freedom of information or speech to rationalize computer trespasses.[168]

Attacks on U.S. Department of Defense ("DOD") websites are probably the product of cultural warfare by foreign-based Internet rebels. The DOD developed firewalls for its computers and networks in the mid-1980s to prevent outside access to classified documents.[169] In a test of the DoD's computer security measures, 7,860 out of 8,932 systems were successfully attacked.[170] Most troubling was that the security managers detected intrusion in only 390 out of the 7,860 systems entered.[171] Although the military was the first beneficiary of Internet technology, it has now become a primary target of radical hackers.[172] The frequency of attacks by foreign governments and rebels not sharing American values is unknown.[173] Over one hundred Chinese websites were defaced by American hackers during the crisis in which twenty-four Americans were held in China after colliding with a Chinese plane.[174]

Today, Ex-hacker members of the *2600* club are increasingly hired by companies as consultants to test the security of computer systems.[175] Ex-hackers who turn their computer skills to conventional means and ends are a rare example of conformity.

6. *Nonutilitarian Hacking*

Merton's theory explains cybercrime as a function of blocked opportunity of individuals with upper class goals and lower class means.[176] His typology, however, does not explain the widespread phenomenon of electronic cyberpunks who hack for nonutilitarian reasons. A large number

---

[167] SUE TITUS REID, CRIME AND CRIMINOLOGY 156–57 (5th ed. 1988) (citing Gresham Sykes & David Matza, *Techniques of Neutralization: A Theory of Delinquency*, *in* THE SOCIOLOGY OF CRIME AND DELINQUENCY 292–99 (Marvin E. Wolfgang et al., eds., 1970)).

[168] Martha Smith, *Global Information Justice: Rights, Responsibilities, and Caring Connections*, 49 LIBRARY TRENDS 519 (2001). *See also* David Fisher, *The Politics of Technology: The Internet Already Has Delivered the New Economy. A New Democracy Is Not Far Behind*, STAR TRIB., Dec. 18, 2000, at D3 (discussing how technology will be affected by traditional notions of democracy).

[169] Gary H. Anthes, *Hackers Stay a Step Ahead*, COMPUTERWORLD, Oct. 17, 1994, at 14.

[170] Stephen Nickson & Jim Kates, *The Reality of Hackers*, 48 RISK MGMT. 50 (2001).

[171] *Id*.

[172] *See generally* Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?*, 22 HOUS. J. INT'L L. 223, 228–29 (2000) (discussing the vulnerability of U.S. military systems and issues of detection and costs associated with the attacks).

[173] There is no case law or commentary on the question of whether the government would be liable for negligent security under the Federal Tort Claims Act for harm caused by negligent information security. The discretionary function exception may be extended to immunize the government of claims for negligent security where there are rapidly evolving standards of information security. *See* William P. Kratzke, *The Supreme Court's Recent Overhaul of the Discretionary Function Exception to the Federal Tort Claims Act*, 7 ADMIN. L.J. AM. U. 1 (1993) (discussing how courts would apply the discretionary function to a wide range of governmental activities).

[174] Michelle Delio, *Crackers Expand Private War*, Wired News, *at* http://www.wired.com/news/politics/0,1283,43134,00.html (Apr. 18, 2001).

[175] *See* Tony Kontzer, *Companies Must Consider Legal Ramifications, Along with Ethics, When They Hire Hackers*, INFO. WEEK, Oct. 23, 2000, at 1.

[176] Merton, *supra* note 63, at 681.

of computer-related crimes involve nonutilitarian motives such as "exhibiting technical expertise, highlighting weaknesses in computer security systems, punishment or retaliation, computer voyeurism, asserting a belief in open access to computer systems or sabotage."[177] DoS attacks are frequently motivated by nonutilitarian thrill seeking.[178] Many nonutilitarian computer crimes are hypothesized to be authored by young male "e-delinquents."[179] The 1995 movie *Hackers* was a "cyberpunk thriller" about teenage hackers outwitting government agents.[180] It portrayed an elite group of teenage hackers with "handles like Zero Cool, Cereal Killer, and Acid Burn."[181] A twenty year-old Northeastern University student from Nigeria was charged with hacking into NASA, the DOD, and a commercial Internet service.[182] He was accused of spraying "cybergraffiti calling for the release of fellow hackers from jail and for war against the FBI."[183] A group of hackers posted "a picture of a jolly fat man wearing nothing but a Santa hat and a smile" on one website.[184] A Brazilian hacker "cracked into more than 100 Brazilian Web sites in January" of 2001 to impress his girlfriend.[185] A juvenile hacker disabled the Worcester, Massachusetts airport, city telephone systems, and a Federal Aviation Administration control tower for six hours.[186] The computer hacker group called "globalHell" goes far beyond mere pranks with its public defacement of websites.[187] Virus-planting delinquents enjoy shutting down corporate servers or infecting millions of home computers.[188] There are no documented cases of defendants planting viruses in an attempt to reap a financial benefit.

---

[177] Michael Hatcher, Jay MacDannell, & Stacey Oslfield, *Computer Crimes*, 36 AM. CRIM. L. REV. 397, 400 (1997).

[178] Jose Martinez, *Experts Say It's a 'Rush' to Hack into Some Sites*, BOSTON HERALD, Feb. 24, 2000, at 6 (describing nonutilitarian hacking by college students in the Boston area who describe themselves as "phreaks" or "script kiddies"); Anne Saita, *Deep Digital Cover*, INFO. SECURITY, Oct. 2001, at 22; Anne Saita, *Protection Starts with Prevention*, INFO. SECURITY, Oct. 2001, at 52; John Yaukey, *'Blended Threats' Latest PC Menace*, GANNETT NEWS SERVICE, Dec. 21, 2001 (citing example of Israeli teens mounting DoS attack from Israel).

[179] Shannon Sutherland, *Hackers Open for Business: The Internet Paradox and Pandora's Box*, NAT'L POST, Sept 18, 2000, at E1.

[180] *See Hackers*, MovieWeb, *at* http://movieweb.com/movie/hackers (last visited Nov. 16, 2001).

[181] *Id*.

[182] David E. Kaplan, *Hacking: Ain't No Joke*, U.S. NEWS & WORLD REP., Aug. 28, 2000, at 44.

[183] *Id*.

[184] Jennifer McKee, *Hackers of a Different Color*, ALBUQUERQUE J., Feb. 11, 2001, at 1.

[185] *Id*.

[186] Sean Silverthorne, *Feds Bust Kid Hacker*, ZDNet, *at* http://www.zdnet.com/zdnn/content/zdnn/0318/295928.html (Mar. 18, 1998).

[187] *See* Press Release, U.S. Dep't of Justice, Computer Hacker Sentenced, *available at* http://www.usdoj.gov/criminal/cybercrime/gregorysen.htm (Sept. 6, 2000) (noting that the "globalHell" hackers stole access devices, including Personal Identification Numbers (PIN) combinations and credit card numbers, and maliciously disrupted services).

[188] *See* Reid Goldsborough, *Keeping Hackers Away with Firewalls*, 12 SCHOOL MGMT. & PLAN. 57 (2000); Sutherland, *supra* note 179.

B. INTERNET-RELATED CRIME ENFORCEMENT: A NEW AUDIT

The Internet began as a research project of the United States Defense Department in the 1960s.[189] The system of computer networks was developed as a means of withstanding a nuclear attack, which might disable critical infrastructure.[190] It evolved into a system of interconnected computers used by educational institutions and defense agencies.[191] The National Science Foundation assumed control of the Internet in 1990.[192] The World Wide Web was not created until 1991 when Tim Berners-Lee developed the user-friendly protocols.[193] Thus, cybercrimes such as transmitting viruses, online fraud, identity theft, and hacking are relatively recent developments.

The first appellate court decision to mention the Internet was the 1991 case, *United States v. Morris*.[194] The defendant in that case was Robert Morris, a Cornell University computer science doctorate student researching information security.[195] As a research project, he designed an "Internet worm" or virus that would test the security of computer networks.[196] Morris' computer code copied itself into computer systems and reproduced.[197] He tested his worm by releasing it from a computer science laboratory at MIT.[198] Due to a defect in the program, the worm replicated at a high rate of speed, shutting down the computers of universities, medical facilities, and defense facilities throughout the United States.[199]

Morris took steps to prevent the further spread of the worm. Nevertheless, he was charged with a federal computer crime. A federal district court had little difficulty finding that the government's case satisfied the scienter requirement under the Computer Fraud and Abuse Act of 1986 ("CFAA") and sentenced Morris to three years probation, 400 hours of community service and a $10,500 fine.[200] The court probably considered the mitigating circumstances, that the virus was unleashed for research purposes, in determining Morris's sentence.

In *United States v. Riggs*, a district court upheld a federal wire fraud indictment against a computer hacker who broke into Bell South Telephone Company's ("Bell South") 911 computer files.[201] The hacker gained unauthorized access to the Bell South system by using the accounts of

---

[189] Ben Segal, *A Short History of Internet Protocols at CERN*, *at* http://ben.home.com.cern.ch/ben/TCPHIST.html (Apr. 1995).
[190] *Id*.
[191] *Id*.
[192] *Id*.
[193] *Id*.
[194] 928 F.2d 504, 505 (2d Cir. 1991) (upholding a criminal conviction under the federal computer crime statute for releasing a computer worm).
[195] *Id*.
[196] *Id*.
[197] *Id*.
[198] *Id*. at 506.
[199] *Id*. at 505–06.
[200] *Id*. at 506.
[201] 739 F. Supp. 414 (N.D. Ill. 1990).

persons with legitimate access to the restricted text files.[202] Shortly after hacking into Bell South's computer network, he published pilfered information in the hacker newsletter, "*PHRACK*."[203] The hacker was charged with federal wire fraud and violation of the CFAA.[204] The U.S. Court of Appeals upheld the indictment, rejecting the hacker's defense that he had no intent to defraud when transmitting confidential information.[205] The defendant in *Riggs* was the leader of a group of phone phreaks who had devised a scheme "to defraud Bell South Telephone Company ('Bell South'), which provides telephone services to a nine-state region."[206] In *People v. Casey*, a phone phreak was convicted of using stolen authorization codes to place long distance telephone calls on the International Telephone and Telegraph Network ("ITT").[207]

In *Computer Professionals for Social Responsibility v. United States Secret Service*, an association of computer professionals filed an action against the U.S. Secret Service for violation of the Freedom of Information Act ("FOIA").[208] The complaint alleged that Secret Service agents violated the FOIA by denying Computer Professionals for Social Responsibility's request to release records related to a break-up of the meeting of *2600 Magazine* in the local mall and the detention of its member by agents.[209] The court held that the Secret Service legitimately refused to release the information because it contained the identity of the arrested hackers. Thus, it was covered under an exception to the FOIA.[210]

There is relatively little cybercrime case law outside the fields of child pornography and traditional crime committed by career criminals. A search of WESTLAW and LEXIS uncovered no successful criminal prosecution in a computer virus case other than *United States v. Morris*.[211] Further case law development must precede a more in-depth study concerning cybercriminal intent using Merton's categories.

The poverty of cybercrime cases reflects a substantial enforcement gap between the cybercriminal law on the books and the law in action. Few cybercrimes have been successfully prosecuted because of several interrelated factors, including the problem of anonymity, jurisdictional issues, and the lack of resources in the law enforcement community. Conventional law enforcement does not make cybercrime a priority nor

---

[202] *Id.* at 417.

[203] *Id.*

[204] *Id.* In October 1996, the Economic Espionage Act of 1991 ("EEA") was enacted to punish the theft of trade secrets. Pub. L. No. 104-294, § 101(a), 110 Stat. 3488 (1996) (codified at 18 U.S.C. § 1831–39 (2000)). Today, it would be possible to prosecute computer hackers who steal telephone authorization codes under the EEA.

[205] United States v. Riggs, 967 F.2d 561 (11th Cir. 1992).

[206] *Riggs*, 739 F. Supp 414 at 416.

[207] 225 Ill. App.3d 82 (Ill. App. Ct. 1992).

[208] 72 F.3d 897, 904 (D.C. Cir. 1996).

[209] *Id.*

[210] *Id.*

[211] In contrast, on August 17, 2001, my search on LEXIS using the search terms "child pornography and Internet" yielded 225 citations. *See, e.g.*, United States v. Wilson, 182 F.3d 737 (10th Cir. 1999) (upholding conviction for possession of child pornography); United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996) (discussing a case involving dissemination of child pornography).

does it have the resources to tackle this type of crime. The next Section examines the key cybercriminal statutes and explains why criminal law is unable to effectively control Internet-related wrongdoing.

C. THE ADEQUACY OF CYBERCRIME STATUTES AND SENTENCING GUIDELINES

Criminal law, by its very nature, lags behind technology. One of the difficulties that cybercrime legislation faces is enacting statutes to control rapidly evolving cybercrimes. It is difficult to discover the identity of cybercriminals, who often operate in countries with corrupt governments that encourage Internet crime as a developing industry. Crimes on the Internet cross national borders, creating the need for international cooperation in law enforcement.

Computer crime statutes were first enacted decades after the invention of computers. For example, the United Kingdom enacted the Regulation of Investigatory Powers Act to bring law enforcement into the age of the Internet. It provides law enforcement with new tools to monitor and to intercept criminal activity.[212] The term "computer crime" is defined by the Department of Justice to include "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution."[213] It is not surprising that lawmakers find it difficult to draft effective statutes, as even this definition of computer crime is imprecise.[214] Furthermore, there is "legal lag" in federal and state criminal statutes.[215] Most computer crime statutes are tailored to address situations where innovative computer criminals hack into computers for financial gain, such as Merton's "innovators." In reality, most cybercriminals are employees, ex-employees, or other insiders who exploit their knowledge of corporate computer networks,[216] thus, many cybercrimes could be prevented through the use of better password controls and employee training and screening.[217]

---

[212] Jonathan Little, *The UK Regulation of Investigatory Powers Act*, 5 CYBERSPACE LAWYERS 12 (2000).

[213] Hatcher et al., *supra* note 177, at 399 (citing NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989)).

[214] Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 934 (1996) (noting the difficulty of developing good definitions of computer crime).

[215] A good example of "legal lag" exists in the field of trade secrets. "Prior to the passage of the EEA, the only federal statute directly prohibiting economic espionage was the Trade Secrets Act, 18 U.S.C. §1905, which forbids the unauthorized disclosure of confidential government information, including trade secrets, by a government employee." United States v. Hsu, 155 F.3d 189, 194 n.5 (3d Cir. 1998). The Trade Secrets Act had applicability to corporate espionage in a globally networked environment. The Act was enacted decades before the rise of the Internet. The National Stolen Property Act ("NSPA"), 18 U.S.C. § 2314 (2000), also had limited utility to corporate espionage. The NSPA was enacted "at a time when computers, biotechnology, and copy machines did not even exist." *Hsu*, 155 F.3d at 194.

[216] Neal, *supra* note 114.

[217] Stephen Nickson & Jim Kates, *The Reality of Hackers, Statistical Data* Included, 48 RISK MGMT. 50 (2001). *See* Clinton Wilder with Stephanie Stahl & Mary E. Thyfault, *A Premium on Safety––Is Computer Crime Insurance a Corporate Lifesaver or an Expensive Redundancy?*, INFO.WEEK, Nov. 29, 1993, *at* 24 (arguing that much of computer crime is preventable.)

Cybercrime cases frequently involve difficult issues of "criminal intent" not currently found in criminal law. As such, sentencing guidelines may need to be adjusted for discretionary conditions based upon the nature of cybercrime.[218] Policymakers should carefully consider the difference between a crime committed by an employee or other insider, and a crime committed by terrorists located in an offshore haven. An organized band of cybercriminals stealing credit cards should not receive the same treatment as a bored sixteen-year-old committing a prank. Should a hacktivist protesting expanded intellectual property rights be treated differently than an ex-employee who destroys computer files in retaliation for being terminated? Should political acts of hacking be treated differently than workplace theft of trade secrets, the crown jewels of an information-age company? Corporate espionage resulting in the loss of trade secrets causes greater economic loss than the damage caused by pranksters who deface websites. Present sentencing guidelines do not consider whether a website is hacked for financial gain, malicious mischief, or as a form of political expression. Cybercrime sentencing guidelines should consider the motives of hackers. The remainder of this Section provides a brief audit of the key federal computer crime statutes governing cybercrime. These statutes lag behind rapidly evolving cybercrime.[219]

1. *The Electronic Communications Privacy Act*

The Electronic Communications Privacy Act ("ECPA")[220] was enacted as an amendment to the Omnibus Crime Patrol and Safe Streets Act Title III of 1968.[221] The ECPA provides criminal and civil remedies for the unauthorized interception or disclosure of electronic communications. An "electronic communication" is defined as any "transfer of signs, signals, wiring, 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 . . . "[222] The ECPA "aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications."[223] Web sites are classified as

---

[218] The United States Sentencing Guidelines presently consider the circumstances of the offense as well as the history and characteristics of the defendant. *See* 18 U.S.C. § 3553 (2000). Sentencing Guidelines must take the motivation of the hacker or other cybercriminal into effect in order to determine a sentence likely to promote optimal deterrence. *See, e.g.*, Christopher M.E. Painter, U.S. Dep't of Justice, *Supervised Release and Probation Restrictions in Hacker Cases*, *at* http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm (Mar. 2001) (arguing that sentencing for computer crimes must consider the nature of cybercrime).

[219] The Privacy Protection Act ("PPA"), 42 U.S.C. §§ 2000aa–aa12 (Supp. V 2000), is sometimes invoked in computer hacking cases. *See* Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997). *See also* 18 U.S.C. § 1362 (2000) (dealing with communication lines, stations or systems).

[220] 18 U.S.C. §§ 2510–2711 (2000).

[221] Davis v. Gracey, 111 F.3d 1472, 1483 n.10 (10th Cir. 1997).

[222] 18 U.S.C. § 2510(12).

[223] *In re* Doubleclick Inc. Privacy Litig., 2001 U.S. Dist. LEXIS 3498, *24 (S.D.N.Y. Mar. 29, 2001).

"users" of Internet access and are governed by the ECPA.[224] Similarly, e-mail systems are electronic communications covered by the ECPA.[225]

Section 2701 of the ECPA prohibits the unauthorized access or alteration of records, stored wire communications, or electronic communications by persons without the authority to access the computer.[226] Section 2702 prohibits the unauthorized disclosure to any person or entity of the contents of an electronic communication obtained in violation of Section 2701.[227] Section 2702 also states: "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[228] The ECPA also provides for private enforcement against violators of the Act by "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of [the Act] in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind."[229] If the disclosing party, however, is not a provider of electronic communication service as defined in Section 2510,[230] the disclosure is outside of the scope of the ECPA. Furthermore, if a party consents to an interception, then there is no liability under the ECPA.[231]

The ECPA is a federal statute that applies to Internet-related crimes occurring within the territory of the United States. It provides civil and criminal remedies against hackers who intercept wire communications, whether from company voice mail or e-mail.[232] The contents of any wire, oral, or electronic communication includes any information concerning the substance, purport, or meaning of that communication, but does not include information concerning the identity of the author of the communication.[233] Law enforcement officers invoke the ECPA in cases involving the search

---

[224] *Id.* at *34.

[225] 18 U.S.C. § 2701(a) (making it an offense to obtain, alter, or prevent authorized access to a wire or electronic communication).

[226] *Id. See, e.g.*, State Wide Photocopy, Corp. v. Tokai Fin. Servs., 909 F. Supp. 137, 144–45 (S.D.N.Y. 1995) (construing 18 U.S.C. § 2701 such that the ECPA did not apply to a fraudulent scheme where the defendant released plaintiff's confidential proprietary information to competitors using fax machines). *See also* Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 820–21 (E.D. Mich. 2000) (holding that unauthorized access by a former contractor to plaintiff's trade secretes and transmittal of those trade secrets to competitors did not violate the ECPA).

[227] 18 U.S.C. § 2702.

[228] *Id.* § 2702(a)(1).

[229] *Id.* § 2707(a).

[230] An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

[231] *Id.* § 2511(2)(d).

[232] *See* United States v. Smith, 155 F.3d 1051, 1059 (9th Cir. 1998) (noting that a hypothetical hacker could be sued for civil damages and criminally prosecuted under the ECPA). *See also* United States v. Sills, 2000 U.S. Dist. LEXIS 5570 (S.D.N.Y. 2000) (indicting defendant, a police officer, under the ECPA for intercepting his employer's alphanumeric pager communications, which were not readily accessible to the general public, and for possession of a device useful for such interception.); State Wide Photocopy, Corp. v. Tokai Fin. Servs., 909 F. Supp. 137, (S.D.N.Y. 1995).

[233] *But see* Jessup-Morgan v. AOL, Inc., 20 F. Supp. 2d 1105 (E.D. Mich. 1998) (dismissing ECPA action against service provider, holding that disclosure of the identity of subscriber who posted messages on AOL system did not violate the ECPA because the identity was disclosed pursuant to a properly executed subpoena).

and seizure of computer systems or computer messages.[234] Employers and corporate entities frequently use the ECPA as a civil cause of action for the illegal seizures of computer systems or the interception of computer communications.[235] A federal court recently considered the question of whether the use of Internet "cookies," which collect potentially personally identifiable profiles to build demographic profiles of website visitors, violated the ECPA.[236] Despite its original purpose, the ECPA is seldom used to prosecute computer hackers for their unauthorized accessing of stored electronic communications.[237]

A company may disclose information stored on its computer system when the Government seeks to obtain information from electronic communications, remote computing services, or Internet service providers ("ISPs"). To compel disclosure under the ECPA, the government must demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation."[238] While, the ECPA applies to unauthorized access to electronic communications, it does not apply to the misuse of data when access is authorized.[239]

2. *Computer Fraud & Abuse Act*

The Computer Fraud and Abuse Act ("CFAA") is the single most important federal statute governing computer crime. The CFAA punishes and deters hacking, creating viruses, and other forms of computer crime, and extends to all computers involved in interstate commerce.[240] The CFAA was enacted in 1984 and has been amended several times.[241] Its jurisdiction includes the Internet. The CFAA prohibits any person from knowingly

---

[234] *See, e.g.*, Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001) (alleging unlawful tapping by the police department of a police officer's pager without a warrant or notice).

[235] *See* Guest v. Leis, 255 F.3d 325 (6th Cir. 2001) (denying claim by operators of computer bulletin boards against law enforcement officers for seizing their computer systems because the systems were seized pursuant to valid warrants). *See also* Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997) (holding that police officers conducting search and seizure with valid warrants did not violate the ECPA).

[236] *In re* Doubleclick Inc. Privacy Litig., 2001 U.S. Dist. LEXIS 3498 (S.D.N.Y. Mar. 29, 2001) (granting defendants' motion to dismiss ECPA claim that use of cookies collecting personally identifiable information violated the Act).

[237] LEXIS' "State and Federal Case Law" database contains eighty cases in which the search terms, "Electronic Communications Privacy Act and computer" are mentioned. Only five of the eighty cases involved any form of computer hacking. Private litigants file many of the ECPA cases for civil damages involving improper access of computer systems, websites, or networks. *See, e.g.*, Konop v. Haw. Airlines, Inc., 236 F.3d 1035 (9th Cir. 2000). *See also* Coronado v. Bank Atlantic Bancorp, Inc., 222 F.3d 1315 (11th Cir. 2000) (dismissing action against defendant bank for unauthorized disclosure of customer's account records); Lopez v. First Union Nat'l Bank, 129 F.3d 1186 (11th Cir. 1997).

[238] 18 U.S.C. § 2703(d) (2000).

[239] In *Education Testing Service v. Stanley H. Kaplan Educational Center*, employees of the test preparation service took the Graduate Record Examination in order to memorize, copy, and obtain questions for their business of preparing students to take the examination. 965 F. Supp. 731, 740 (D. Md. 1997). The court rejected the testing service claim that an unauthorized use of the examination constituted a violation of the ECPA. *Id.* The court stated that, "the Stored Communications Act applies . . . [where a] trespasser gains access to information to which he is not entitled to see, not . . . [where] the trespasser uses the information in an unauthorized way." *Id.*

[240] 18 U.S.C. § 1030 (2000).

[241] *Id.*

causing the transmission of information that intentionally damages a protected computer.[242] It is a violation of the CFAA for persons to obtain unauthorized access to the computer networks of government agencies and financial institutions, as well as computers used in interstate or foreign commerce.[243] It is also a violation of the CFAA for persons to intentionally infect a computer system with a virus, thereby damaging the computer system.[244]

The CFAA punishes those who "knowingly access[es] a computer without authorization or exceed[s] authorized access, and by means of such contact . . . obtain[s] information."[245] It is also a crime to intentionally access protected computers without authorization and recklessly cause damage.[246] The CFAA criminalizes trafficking in passwords or other information used to break into computer networks.[247] It is also a crime to threaten to cause damage to a protected computer,[248] the value of the use of which must be at least $5,000 in a one-year period.[249] The CFAA provides for civil liability for the intentional introduction of viruses or malicious codes into a computer system.[250] It also punishes conduct committed "in furtherance of any . . . tortious act in violation of the . . . laws of the United States or of any State."[251]

The use of a computer to "extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value," is also a violation of the CFAA.[252] The CFAA punishes criminal attempts, as well as acts that actually cause damage to a computer.[253] The CFAA punishes the knowing access of computer systems with graduated fines or imprisonment. Threats against national defense or foreign relations are punishable by a "fine . . . or imprisonment for not more than ten years, or both."[254] Moreover, repeat offenders endangering national defense or foreign relations may receive a fine or imprisonment "for not more than twenty years or both . . . after a conviction for another offense."[255]

The CFAA has been expanded to encompass evolving technologies. The National Information Infrastructure Protection Act of 1996 was

---

[242] *Id.*

[243] *Id.* § 1030(a)(2). The CFAA criminalizes access to a computer without authorization or exceeding authorized access and the obtainment of the records of a financial institution or an issuer of a credit or debit card. § 1030(a)(2)(A).

[244] *Id.* § 1030(a)(5)(A). The CFFA makes it a crime to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer." *Id.*

[245] *Id.* § 1030(a)(1).

[246] *Id.* § 1030(a)(5)(B).

[247] *Id.* § 1030(a)(6).

[248] *Id.* § 1030(a)(7).

[249] *Id.*

[250] *Id.* § 1030(g) (stating that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator . . .").

[251] *Id.* § 1030(c)(2)(B)(ii).

[252] *Id.* § 1030(a)(7).

[253] *Id.* § 1030(b).

[254] *Id.* § 1030(c)(1)(A).

[255] *Id.* § 1030(c)(1)(B).

enacted to extend federal computer crime statutes to include the Internet.[256] These amendments to the CFAA extended the scope of the statute from "federal interest computers" to "protected computers."[257] They specifically address the subject of computer hacking, making it a federal crime to intentionally cause damage to a protected computer or to "cause damage recklessly, negligently or otherwise if the protected computer was intentionally accessed without authorization."[258] The 1996 amendments punish company insiders for intentional damage and hackers for intrusions "even if the transmission was only reckless or negligent."[259] They also permit the prosecution of outside hackers and trusted insiders who exceed the scope of their duties, as well as those who spread viruses.[260] Only a handful of defendants, however, have been prosecuted nationwide under the CFAA for spreading computer viruses.

3. *Economic Espionage Act*

The Economic Espionage Act ("EEA") provides criminal sanctions and civil damages for the misappropriation of trade secrets. The EEA was enacted against "a backdrop of increasing threats to corporate security and a rising tide of international and domestic economic espionage."[261] The act criminalizes "economic espionage"[262]and the "theft of trade secrets"[263] by making such actions by ex-employees, business competitors, and foreign powers federal crimes. The EEA punishes those who misappropriate trade secrets with the intent to benefit foreign governments, foreign instrumentalities, or agents.[264] An individual whose misappropriation of trade secrets benefits a foreign government, instrumentality, or agent may be sentenced to serve time in a federal prison for up to fifteen years and may be fined up to $500,000.[265] A business competitor or other entity that steals a trade secret benefiting a foreign government can be fined up to $10,000,000.[266] The EEA permits parallel civil actions to restrain the misappropriation of trade secrets, including "appropriate injunctive relief against any violation" of the statute.[267]

The EEA applies to any individual who transmits, receives or possesses stolen trade secrets.[268] It is questionable whether the EEA applies to nonutilitarian hackers who deface websites as a form of protest. A defendant must have the *mens rea* needed to commit a calculative crime of

---

[256] 32 Pub. L. No. 104-294, Title II, § 201, 110 Stat. 3488, 3491–94 (1996) (codified as amended at 18 U.S.C. § 1030 (2000)).
[257] 18 U.S.C. § 1030(e)(2).
[258] Hatcher et. al., *supra* note 177, at 405.
[259] *Id.*
[260] *Id.*
[261] United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998).
[262] 18 U.S.C. § 1831 (2000).
[263] *Id.* § 1832. Misappropriating trade secrets for the benefit of "anyone other than the owner" is punishable by criminal and civil penalties. *Id.*
[264] *Id.* § 1831.
[265] *Id.* § 1831(a)(5).
[266] *Id.* § 1831(b).
[267] *Id.* § 1836(a).
[268] *Id.* §§ 1832(a)(2)–(a)(3).

data theft.[269] Section 1832 requires that a defendant convert a trade secret "to the economic benefit of anyone other than the owner thereof."[270] In addition, Section 1831 requires defendants to have intent or knowledge that their offense will benefit a foreign government, instrumentality or agent.[271] Thus, a foreign hacker who defaces a corporate website or places a political slogan on a government website would not be liable under Section 1832.

The EEA also applies to anyone who make copies or "duplicates, . . . downloads, uploads, alters, destroys, . . . replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret."[272] In addition to criminal sanctions, the EEA provides tort-like remedies for the electronic misappropriation of trade secrets. There have been relatively few criminal prosecutions under the EEA, presumably because of the difficulty of detecting computer intrusions involving trade secrets.[273] Private enforcement of the EEA has played a role in most trade secret cases. The corporate victim in such a case conducts an internal investigation, turning evidence of wrongdoing over to the authorities. There are few reported cases in which public authorities took the lead in uncovering a misappropriation of a trade secret from a computer system.[274]

4. *The Federal Wiretap Statute*

The Federal Wiretap Statutes,[275] like the ECPA, are part of The Omnibus Crime Patrol and Safe Streets Act of 1968.[276] The federal wiretapping statutes cover "wire," "oral" and "electronic" communications. These statutes distinguish between the "interception of an electronic communication at the time of transmission and the retrieval of such a communication after it has been put into "electronic storage."[277] During the transmission phase, any protection against unlawful interception is governed by Section 2511.[278] Once messages have been stored, they are governed by Section 2701.[279] The Fifth Circuit held in *Steve Jackson*

---

[269] *Id.* § 1831.
[270] *Id.* § 1832(a).
[271] *Id.* § 1831.
[272] *Id.* § 1831(a)(2).
[273] A LEXIS search on August 19, 2001, yielded only twelve cases containing the phrase "Economic Espionage Act." Three of the cases concerned a conspiracy to steal processes, methods, and formulas for an anticancer drug produced by a major pharmaceutical company. *See* Hsu v. United States, 40 F. Supp. 2d 623 (E.D. Pa. 1999). *See also* United States v. Hsu, 155 F.3d 189, 189 (3d Cir. 1998); United States v. Hsu, 982 F. Supp. 1022 (E.D. Pa. 1997).
[274] *See, e.g.*, United States v. Martin, 228 F.3d 1 (1st Cir. 2000) (involving a defendant who inadvertently sent an e-mail attachment containing stolen trade secrets to a company manager). *See also* United States v. Yang, 74 F. Supp. 2d 724 (N.D. Ohio 1999) (involving a defendant who was caught through joint collaboration of the FBI and the corporate victim); *Cf. Hsu*, 40 F. Supp. 2d at 623; *Hsu*, 155 F.3d at 189; *Hsu*, 982 F. Supp. at 1022 (resulting from an investigation spearheaded by an undercover FBI agent whom the defendant mistakenly believed to be a technological information broker).
[275] 18 U.S.C. §§ 2510–20 (2000).
[276] *Id.*
[277] "Interceptions" are covered by 18 U.S.C. §§ 2510–22, and access to information in electronic storage is covered by 18 U.S.C. §§ 2701–11. *See* Bohach v. Reno, 932 F. Supp. 1232, 1235 (D. Nev. 1996).
[278] *Id.* at 1236.
[279] *Id.*

Games, Inc. v. United States Secret Service that the electronic storage of an electronic communication is, by definition, not a part of the communication itself.[280]

Section 2511(1)(a) forbids the interception of electronic communications. An interception is the acquisition of the contents of any electronic communication through the use of any electronic, mechanical or other device.[281] An electronic communication cannot be intercepted when it is in electronic storage because only in-transit communications can be intercepted.[282]

One of the difficulties facing prosecutors is a lack of information technologies necessary to investigate cybercriminals. When they have adequate technical expertise to track a wily hacker, they may be impeded by the warrant requirements and other procedural limitations on the use of technology to catch cyberthieves. The wiretap statutes require law enforcement officers to obtain court orders before intercepting telephone conversations.[283] They also limit government eavesdropping into voice communications, even those connected to the topic under investigation. The government, however, may obtain a warrant by demonstrating that wiretaps are necessary because other normal investigating procedures have been tried and either have failed or are too dangerous.[284]

5. *International Cybercrime Statutes*

During its May 2001 meeting, the Council of Ministers of Europe agreed on the need for a European Union instrument to regulate cybercrime. The Council outlined plans for a European Forum on cybercrime to be launched in the near future.[285] Similarly, the Council of Europe[286] has proposed a draft Convention on Cybercrime to deal with the transborder character of Internet-related offenses.[287] Similar to the CFAA, the draft Cybercrime Convention criminalizes the intentional destruction of data, but specifies no monetary threshold.[288] The Convention also

---

[280] 36 F.3d 457, 461, 462 (5th Cir. 1994).

[281] 18 U.S.C. § 2510(4).

[282] *Id.*

[283] *See, e.g.*, United States v. Reyna, 217 F.3d 1108, 1112 (9th Cir. 2001) (granting defendants' motion to suppress evidence of intercepted telephone conversations on the ground that the government had not obtained proper wiretap authorization order). *Cf.* United States v. Nerber, 222 F.3d 597, 605 (9th Cir. 2000) (ordering suppression of evidence from video surveillance because it was warrantless and the government had not obtained the consent of the participants to be monitored).

[284] United States v. Arrington, 2000 U.S. App. LEXIS 5762 (10th Cir. Mar. 29, 2000) (ordering suppression of wiretap evidence because the government failed to show necessity, including the showing that other investigative methods were tried and either failed or were too dangerous to proceed).

[285] Press Release, 2337th Council Meeting—Justice, Home Affairs and Civil Protection—Brussels, 15 and 16 March 2001, (March 17, 2001), *available at* LEXIS, News Group File.

[286] The Council of Europe consists of forty-one member states, including the entire membership of the European Union. The Council was established in 1949 "to uphold and strengthen human rights, and to promote democracy and the rule of law in Europe." U.S. Dep't of Justice, *supra* note 5.

[287] *Draft Explanatory Memorandum to the Draft Convention on Cybercrime*, European Committee on Crime Problems, *at* http://www.conventions.coe.int/treaty/en/projects/cybercrime.htm (Feb. 14, 2001) [hereinafter *Draft Explanatory*].

[288] U.S. Dep't of Justice, *supra* note 5 (explaining the differences between U.S. federal criminal statutes and the proposed Cybercrime Convention).

criminalizes the possession and trafficking of unauthorized access and interception devices. Before Congress, the European Commission, or any other transnational entity enacts new measures to control cybercrime,[289] further empirical study about the nature of cybercrime is needed. Internet law reform must utilize systematic study, rather than anecdotal data. Criminal laws establishing cybercrime offenses must be drafted to account for the different social harms of these offenses against computer networks.

Cybercrime, by its nature, is often international, and requires new forms of creative multilateral law. Increasingly "criminals around the world [use] computers to commit traditional crimes, including fraud, copyright infringement, distribution of child pornography, and other crimes."[290] The *I Love You* virus is a paradigmatic example of the international nature of Internet crime. The arm of criminal law cannot easily reach a hacker living on another continent or operating in an offshore haven.[291] At the present, there is no uniform treaty addressing cybercriminal law or the procedural aspects of policing Internet-related crimes. Stein Schjolberg, a Norwegian judge and an expert on computer law, stated at a Group of Eight countries meeting: "Computer attacks, unlike murder or robbery, [are] still not universally recognized as a crime."[292] The Council of Europe's Convention on Cybercrime is the first international instrument dealing with cybercrime.[293] The goal of the Convention is to adopt "a common criminal policy aimed at the protection of society against cyber-crime . . . by adopting appropriate legislation and fostering international co-operation."[294] The Cybercrime Convention provides uniform guidelines for the legal definition of computer crimes and formulates international standards for transborder search and seizure.[295]

The Convention proposes uniform substantive criminal law to govern the "confidentiality, integrity and availability of computer systems or data."[296] The Convention makes the illegal interception of wireless communications a crime.[297] Computer viruses and the deliberate

---

[289] There is little agreement on the definition of cybercrime.

> Law enforcement experts and legal commentators are divided. Some experts believe that computer crime is nothing more than ordinary crime committed by high-tech computers and that current criminal laws on the books should be applied. . . . Others view cybercrime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies.

Sinrod & Reilly, *supra* note 78, at 180.

[290] U.S. Dept. of Justice, *supra* note 5.

[291] The Hague Convention on Jurisdiction and Foreign Judgments will make it easier to obtain jurisdiction and enforce judgments in the global marketplace. Negotiations on the draft Hague Convention have been ongoing since 1994. The Hague Convention would apply to criminal offenses on the Internet as well as to civil and commercial causes of action. *See E-Commerce Dominates Talks on More Legal Co-Operation*, EUROPEAN REP., Feb. 28, 2001, at 2572, LEXIS, News Group File.

[292] *G8 Leaders Meet to Fight Cybercrime*, GLEANER, May 16, 2000, LEXIS, News Group File.

[293] Press Release, EU—Canada Summit—Ottawa—19 December 2000 (Dec. 20, 2000), *available at* LEXIS, News Group File.

[294] *Draft Convention on Cyber-Crime*, European Committee on Crime Problems, Committee of Experts on Crime in Cyberspace, *at* http://conventions.coe.int/treaty/en/projets/cybercrime.htm (April 25, 2000) (citing from Preamble) [hereinafter *Draft Convention*].

[295] *Draft Explanatory*, *supra* note 287.

[296] *Draft Convention*, *supra* note 294 (citing ch. II, sec. 1, tit. 1).

[297] *Id*. at art. 3.

destruction of data are crimes of "Data Interference"[298] and "System Interference."[299] The sale and distribution of anti-circumvention devices and other hacker tools are also proscribed by the Convention.[300]

Title One of the Cybercrime Convention proposes that each country make offenses against the confidentiality, integrity, and availability of computer data and systems crimes.[301] It notes that international cooperation is required to detect and punish computer hacking, data theft, and interference with computer systems.[302] Title Two establishes a number of computer-related offenses for computer-related forgery[303] and computer-related fraud.[304] Titles Three and Four cover content-related offenses related to copyright offenses,[305] as well as representations of children engaged in sexual conduct or virtual child pornography.[306] Title Five covers aiding and abetting,[307] liability in international corporate espionage,[308] and proportionate sanctions for computer crimes.[309] A corporate employee, for example, would face criminal, civil, or administrative liability for intruding into a competitor's computer network.[310]

Title Two provides the rules of international criminal procedure for computer crimes. The draft convention requires each signatory to develop rules for the search and seizure of stored computer data.[311] The rules for discovery are covered in production orders,[312] the preservation of electronic or computer evidence,[313] expedited disclosure of traffic and other related data by Internet providers,[314] and the interception of data.[315] The Convention calls for legislative and other measures to establish jurisdiction over computer and Internet-related crimes.[316]

The proposed Cybercrime Convention provides for international cooperation for computer crime investigations[317] and treats computer crime as an extraditable offense.[318] It also addresses mutual assistance in the investigation and prosecution of computer crimes based upon electronic evidence.[319] Article Twenty-three develops a mechanism for responding to

---

[298] *Id.* at art. 4.
[299] *Id.* at art. 5.
[300] *Id.* at art. 6.
[301] *Id.* at ch. II, sec. 1, tit. 1.
[302] *See id.*
[303] *Id.* at art. 7.
[304] *Id.* at art. 8.
[305] *Id.* at art. 10.
[306] *Id.* at art. 9.
[307] *Id.* at art. 11.
[308] *Id.* at art. 12.
[309] *Id.* at art. 13.
[310] *Id.* at art. 12.
[311] *Id.* at art. 14.
[312] *Id.* at art. 15.
[313] *Id.* at art. 16.
[314] *Id.* at art. 17.
[315] *Id.* at art. 18.
[316] *Id.* at art. 19.
[317] *Id.* at art. 20.
[318] *Id.* at art. 21.
[319] *See, e.g.*, *id.* at art. 22.

mutual assistance requests for borderless computer crimes.[320] Articles Twenty-four through Twenty-nine of the proposed Cybercrime Convention require signatory states to adopt legislative measures to implement mutual assistance.[321] Article Twenty-four, for example, provides mechanisms for obtaining an "expeditious preservation of data" on a computer system or server in another territory.[322] Parties must promptly disclose traffic data and may refuse a request only if compliance would threaten sovereign immunity, security, the public order, or other essential interests.[323]

The Cybercrime Convention is likely to result in the greater international cooperation necessary to enforce and prosecute crimes on the borderless electronic frontier. Fighting cybercrimes, such as hacking, requires the cooperation that is already instituted for intellectual property offenses, money laundering, child pornography, and illegal drug trafficking.

Critics of the Cybercrime Convention complain that it lacks balance and gives too much power to the law enforcement community at the expense of civil liberties.[324] Balancing privacy and enforcement is made even more difficult because the signatory countries have radically different fundamental rights and freedoms.[325] Few question the need for some kind of convention, but this Convention is opposed by a wide variety of industry stakeholders and ISPs who seek a minimal global enforcement regime.[326] The United States Chamber of Commerce, a prominent business lobby, favors a market-based international enforcement regime.[327] At present, there is no effective global cybercrime enforcement and greater international cooperation is urgently needed.

D. WHY SO FEW CYBERCRIME PROSECUTIONS?

1. *Cyberlaw Enforcement Lag*

By the time a statute is enacted to counter an Internet-related threat, the creative cybercriminal finds new technologies to bypass an essential element of the prohibited act or offense. The difficulty of prosecuting cybercrimes is illustrated by *United States v. LaMacchia*.[328] David LaMacchia, an MIT student, was prosecuted for distributing software using the Internet.[329] He hosted a computer bulletin board where anyone could

---

[320] *Id.* at art. 23.
[321] *Id.* at arts. 24–29.
[322] *Id.* at art. 24.
[323] *Id.* at art. 25.
[324] *Freedom v Rules Bring Cybercrime Treaty Clashes*, REUTERS, Mar. 6, 2001, *at* http://www.cyber-rights.org/cybercrime (Mar. 6, 2001).
[325] *See* Cyber-Rights & Cyber-Liberties (UK), *Information Related to Cybercrime Policy Making Process Within the Council of Europe, European Union, G8, and the United Nations*, *at* http://www.cyber-rights.org/cybercrime (last visited Aug. 14, 2001).
[326] *See id.*
[327] *See U.S. Chamber Opposes European Cyber Crime Treaty*, *at* http://www.cyber-rights.org/cybercrime (Dec. 2000).
[328] 871 F. Supp. 535 (D. Mass. 1994).
[329] *Id.* at 536.

copy copyrighted computer software for free.[330] The criminal action against David LaMacchia was ultimately dismissed because the criminal wire fraud penalties could not be imposed. The court found no proof that LaMacchia had received financial gain from the acts of illegal copying.[331] Not until the end of 1997 was the *LaMacchia* loophole eliminated by the No Electronic Theft Act of 1997 ("NET").[332] NET broadens criminal liability for copyright infringement to cases in which no financial gain is involved.[333] There is little case law interpreting NET, suggesting that Congress may have patched a statutory loophole that no longer exists.[334]

Although Internet-related hacking represents a serious societal threat, criminal law lags behind the rapidly evolving Internet. Sentencing guidelines, for example, must take into account whether a hacker is motivated by financial gain (innovation) or by curiosity (retreatism).[335] Federal enforcement of Internet-related crimes is also hampered by constraints not found in the cybercrime community. Cybercriminals have long used packet-sniffing software to intercept e-mail. Corporate spies routinely use diagnostic tools to intercept their competitors' messages. These technologies, however, are not always available to the law enforcement community.

Law enforcement agencies are restricted by constitutional constraints that do not encumber foreign terrorists. Civil liberties groups, for example, have criticized the FBI for its proposed use of *Carnivore*, an e-mail sniffing software, to pursue hackers and other criminals in cyberspace.[336] The FBI describes *Carnivore* as a diagnostic device "with a surgical ability . . . ignoring those communications which they are not authorized to intercept."[337] It claims that *Carnivore* operates like other packet sniffers and network information security tools used by private companies.[338]

The FBI's use of *Carnivore* has been criticized by The Electronic Privacy Information Center ("EPIC") and other privacy advocates,[339] even after it was revealed that the FBI can "reliably capture and archive all unfiltered traffic."[340] EPIC has not expressed the same degree of concern about corporate systems administrators, and organized criminals, who

---

[330] *Id.*

[331] *Id.* at 540, 545.

[332] Pub. L. 105-147, § 2(b), 111 Stat. 2678 (1997) (codified as amended at 17 U.S.C. § 506(a) (2000)).

[333] *See id.*

[334] A LEXIS search of all state and federal case law on August 20, 2001 revealed only one case mentioning the NET. *See* Eldred v. Reno, 74 F. Supp. 2d 1 (D.C. 1999).

[335] *See Hill Leaders Eye Government Involvement with Internet*, COMM. DAILY, Mar. 29, 2000, LEXIS, News Group File.

[336] *See Carnivore Devours Trust*, ST. PETERSBURG TIMES, Jan. 3, 2001, at 12A.

[337] FBI, *Carnivore: Diagnostic Tool*, *at* http://www.fbi.gov/programs/carvnivore/carnivore2.htm (last visited Jan. 21, 2001) [hereinafter *Carnivore: Diagnostic Tool*]. Carnivore has been described as a narrowly tailored tool that "digests only data relevant to an investigation." Declan McCullagh, *FBI Gives a Little on Carnivore*, Wired News, *at* http://www.wired.com/news/politics/0,1283,37765,00.html (July 25, 2000).

[338] FBI, *supra* note 337.

[339] *See* Jennifer DiSabtino, *Final Version of Carnivore Study Released*, NETWORK WORLD, Dec. 18, 2000, LEXIS, News Group File.

[340] *Carnivore Devours Trust*, *supra* note 336.

already use *Carnivore*-like packet sniffers to commit crimes. Foreign terrorists in offshore havens might already have advanced software tools to protect themselves from *Carnivore*. The Taliban, for example, may have used encryption in secure websites to plan the September 11, 2001 attacks on the Pentagon and the World Trade Center. The FBI is conducting a widespread investigation on how Osama Bin Laden and his followers used "the Internet through numerous temporary accounts and postings to send encrypted messages and photographs on commonly used Web sites."[341] Foreign terrorist groups such as Hezboallah, HAMAS, and Bin Laden's al Qaeda organization use the Internet as a target and a tool "to formulate plans, raise funds, spread propaganda, and to communicate securely."[342]

2. *Borderless Cybercrime Scenes*

Internet crimes are seldom detected or prosecuted largely because there is no traditional crime scene. In contrast to a traditional crime scene, online forgers or intruders leave few digital footprints. DNA evidence, fingerprints, or other information routinely tracked in law enforcement databases are useless for investigating cybercrimes. In addition, computer records are easier to alter than paper and pencil records. Electronic robbers and forgers leave fewer clues than white-collar criminals who alter checks or intercept promissory notes. For example, a skilled forger who adds zeroes to a check leaves more clues than a digital thief. The use of false e-mail headers, offshore sites, and anonymous e-mailers also make catching cybercriminals more difficult.

Because cybercrime is borderless by its nature, it creates new methods of concealing wrongdoing.[343] An international cybercriminal group calling themselves the "Phonemasters" was able to penetrate the "computer systems of MCI, SPRINT, AT&T, Equifax and even the National Crime Information Center."[344] Another network of cybercriminals stole $10 million in funds from "bank accounts in California, Finland, Germany, the Netherlands, Switzerland and Israel."[345]

3. *Low Priority and Lack of Fiscal Resources for Computer Crime Prosecution*

Law enforcement agencies are far more prepared to address crime in the streets, than to address computer crime. Most states have computer crime statutes, but do not have significant law enforcement presence in

---

[341] Jerry Seper, *Terrorists May Have Used Internet to Plot*, WASH. TIMES, Oct. 6, 2001, at A3. *See* Jim Puzzanghera, *FBI Tries to Find Clues on Internet, Computer E-Mail Terrorists Used Computers Inside Public Libraries in Florida to Cover Their Tracks*, ARKANSAS-DEMOCRAT GAZETTE, Sept. 21, 2001, at A4 (discussing terrorists' use of the Internet to plan attack).

[342] *Id.*

[343] *Cybercrime Before the S. Judiciary Comm., Criminal Justice Oversight Subcomm. and House Judiciary Comm., Crime Subcomm.*, 106th Congress (2000) (statement of Michael A. Vatis, Dir., Nat'l Infrastructure Prot. Ctr., FBI), *available at* http://www.usdoj.gov/criminal/cybercrime/vatis.htm.

[344] *Id.*

[345] *Id.*

cyberspace.[346] Although the number of cybercrimes is increasing, appropriating enforcement funds to fight these crimes is not a priority at the local level. In other words, crime on the streets receives greater attention than crime in the suites.

Many online fraud cases go undetected and unprosecuted because these crimes are difficult to trace. For Internet crimes such as releasing computer viruses, the probability of prosecution is even lower. In order for criminal law to function, law enforcement units will require officers who understand encryption, digital signatures, and computer viruses, and know how to track computer criminals on the Internet. Local law enforcement lacks the resources to recruit, train, and retain law enforcement officers with good computer skills.[347] Low salaries and a high turnover of experts in cybercrime curtail the effectiveness of law enforcement at both the state and federal level. Even if a local law enforcement agency had the resources to pay its employees salaries comparable to those in the private sector, an enforcement gap would continue to exist as law enforcement often lacks the software necessary to track cybercriminals operating in the global computer network.

Relatively few countries have specialized cybercrime units, making the Internet an almost ideal venue for transnational criminal activities. These few countries include the United Kingdom and the United States. The United Kingdom recently launched a National Hi-Tech Crime Unit that will work with police forces to investigate organized crime on the Internet.[348] The FBI and the United States Department of Justice each have newly fortified computer crime units. Each of the ninety-three U.S. Attorney Offices has at least one high-tech expert.

4. *Other Barriers to Cybercrime Prosecutions*

There is little question about the pervasiveness of criminal activity on the Internet. Criminal laws inadequately address this problem. "'In most cases, our laws do work' on [the] Internet, Commerce Sec[retary William M.] Daley said, but in some cases authorities 'need more resources.'"[349] In the past year, there have been a large number of computer viruses, but few

---

[346] "Florida and Arizona became the first states to pass specific laws against computer abuse." Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, *in* CRIME, DEVIANCE AND THE COMPUTER 101, 101 (Richard C. Hollinger ed., 1997). By 1988, forty-seven states enacted specific laws against computer crime. *Id.* The Massachusetts Attorney General's Office has a cybercrime unit with two attorneys working full time prosecuting computer crime offenses. Few other states, however, have any significant prosecutorial and law enforcement presence in cyberspace. Interview with Julie Ross, Assistant Attorney General, Member of Computer Crime Unit, Massachusetts Attorney General's Office (Dec. 8, 2000).

[347] Former FBI Director Louis Freeh acknowledged that it is difficult to retain cybercrime law enforcement officers when they can make "six figures in the private sector." William New, *FBI Struggles to Retain Cybercrime Experts*, *at* http://www.govexec.com/dailyfed/0401/040501td.htm (Aug. 5, 2001) (quoting FBI Director Louis Freeh).

[348] Kieren McCarthy, *Cybercops Are Go!*, The Register, *at* http://www.theregister.co.uk/content/6/18341.html (May 4, 2001); *New Hi-Tech Crime Investigators in £25 Million Boost to Combat Cybercrime*, Cyber-Rights & Cyber-Liberties (UK), *at* http://www.cyber-rights.org/cybercrime (Nov. 13, 2000).

[349] *Cybercrime Report Seen to Presage Loss of Internet Anonymity*, COMMS. DAILY, Mar. 10, 2000, LEXIS, News Group File.

successful prosecutions because of the expense of the investigative work. Even if a high-tech crime unit finds the evidence necessary to prosecute a cybercriminal, the trial is likely to be lengthy and expensive.

In a cybertheft of a trade secret case, for example, an information security expert might need to reconstruct e-mails or other electronic smoking guns. Because the burden of proof in such a criminal prosecution is "beyond a reasonable doubt," the standard is difficult to satisfy when the origin of an e-mail or Internet posting is uncertain. Juries may find it difficult to understand the difference between a source code and an object code or to comprehend anti-circumvention devices under the DMCA.[350] Finally, the rules of evidence in criminal law may bar proof of prior wrongdoing of a similar nature, which would strongly suggest a pattern and practice of cybercrime.

Few cyberstalking cases have been prosecuted because few states have statutes addressing the elements of this evolving crime. As a result, victims of Internet-related crimes and torts are more likely to find civil redress. Because many crimes and torts overlap,[351] one computer forensics expert suggested that for computer crimes, individuals must discover it, and get legal advice, then, if they are unable to stop it, "file a civil suit."[352]

II. THE PRIVATE POLICE IN CYBERSPACE

The Internet has become a haven for cybercriminals due to the possibilities for instant wealth without detection or prosecution. In this Part, I argue that a strong regime of private enforcement must supplement public law enforcement. Private enforcement in the form of "E-cops" is already becoming well established on the Internet, as many American Internet companies are skeptical about the role of government in detecting and punishing hackers. In 2000, private companies spent an estimated $300 billion in private enforcement efforts against hackers and viruses.[353]

E-Bay, the online auction house, for example, employs private investigators to patrol its website.[354] The website has 22.4 million members and six million items for sale at any one time, making it impossible for law

---

[350] The Digital Millennium Copyright Act of 1998 makes it a crime to circumvent copyright protection technologies. 17 U.S.C. § 1201 (2000). Juries will need to understand the concept of "circumvention" as well as typologies for encryption and decryption in anticircumvention cases.

[351] Assault, battery and fraud are also classified as torts. "A tort is not the same thing as a crime, although the two sometimes have many features in common." W. PAGE KEETON, PROSSER & KEETON ON THE LAW OF TORTS 7 (1984).

[352] Deborah Radcliff, *A Case of Cyberstalking: Law Enforcement Agencies Appear Powerless to Stop Electronic Harassment*, NETWORK WORLD, May 29, 2000, at 56 (quoting a computer forensics lab manager).

[353] Anthony Shadid, *FBI Officials Says Law Enforcement Technology Lags Behind Cybercrime*, BOSTON GLOBE, Mar. 21, 2001, LEXIS, News Group File.

[354] Joelle Tessler, *E-Cops Patrol Web Site: Former Federal Officers Take Lead Roles on Issues Ranging from Criminal Investigations to Setting Rules*, MERCURY NEWS, *at* http://www.siliconvalley.com/docs/news/depth/ebay040801.htm (Aug. 7, 2001).

enforcement to monitor all bad acts on the site.[355] Their private police uncovered the online sale of a human kidney.[356]

The Internet Fraud Watch is a watchdog group formed by the National Consumers League to enforce laws privately.[357] Federal agencies, such as the Department of Energy Commission, educate consumers about self-help measures for online fraud such as e-mail chain letters and pyramid schemes.[358] State attorneys general in a growing number of states have similar programs to help consumers uncover and report online fraud and other cybercrimes.[359]

Private enforcement by the Software Publishers Association ("SPA") is conducted by a well-funded worldwide e-police force that actively detects and prosecutes copyright infringement and software piracy.[360] The software industry employs private investigators to track companies and individuals who make unauthorized or counterfeit software copies.[361] Software private police participate in raids on companies to confiscate unlicensed copies of software. The U.S. Software and Information Industry Association claims that $7.5 billion worth of American software is illegally copied and distributed annually.[362]

The SPA's private enforcement campaign serves to thwart software pirates who are unlikely to be prosecuted for criminal copyright infringement.[363] The SPA mounted an educational campaign against illegal copies, including a rap video entitled "Don't Copy That Floppy," which has been used in schools and companies.[364] The SPA claims that its campaign of private policing and education has slowed the rate of piracy.[365]

An act of online banking fraud was detected and enjoined as a result of the investigative work of the International Chamber of Commerce's ("ICC") Commercial Crime Bureau.[366] The ICC routinely polices financial and intellectual property offenses on the Internet and has uncovered a number of fraudulent financial sites ranging in value from $50 million to

---

[355] *Id*.
[356] *Id*.
[357] *Id*.
[358] The Department of Energy, for example, has a web page devoted to "Hoaxbusters" to help consumers take self-help measures against fraudulent schemes, viruses, and other forms of Internet wrongdoing. *See Welcome to the New CIAC Hoax Pages*, Hoaxbusters, *at* http://hoaxbusters.ciac.org (last visited Aug. 14, 2001).
[359] The Massachusetts' attorney general takes a proactive approach to helping consumers report Internet-related wrongdoing. For example, the Computer Crime unit works with Massachusetts State Police specially trained investigators. Interview with Julie Ross, *supra* note 346.
[360] Dan Bricklin, *The Software Police vs. the CD Lawyers*, *at* http://www.bricklin.com/softwarepolice.htm (last visited Aug. 15, 2001).
[361] *See id.*
[362] *Crime on the Internet*, Jones Telecommunications & Multimedia Encyclopedia, *at* http://www.digitalcentury.com/update/crime.html (last visited Aug. 18, 2001).
[363] *See* Bricklin, *supra* note 360.
[364] *Sci-Fi Can Help Teach Students Ethical Implications of Technology Use*, EDUC. TECH. NEWS, July 5, 2000, LEXIS, News Group File.
[365] *Economy Instability Slows Down BSAS Anti-Piracy Blitz*, FIN. GAZETTE, Apr. 25, 2001, at 1.
[366] *Online Banking Scam Shut Down by ICC Commercial Crime Bureau*, Pike & Fischer Internet Law & Regulation, *at* http://internetlaw.pf.com/subscribers/pdf/ira042001.pdf (Aug. 13, 2001).

over $400 million.[367] Private investigators uncovered a complex financial scheme involving false bank guarantees and financial documents on twenty-nine websites potentially worth $3.9 billion.[368] The websites had the "look and feel" of Euroclear Bank, the international clearinghouse for the settlement of securities sales and Eurobonds.[369]

Another example of private enforcement involves the victimization of Bloomberg Financial News by hackers operating in former Russian Republics.[370] The hackers impersonated Bloomberg employees and collected personal information such as credit card numbers from the corporate website.[371] The perpetrators also sent an e-mail message to Michael Bloomberg requesting $20,000 for security services and threatening that if the "consulting fee" was not paid, it would expose the security weaknesses of Bloomberg's network to the press and the public.[372] Bloomberg's private police worked with the FBI to conduct a sting operation that resulted in the arrest and extradition of the perpetrators.[373]

Private enforcement of cybercrime is a rapidly evolving legal institution that is filling the public law enforcement gap in this area. The Computer Emergency Response Team ("CERT") at Carnegie Mellon University is the first line of defense against many forms of cybercrime such as computer intrusions and viruses.[374] CERT officials review materials provided by the victims of cybercrime to develop ways to address attacks. CERT also develops software designed to remedy software soft spots and other vulnerabilities.[375] In coordination with the Electronic Industries Alliance, CERT recently launched a new security alliance to provide reports on risk management, computer vulnerabilities, computer viruses, and data crimes.[376] CERT also issues advisories to assist network administrators in rapidly responding to computer crimes by auditing for anomalies or unauthorized devices.[377] Private enforcement has been more successful in detecting fraud than in uncovering the sources of computer viruses or DoS attacks.

---

[367] *Id*.
[368] *Id*.
[369] *Id*.
[370] John Leyden, *Extradition Hearing in Bloomberg Hack/Extortion*, The Register, *at* http://www.theregister.co.uk/content/8/18196.html (Sept. 4, 2001).
[371] *Id*.
[372] *Id*.
[373] *Id*.
[374] CERT is located at Carnegie Mellon University and on the web at http://www.cert.org.
[375] The Department of Justice frequently works with CERT to develop advisories on software vulnerabilities or reports of new forms of cybercrime. The victims of cybercrime are also encouraged to report computer crime to the National Infrastructure Protection Center ("NIPC") Watch of the Department of Justice. U.S. Dep't of Justice, *supra* note 94.
[376] *New Internet Security Alliance Is Born*, Newsbytes, *at* http//www.newsbytes.com/news/01/164661.html (last visited Aug. 19, 2001).
[377] "Anomaly" is a general term used by information security experts to refer to any suspicious or unusual activity or code in a computer system.

A. THE EVOLUTION OF THE PRIVATE ATTORNEY GENERAL

The concept of the "private attorney general" was first articulated by Second Circuit Judge Jerome Frank in *Associated Industries of New York v. Ickes*.[378] Judge Frank used the term to refer to "any person, official or not, [who] institute[s] a proceeding . . . even if the sole purpose is to vindicate the public interest.[379] Such persons, so authorized, are, so to speak, private Attorney Generals [*sic*]."[380] Private attorneys general have played a critically important role in developing modern tort law. Tort law assigns responsibility for injuries by requiring the wrongdoer to pay compensation. Tort law, however, does not require that defendants receive advance warning that some specific conduct is punishable by punitive damages. This greater flexibility gives tort law a considerable advantage over criminal law in controlling socially harmful conduct in cyberspace.

The private attorney general plays two roles: the first, to serve the client and second, to serve the public interest. Each state's professional responsibility code requires that all attorneys zealously represent their clients' interests. The unintended consequence of the contingency fee system is that trial attorneys serve the public interest when they uncover threatening conduct. When plaintiffs' attorneys serve the public interest they are called "private attorneys general."[381] In the field of toxic torts, the government relies on private litigants to enforce certain environmental statutes.[382] Similarly, private attorneys general uncover information about a wide variety of cybercrimes.

1. *Federal Statutes with Private Enforcement*

Since the 1940s, Congress has provided private citizens with a cause of action to enforce federal statutes such as the Clean Water Act, Sherman Anti-Trust Act, and Federal Trade Commission Act. Private attorneys general are private litigants who fulfill a public purpose while pursuing a private cause of action. Congress provided for a private attorney general role to police unfair competition in the 1946 Lanham Act, which gives commercial parties standing to sue defendants for unfair and deceptive trade practices in federal courts, and provides private litigants with tort-like consumer remedies to correct unfair practices.[383] Courts have long interpreted Section 43(a) as creating a federal statutory tort action

---

[378] 134 F.2d 694 (2d Cir. 1943).

[379] *Id*. at 704.

[380] *Id*.

[381] By private attorney general, I am referring to both the litigant and plaintiff, and plaintiff's attorney.

[382] Robert F. Blomquist, *Rethinking the Citizen As Prosecutor Model of Environmental Enforcement Under the Clean Water Act: Some Overlooked Problems of Outcome-Independent Value*, 22 GA. L. REV. 337, 367 (1988) (noting that Congress enlisted citizens to supplement the work of the Environmental Protection Agency).

[383] "Any person who . . . uses in commerce . . . any false designation of origin, false or misleading description of fact, or false of misleading representation of fact . . . shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act."15 U.S.C. § 1125(a) (2000).

providing relief for a broad class of injured or likely to be injured plaintiffs.[384]

The CFAA envisions a private attorney general role filled by the deputized victims of hackers, spammers, and other computer abusers. America Online ("AOL") has served as a private attorney general to punish e-mail spammers and other computer abusers who victimize its millions of subscribers. In one instance, AOL argued that a bulk e-mailer who sent its subscribers large numbers of unauthorized and unsolicited e-mail advertisements ("spam") violated the CFAA, as well as Virginia's state computer crime statute.[385] AOL also claimed that the bulk e-mailer violated AOL's service agreement and trademarks and committed a variety of torts.[386]

2. *State Private Attorney General Statutes*

Theoretically, injured consumers could use state consumer protection statutes to punish and deter cybercrimes on the Internet. State FTC acts modeled after the Uniform Deceptive Trade Practices Act ("UDTPA") provide for private tort-like enforcement, as well as public enforcement actions. For example, Chapter 93A of the Massachusetts General Law authorizes lawsuits by the Attorney General,[387] individual consumers, [388]or business competitors.[389] It provides for monetary damages and equitable relief for consumers "injured" as a result of an unfair or deceptive trade practice. While there is no case law determining whether false and deceptive Internet communications violate Chapter 93A or other UDTPA inspired acts, courts would probably extend these state-based causes of action. Chapter 93A also provides for punitive damages, such as multiple damages for "a willful or knowing violation."[390] Attorneys' fees may be recoverable, along with injunctive relief, monetary damages, and treble damages.[391] Relief under Chapter 93A is in addition to traditional tort remedies, [392] as well as relief under the Lanham Act.

3. *Tort Law & The Private Attorneys General*

The rubric under which all of the definitions of the private attorney general fall is "private action for offenses committed against the public as a

---

[384] *See, e.g.*, L'Aiglon Apparel v. Lana Lobell, Inc., 214 F.2d 649, 651 (3d Cir. 1954).

[385] AOL, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998).

[386] AOL's complaint had seven counts: Count I (False Designation of Origin under the Lanham Act); Count II (Dilution of Interest in Service Marks under the Lanham Act); Count III (Exceeding Authorized Access in Violation of the Computer Fraud and Abuse Act); Count IV (Impairing Computer Facilities in Violation of the Computer Fraud and Abuse Act); Count V (Violations of the Virginia Computer Crimes Act); Count VI (Trespass to Chattels under the Common Law of Virginia); and Count VII (Common Law Conspiracy to Commit Trespass to Chattels and Violate Federal and Virginia Statutes). *Id.* AOL sought compensatory and punitive damages, attorney's fees, costs, and permanent injunctive relief. *Id.*

[387] MASS. GEN. LAWS ANN. ch. 93A, § 4 (1997).

[388] *Id.* § 9.

[389] *Id.* § 11.

[390] *Id.*

[391] *See id.*

[392] Linthicum v. Archambault, 379 Mass. 381, 383 (1979).

whole." For example, an industry-wide cover-up of the deadly consequences of unprotected exposure to asbestos dust, which destroyed the health of hundreds of thousands of American workers, was unmasked in asbestos products liability cases.[393] Johns-Manville Sales Corporation had definite knowledge, as early as the 1930s, of the deadly consequences of unprotected exposure to asbestos dust and had a corporate policy not to inform employees that x-rays taken by company doctors revealed clear evidence of asbestosis.[394] Johns-Manville executives claimed that this policy was motivated by their concern that their employees "live and work in peace and the company . . . benefit by their many years of experience."[395] As a result, the asbestos industry lulled government regulators into complacency for decades with false assurances that their products posed no health hazard.[396]

The line between public and private has blurred in the past three years, as state and city governments have begun to hire private attorneys to prosecute class action lawsuits against industries whose hazardous products create a financial burden borne by taxpayers. Forty-six states have joined in a multi-billion dollar settlement to compensate for the public health costs of tobacco addiction.[397] Similar partnerships may be formed to address cybercrime, as private litigants are frequently in a better financial position to underwrite litigation costs than state and federal law enforcement authorities, who are already burdened by a costly war on drugs.[398] Existing torts are being adapted to include Internet-related wrongdoing in order to deter online harassment, spam e-mail, invasions of privacy, and hate speech. For example, a doctor won a $675,000 libel damages award for a false charge of accepting kickbacks posted on a Yahoo! message board.[399] Plaintiffs are successfully using John Doe subpoenas[400] to identify anonymous wrongdoers on the Internet. A John Doe subpoena was used to identify an anonymous poster who charged a physician with underbidding on contracts for Emory University's Pathology Department.[401] Old torts are readily adaptable to cyberspace.

---

[393] Michael L. Rustad, *In Defense of Punitive Damages in Products Liability: Testing Tort Anecdotes with Empirical Data*, 78 IOWA L. REV. 1, 40, 70 (1992); Michael L. Rustad, *Nationalizing Tort Law: The Republican Attack on Women, Blue Collar Workers and Consumers*, 48 RUTGERS L. REV. 673 (1996) [hereinafter *Nationalizing Tort Law*. *See* Thomas Koenig & Michael Rustad, *His and Her Tort Reform: Gender Injustice in Disguise*, 70 WASH. L. REV. 1 (1995).

[394] Johns-Manville Sales Corp. v. Janssens, 463 So. 2d 242 (Fla. Dist. Ct. App. 1984).

[395] *Id.* at 250.

[396] *See* Prudential Ins. Co. v. U.S. Gypsum Co., 828 F. Supp. 287, 290–92 (D.N.J. 1993).

[397] Ruth Gastel, *The Liability System*, INS. INFO. INST., July 2001, LEXIS, News Group File.

[398] Law enforcement agencies have been slow to adapt to Internet-related wrongdoing. Michigan Governor John Engler recently proposed a Michigan state "cybercourt" to address high-tech issues. *See* Doug Isenberg, *The Pros and Cons of 'Cybercourts'*, GigaLaw.com, *at* http://www.gigalaw.com/articles/2001/isenberg-2001-04-01.html (last visited Aug. 8, 2001). Law enforcement agencies such as the Secret Service, FBI, State Department, Customs Service, and the Department of Defense have all received increased budgetary allocations for greater cybercrime prosecution. Kelli Arena, *Special Report: Crime on the Internet*, CNN.com/Law Center, *at* http://www.cnn.com/2001/LAW/04/16/cybercrime.overview/index.html?s+7 (April 18, 2001).

[399] Margaret Cronin Fisk, *Net Libel Verdict Is Upheld*, NAT'L L.J., Dec. 25, 2000, at A19.

[400] John Doe subpoenas are served on the Internet Service Provider, requiring the disclosure of the identity of customers who post anonymously on the Internet. *Id.*

[401] Fisk, *supra* note 399.

B. TORT REMEDIES FOR COMPUTER MISUSE & ABUSE

1. *Trespass to Chattels*

Trespass is a broad "form of action that, at common law, provide[s] for a wide spectrum of injuries, from personal injuries caused by negligence to business torts and nuisances."[402] A trespass to chattels occurs when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization.[403] Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action. Courts have held that a hacker's intrusion into a computer network constitutes a trespass to chattels.[404] Trespass to chattels is actionable only if the defendant dispossesses chattels belonging to another and the chattel is impaired as to its condition, quality, or value. This tort is triggered when the possessor is deprived of the use of the chattel for a substantial period of time. If harm is caused to some person or thing in which the possessor has a legally protected interest, then there may also be a trespass to chattels.

An ex-employee of Intel Corporation was found to have committed trespass to chattels by sending thousands of e-mails to current employees of the company.[405] His purpose in sending the e-mails was to form an organization of former Intel employees who have filed claims against the company. Intel ordered the ex-employee to stop sending mass e-mails to its employees. When the ex-employee continued sending messages, Intel charged him with trespass to chattels, arguing that the ex-employee's unsolicited e-mails constituted a trespass of Intel's computer system.[406] The court agreed, rejecting the former employee's First Amendment defense, because Intel was a private corporation and there was no state action.[407]

In *Register.com, Inc. v. Verio, Inc*., a register of Internet domain names sought an injunction against a competitor to prevent the use of automated software robots to access and collect registrants' contact information contained in its database.[408] The district court issued a preliminary injunction barring the defendant from using its search robots to extract information from the plaintiff's website. The court found that the defendant was trespassing on the plaintiff's site by violating the "Terms of Use" applicable to the database.[409]

---

[402] BRYAN A. GARNER, A DICTIONARY OF MODERN LEGAL USAGE 995 (2d ed. 1995).
[403] RESTATEMENT (SECOND) OF TORTS § 217(b) (1965).
[404] CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).
[405] *Ex-Employee's E-Mails to Intel Workers Are Not Protected Speech, Judge Rules*, COMPUTER & ONLINE INDUS. LITIG. REP., May 18, 1999, at 8.
[406] *Id*.
[407] *Id*.
[408] 126 F. Supp. 2d. 238 (S.D.N.Y. 2000).
[409] *Id*. at 255.

2. *Spamming As Cyber-Trespass*

"Spamming" is the practice of sending unsolicited or unwanted e-mail in an indiscriminate fashion. "Spam" is commercial bulk e-mail akin to the junk mail sent through the postal mail. There may be twenty-five million junk e-mail messages sent every day.[410] Spammers open accounts with providers such as AOL, Hotmail, and Prodigy to obtain the e-mail addresses of subscribers. The e-mail accounts are used to collect responses to the spammer's e-mails and "bounced back" messages.

Hotmail, a Silicon Valley company that provides free electronic mail on the World Wide Web, filed a trespass to chattels action against a spammer who sent thousands of unsolicited e-mails to its subscribers advertising pornographic materials.[411] A court found that the spammers trespassed upon Hotmail's computer space by causing tens of thousands of misdirected and unauthorized e-mail messages to occupy company computer resources.[412] In *America Online, Inc.* v. *LCGM, Inc*., AOL sued spammers who sent unsolicited bulk e-mails to AOL subscribers.[413] The spammers used false "aol.com" addresses in their spam headers to send over 60 million pieces of unauthorized bulk e-mail to AOL subscribers.[414] AOL's complaint included charges of trespass to chattels, false designation, and dilution by tarnishment.[415] The district court ruled in favor of AOL, finding that the defendants violated the Lanham Act's false designation of origin and dilution provisions, breached its terms of services, and violated the CFAA.[416] The court imposed punitive damages, treble damages, and attorneys' fees against the spammer.[417]

3. *The Duty to Maintain a Secure Website*

In July 2000, a hacker broke into the University of Washington Medical Center's internal network and downloaded computerized admissions records for four thousand heart patients.[418] The medical facility would have been negligent had it failed to exercise reasonable care under these circumstances, namely, had it not had adequate information security. The hacker's motivation in this case was to document the inadequate

---

[410] James W. Butler, *The Death of Spam and the Rise of DEM: A Bill to Ban It Could Backfire*, INTERNET NEWSL., Sept. 1998, at 3.

[411] Hotmail Corp. v. Van Money Pie, Inc., No., 98-20064, 1998 U.S. Dist. LEXIS 10729 (N.D. Cal. April 16, 1998).

[412] *Id*. at *19, *20.

[413] 46 F. Supp. 2d 444, 444 (E.D. Va. 1998).

[414] *Id*. at 448.

[415] *Id*. at 444.

[416] *Id*. at 449.

[417] AOL, Inc. v. LCGM, No. CA-98-102-A, 1998 U.S. Dist. LEXIS 20243 (E.D. Va. Dec. 7, 1998). *Accord* Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292 (D. Colo. 1998). In *Seidl*, the owner of an internet domain name alleged that a mortgage company violated Colorado's Deceptive Trade Practices Act and the Junk Fax law by using the domain name a an e-mail identifier for a bulk e-mail advertising campaign. *Id.* The plaintiff also alleged the commission of common law torts including trespass to chattels, negligence, violation of right of publicity, and false light invasion of privacy. *Id.*

[418] Kevin Poulsen, *Hospital Records Hacked Hard*, Infowar.com, *at* http://www.infowar.com/hacker/00hack_120700a_j.shtml (Dec. 7, 2000).

information security protecting confidential patient information at the medical center. This incident raises the question of whether the victims of hacker activity may be liable for negligently securing their computer systems. The remainder of this Section explores the potential liability of a website or computer system to third parties for permitting a hacker to invade its computer system.[419]

a. Duty of Care to Maintain a Secure Website

"An actor is negligent in engaging in conduct if the actor does not exercise reasonable care under all the circumstances."[420] Under a negligence formula, the greater the risk, the greater the duty. A hospital has a statutory duty to protect the privacy of its patients' records. It is unclear, however, whether a website owes a general duty of care to website visitors when there is no statutorily mandated standard of care. Even if a website's weak computer security is the legal cause of a website visitor's harm, the company may not be liable if a court determines that no duty exists.[421]

The negligence equation balances the burden of precaution against the foreseeable likelihood and severity of harm, thereby providing the defendant with the incentive to implement safety measures to reduce the radius of the risk.[422] The information industry will oppose this standard, recognizing that a duty of care in cyberspace will have a chilling impact on e-commerce. The insurance industry will argue that the threat of liability will cause companies to abandon their e-businesses during the midst of a new economic recession.

b. Setting the Standard of Care

Traditionally negligence has been based upon the standard of the reasonable person. The elements of negligence are duty, breach, causation and damages. In the case of information security, the corporate website must have a duty to exercise ordinary reasonable care for the benefit of website visitors before the plaintiff can prove that a corporation has breached its duty of reasonable care. The following discusses different tests for setting the standard of care in Internet security cases.

---

[419] Microsoft SQL Server Version 7.0 and Microsoft Data Engine ("MSDE") 1.0, for example, permit unauthorized users "to execute shell commands," which allows hackers to access secured, nonpublished files. U.S. Dep't of Justice, *supra* note 94. Another closely related question beyond the scope of this Article is whether a software vendor would also be liable for marketing or failing to recall software with known vulnerabilities. Microsoft, for example, has advised the NIPC that there are serious vulnerabilities with its software that permit "malicious users to run system commands on a web site." *Id.* It is unclear whether Microsoft has a postmarketing duty to take prompt remedial measures beyond a simple advisory. Another open question is whether software license agreement provisions disclaiming the implied warranty of merchantability would cover known vulnerabilities permitting intrusions.

[420] RESTATEMENT (THIRD) OF TORTS: GENERAL PRINCIPLES § 3, (Discussion Draft 1999).

[421] *Id*.

[422] Kenneth Simon, *The Hand Formula in the* Draft Restatement (Third) of Torts*: Encompassing Fairness As Well As Efficiency Values*, 54 VAND. L. REV. 901 (2001) (discussing the role of safety incentives in the negligence equation under the *Restatement (Third) of Torts*).

i. Custom or Industry Standard

A company's departure from industry standards or custom may be evidence of negligence. On the other hand, a company's compliance with custom may also be evidence of negligent website security. In a developing Internet economy, customary standards of care for security may not yet exist or may be woefully inadequate. The Internet security profession is developing standard protocol, such as secure sockets layers ("SSL") for constructing firewalls. De facto industry standards also exist for public key cryptography, digital signatures, and application gateways.

Evidence that a company has implemented "state of the art" security is some proof that it has not been negligent, but it is not dispositive. The standard of care followed by a particular industry may be the floor, but not the ceiling, of due care.[423] "A custom is little more than the law's term for a norm. The hornbook rule is that evidence of compliance with, or violation of, a customary way of doing things is admissible but not dispositive on the issue of the actor's negligence."[424] Judge Learned Hand was of the opinion that compliance with industry standards was not always a complete defense.[425] If a company fails to implement information security customarily used in the Internet industry, it may be found to be negligent.[426] In some circumstances, however, a defendant may be negligent, despite adherence to weak or non-existent information security practices.

A violation of a well-accepted information security standard may be a sufficient basis for a finding of negligent security. Microsoft, for example, sells products such as Microsoft Exchange 5.5 and 2000 with substantial security flaws.[427] Information security, is similarly based upon the salutary principle: the greater the risk, the greater the duty of care.[428] A company must take greater measures to guard the secrecy of information transmitted on the Internet. Companies protecting highly sensitive trade secrets from competitors may utilize one-time passwords or digital certificates. The

---

[423] The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) (stating that a "whole calling may have unduly lagged in the adoption of new and available" radios on barges).

[424] Kenneth S. Abraham, *The Trouble with Negligence*, 54 VAND. L. REV. 1187, 1207 (2001).

[425] In *The T.J. Hooper*, a tugboat owner was held to be negligent for not providing radio sets for its vessels:

> [I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.

60 F.2d at 740.

[426] Michael L. Rustad & Lori Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 248 (1995) (arguing that failure to comply with industry security standards constitutes negligence).

[427] *See St. Bernard Software's Update EXPERT V5.1 Helps Network Administrators Protect Their Servers and Workstations from Vastly Increasing Security and Stability Problems Found in Many Popular Microsoft OS*, BUS. WIRE, Aug. 3, 2001, LEXIS, News Group File. *See also U.S. Nuclear Tracking Software Had Glitch*, INDUSTRY STANDARD.COM, July 24, 2001, LEXIS, News Group File.

[428] Internet security policies are based upon risk profiling. The burden of precaution depends upon the radius of the risk or consequences of potential computer intrusion. *See generally Internet Security Policy: A Technical Guide (DRAFT)*, NIST, *at* http://www.csrc.nist.gov/isptg/html/ISPTG-3.html (July 31, 1997).

DOD, for example, would not use packet filter firewalls appropriate for a Mom and Pop store selling knitted socks on the Internet.

ii. Statutory Levels of Care

Some predict that the government will take a more active role in specifying minimum levels of information security. Legislatures will begin to set statutory standards of care for certain Internet activities.[429] For example, a few jurisdictions require lawyers to encrypt e-mail messages to clients or to obtain the consent of their clients to use unencrypted messages. There are hundreds of examples of legislators setting the standard of care under traditional tort law. Where a statutory standard of care exists, plaintiffs may prove negligence by showing: (1) that they are members of the class of persons protected by the statute; (2) that the statute protects against the particular interest invaded; and (3) that the harm suffered was the particular harm or hazard envisioned by the statute.[430]

The promulgation of statutory or administrative standards of care might be state standards regarding encryption, digital signatures, and other information security devices. To promote the development of e-commerce, federal or state governments may adapt commercial-sector standards. For example, the National Computer Security Center of the National Security Agency ("NSA") administers the process for the C2 level of computer security certification.[431] Commercial-sector security standards are modeled

---

[429] An example of a statutory standard of care is the negligence standard under the Employer's Liability Act, ch. 149, § 2, 35 Stat. 65 (1908) (codified as amended at 45 U.S.C. § 51–60 (1994)). If an employer fails to meet the statutory standard of care and injury or death results, the employer is liable without additional evidence of negligence. Jeremy S. Sosin, *The Price of Killing a Child: Is the Fair Labor Standards Act Strong Enough to Protect Children in Today's Workplace*, 31 VAL. U. L. REV. 1181, 1193–94 (1997). In a common law negligence action, statutory standards may create a presumption of negligence arising from the violation of a statute enacted to protect a class of persons of which the plaintiff is a member against the type of harm suffered as a result of the violation. *See* Vesely v. Sager, 486 P.2d 151, 164 (1971). Many courts cite Section 286 of the RESTATEMENT (SECOND) OF TORTS (1965), which provides:

> The court may adopt as the standard of conduct of a reasonable man the requirements of a legislative enactment or an administrative regulation whose purpose is found to be exclusively or in part
>
> (a) to protect a class of persons which includes the one whose interest is invaded, and
>
> (b) to protect the particular interest which is invaded, and
>
> (c) to protect that interest against the kind of harm which has resulted, and
>
> (d) to protect that interest against the particular hazard from which the harm results.

RESTATEMENT (SECOND) OF TORTS, *supra* note 403, at § 286. Negligence formulas frequently use statutory violations to set the standard of care. For example, a landlord's defective electrical wiring of a dryer resulted in a child being injured by an electrical shock in *Smith v. Owen*, 841 S.W.2d 828 (Tenn. Ct. App. 1992). The court found that the defendant's violation of the ordinance was the proximate cause of the injury. *Id.* at 833.

[430] RESTATEMENT (SECOND) OF TORTS, *supra* note 403, § 286. Courts vary on whether a statutory violation is negligence per se or merely some evidence of negligence.

[431] De facto evaluation of security products vis-à-vis government standards is already occurring. Novell, Inc. formally applied for federal certification for their general-purpose network operating system. According to a research director: "a C2 rating . . . has become a standard for commercial businesses as well as government and military organizations. Customers are using it as a differentiator when making product purchasing decisions." *NetWare 4 Enters Final Phase of C2 Evaluation: On Track to Receive First Client-Server Network Rating*, PR NEWSWIRE, Aug. 28, 1995, LEXIS, News Group File (statement of John Pescatore).

after government-published standards. A minority of jurisdictions hold that the violation of a statutory duty is only some evidence of negligence in determining whether a defendant exercised due care.[432] The majority of jurisdictions provide that an unexcused violation of a statute that results in harm to the class the statute protects is negligence per se regarding the consequences that the statute is designed to prevent.[433] If a statute declares conduct unlawful, then the conduct is also deemed unreasonable for purposes of civil liability or negligence. "If the plaintiff already has a claim for negligence, then proof that the defendant violated an applicable statute reinforces that claim."[434] Few statutes impose penalties for inadequate Internet security. The Health Insurance Portability and Accountability Act ("HIPAA"), however, imposes public law penalties on health providers whose inadequate security endangers the integrity of patients' records. HIPAA imposes new medical data privacy rules that mandate greater information security for patients' online records.[435] Thus, a hospital or medical provider has a higher duty to prevent its computer system from being attacked than another business.

iii. Risk/Benefit Analysis

The common law tort of negligence recognizes a duty to protect data in a reasonable manner.[436] Under the negligence formula, the higher the risk, the greater the duty of precaution. Information may be classified according to the risk of loss from destruction or disclosure. Security may be altered depending upon whether the protected information is classified as sensitive, confidential, private, or public.[437] Judge Learned Hand's formulation of the reasonable care standard asks whether the burden of precaution is less than the probability and extent of damages (B < P x L). In *United States v. Carroll Towing Co.*,[438] Judge Hand articulated his famous theory of negligence:

> Since there are occasions when every vessel will break from her moorings, and since, if she does, she becomes a menace to those about her; the owner's duty, as in other similar situations, to provide against

---

[432] Dan B. Dobbs, THE LAW OF TORTS 316–17 (2000).

[433] Jurisdictions vary widely in the impact of statutory violations on tort duties. Many statutes provide administrative or criminal sanctions not explicitly prescribing tort remedies. *Id.* at 315. The effect of the violation of an Internet security standard may be treated as negligence per se or as only evidence of negligence. The majority of courts impose the rule of negligence per se when applying "the standard or rule of conduct from a nonprescriptive statute." *Id.* at 315.

[434] Michael Traynor, *Public Sanctions, Private Liability, and Judicial Responsibility*, 36 WILLIAMETTE L. REV. 787, 798 (2000).

[435] Mary Cesare-Murphy, *HIPAA Requirements Could Alter Focus of JCAHO Accreditation Surveys*, BEHAV. HEALTH ACCREDITATION & ACCOUNTABILITY ALERT, Sept. 1, 2001, LEXIS, News Group Files. Health care providers face tort liability for a wide variety of privacy-based information torts. *See generally* Nicolas P. Terry, *Cyber-Malpractice: Legal Exposure for Cybermedicine*, 25 AM. J.L. & MED. 327, 329–30 (1999).

[436] In the case of hospitals, financial institutions, or fiduciaries, the special relationship between the parties creates a duty to act in a reasonable manner to protect the weaker parties' interest. *See, e.g.*, Holtz v. J.J. B. Hilliard W.L. Lyons, Inc., 185 F.3d 732, 744 (7th Cir. 1999) (holding that where there is a special relationship between the parties, each party has a duty to act in a reasonable manner).

[437] *Internet Security Policy: A Technical Guide (DRAFT)*, *supra* note 428.

[438] 159 F.2d 169 (2d Cir. 1947).

> resulting injuries is a function of three variables: (1) the probability that she will break away; (2) the gravity of the resulting injury, if she does; and (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B < P."[439]

Judge Hand's formula is readily adaptable to a wide variety of computer security risks, including hacker attacks. A private litigant might argue that a company failed to implement industry standard security measures to protect the confidentiality of personal information. The key question balances risk and utility to question whether the cost of an information security measure is warranted; that is, whether the cost is less than the probability of harm multiplied by the gravity of the resulting injuries.[440]

A greater burden of precaution exists for the protection of the trade secrets of trading partners than for routine transactions. Third parties may pursue a negligence action against a company for failing to protect confidential information like trade secrets. A company may have a duty of special responsibility to safeguard the confidential or proprietary data on its computer system. Just as a hospital has a duty not to disclose patient treatment records, a company has a duty to use reasonable care to protect the confidential information of trading partners, customers, and website visitors.[441] A defendant is negligent when it fails to exercise reasonable care under all circumstances.

iv. Professional Standard of Care

Financial or business information specialists, such as CPAs, are potentially liable for negligently failing to secure business information on the Internet. In contrast, a financial or business ISP may "be insulated from liability for negligently disseminating false or misleading . . . information" on the Internet or for a wide variety of torts.[442] There is no case law holding Internet security professionals to the high standard of care required of other professionals like doctors and lawyers. The movement to professionalize security professionals and certify information systems will probably result in a professional standard of care.[443]

c. Economic Loss Doctrine

Assuming that a corporate website must bear liability for harm caused by its inadequate security, the economic loss doctrine poses an additional

---

[439] *Id.* at 173.

[440] A computer website will not be held to a bulletproof standard. Rather, courts must examine whether reasonable security measures were employed under a negligence-based theory. Rustad & Eisenschmidt, *supra* note 426, at 245–56.

[441] *See* Holtz, 185 F.3d at 744.

[442] Carl Pacini & David Sinason, *Auditor Liability for Electronic Commerce Transaction Assurance: The CPA/CA WEBTRUST*, 36 AM. BUS. L.J. 479, 499 (1999).

[443] NIST, for example, produces documents on best practices for firewalls, access control, and user authorization. *See generally Programs*, NIST, *at* http://www.nist.gov (last visited Aug. 19, 2001).

problem. Negligence liability has evolved as a remedy for physical harm, but not for economic losses. When a company's security is negligent, the resulting loss of trade secrets is chiefly an economic loss. Private litigants may choose from a wide array of remedies for trade secret misappropriation, including preliminary injunctive relief, monetary damages, lost profits, consequential damages, lost royalties, attorneys' fees, and punitive damages.[444] Trade secret protection, however, lasts only as long as the information is kept secret.[445] The economic loss rule adopted by most courts is a barrier to tort recovery for Internet-related security breaches. It is well established that physical damage to property other than the product itself is required in order to recover in tort.[446] It is doubtful that tort recovery is available for purely economic losses from negligent website security. A few courts, however, have side-stepped the economic loss rule where the plaintiff class is easily identifiable and the defendant is not exposed to indeterminate liability from an unknown number of claimants.[447]

4. *Tort Remedies for Computer Viruses*

Electronic viruses are virulent codes that may destroy the hard drive of a company computer. They are destructive computer instructions designed to alter or destroy data or information. They infect "executable files or the system areas of hard and floppy disks, and then make copies of [the virulent code]."[448] The threat of a computer virus is a serious concern for companies who may lose money, time, and key information assets when a malicious code is unleashed. In May of 1999, computers throughout the world were infected with the *CIH* virus.[449] Likewise, in March of 1999, the *Melissa* virus infected thousands of computers worldwide.[450]

The deliberate introduction of a virus into a computer system can constitute criminal as well as tortious trespass, and violates state and

---

[444] The Uniform Trade Secrets Act ("UTSA") § 3 (codified as CAL. CIV. CODE § 3426.3 (1997)) (enumerating remedies for misappropriation which include exemplary damages for "willful and malicious misappropriation").

[445] *Id.* § 1 (d). The UTSA is a model statute approved by the National Conference of Uniform State Laws ("NCCUSL") in 1979 and amended in 1985. The UTSA defines trade secrets to include "information, including a formula, pattern, compilation, program, device, method, technique or process that (1) derives independent economic value, actual or potential, from not being general known . . . ." *Id.* A company must use reasonable efforts to protects its trade secrets, not every possible or conceivable step. Rockwell Graphic Sys., Inc. v. DEV. Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991). The negligence-based formula would dictate that computer security against hackers be proportional to the profile of risk. Computer security is greater for valuable trade secrets than routine business information. Digital signatures with encrypted messages, for example, may be the only reasonable means of protecting customer lists transmitted on the Internet.

[446] *See* Moorman Mfg. Co. v. Nat'l Tank Co., 435 N.E.2d 443, 447–52 (Ill. 1982) (holding there is no tort liability for economic losses). *See generally* W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON, & DAVID G. OWEN, PROSSER AND KEETON ON THE LAW OF TORTS § 129, at 997 (W. Page Keeton ed., 5th ed. 1984).

[447] *See, e.g.*, People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107 (1995) (permitting tort recovery for purely economic loss to airline whose terminal was shut down due to negligent toxic spill in nearby railroad yard).

[448] *Computer Virus FAQ for New Users*, Internet FAQ Archives, *at* http://www.faqs.org/faqs/computer-virus/new-users/ (last visited July 19, 1999).

[449] *Id*.

[450] John D. Penn, *Beyond the Quill: Big Brother Really Is Watching: Following Computers' Trails*, 18 AM. BANKR. INST. J. 12 (1999).

federal laws. A company that knowingly distributes infected computer software might be held liable for fraud or misrepresentation. The introduction of a computer virus might also constitute conversion or trespass to chattels.[451] The vast majority of virus cases involve unknown perpetrators, as extraordinary law enforcement efforts are necessary in order to locate the source of a virus. State and federal computer crime statutes have been involved on a few occasions to punish those who release viruses, but these cases are the exception, not the rule. For example, the author of the *Melissa* virus pled guilty to violating New Jersey and federal law after the virus caused eighty million dollars of damage.[452] The inability of criminal law to address effectively new threats to the common good was illustrated by the dismissal of all charges against the author of the *Love Bug*, the "most destructive computer virus to attack the Internet."[453] Although forty-five million computers were infected by this computer virus,[454] Philippine law enforcement authorities were powerless to prosecute the perpetrator, since no criminal statute had been violated.[455]

Tort remedies may be used to fill the gap in punishing the planting of computer viruses. For example, a company that has failed to use antiviral software might be liable based on a negligence theory. Additionally, the propagators of computer viruses have probably committed several intentional torts. A computer virus creating a DoS attack might be viewed as a trespass to chattels. In contrast, a virus that destroys a hard drive might be conceptualized as the tort of conversion.[456] Consequently, tort liability for Internet security violations will probably result in greater investments in computer security to protect our most critical assets from terrorists and other cybercriminals.

III. CONCLUSION

In less than a quarter of a century, software publishing has grown from an infant industry to become America's third largest industrial sector.[457] In less than a decade, the Internet has become part of mainstream culture. It is now difficult to imagine a world without bandwidth, browsers, and bytes. By September of 2001, an estimated 169,355,382 Americans spent an

---

[451] Robin A. Brooks, *Deterring the Spread of Viruses On-line: Can Tort Law Tighten the 'Net'?*, 17 REV. LITIG. 343, 366 (1998).

[452] *CERT Taking on New Role*, NETWORK WORLD, Dec. 13, 1999, at 6.

[453] *Love Bug Suspect Can Still Face Civil Suits: Philippine Prosecutor*, AGENCE FRANCE PRESSE, Aug. 23, 2000, LEXIS, News File Group.

[454] *Id.*

[455] Patti Waldmeir, *Dark Side of Cybercrime Fight: An International Treaty on Law Enforcement for the Web Poses Unsettling Questions About Civil Liberties*, FIN. TIMES (LONDON), May 10, 2001, at 17.

[456] The difference between trespass to chattels and conversion is in the degree of loss or damages. In the tort of conversion, the chattel has been destroyed or substantially interfered with. The tort of trespass to chattels is an interference with rights in tangible property. The measure of damages for conversion is replacement of the chattels, whereas the measure of damages for trespass to chattels is the actual harm to the chattel. DAN B. DOBBS, THE LAW OF TORTS 122 (2000).

[457] Steve Lohr, *Study Ranks Software As Number 3 Industry*, N.Y. TIMES, June 3, 1997, at D2 (citing study by Nathan Associates funded by the Business Software Alliance).

average of three hours per week on the Internet.[458] By 2002, 490 million people around the world will have Internet access.[459] As the numbers demonstrate, the Internet is the place where increasingly millions of Americans pay bills, do their banking, consult professionals, shop for gifts, communicate electronically, and connect with family and friends.

The rise of the Internet has created new subcultures of cybercrime. Cybercriminals are attracted to the Internet because, as the famous bank robber Willie Sutton once said, "That's where the money is." This attraction has been illustrated by the wave of recent attacks against major websites and portals, which drew attention to the vulnerability of prominent e-businesses such as Microsoft, Amazon.com, and E*Trade. "Today's terrorist groups and anti-social elements are more like tech-savvy businessmen than bandits of yesteryears. Armed with laptops, satellite phones, and Internet access, they are embracing technology to further their objectives."[460] Foreign terrorists already use "information warfare" techniques to disrupt military operations by harming command and control systems, the public switch network, and other high-tech systems.[461] While each session of Congress has prompted new legislation to deal with cybercrime,[462] the executive branch is also advocating a wide range of new substantive federal laws to deal with "unlawful conduct committed through the use of the Internet."[463]

A legal time lag in cybercrime enforcement is inevitable because state and federal statutes cannot keep pace with Internet developments. Criminal statutes quickly become outdated because of technological changes. A fundamental principle of criminal law is that there must be "advance warning to the public as to what conduct is criminal and how it is punishable."[464] This is an almost impossible burden to meet at a time when emerging technologies give rise to novel forms of socially harmful behavior.

Private policing punishes and deters conduct inimical to public safety that is not detected by public authorities. Private enforcement is particularly necessary for litigating against powerful corporate actors in cyberspace.[465] Tort law's remarkable capacity to adapt and evolve to meet new threats and dangers makes it an important institution of social control

---

[458] *Average Web Usage*, Nielsen/NetRatings, *at* http://pm.netratings.com/nnpm/owa/Nrpublicreports.usageweekly (visited Oct. 3, 2001) (showing figures for the week ending Sept. 30, 2001).

[459] CyberAtlas, *The World's Online Population*, *at* http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html (Oct. 26, 2001).

[460] Kavita Kaur, *Terrorists on the Net: Dynamiting the Peace Domain*, COMPUTERS TODAY, Aug. 15, 1999, at 78.

[461] Parker, *supra* note 7.

[462] For example, in 2000, Senator Kay Bailey-Hutchinson (R-Tex) proposed legislation that would double the five-year criminal sentence for "fraud or related activity in connection with computers." *See* Robert MacMillon, *Sen. Hutchinson Seeks to Double Hacker Sentences*, Newsbytes, *at* http://www.newsbytes.com/news/00/143996.html (Feb. 16, 2001).

[463] U.S. Dep't of Justice, *supra* note 1.

[464] THOMAS H. KOENIG & MICHAEL L. RUSTAD, IN DEFENSE OF TORT LAW 220 (2001).

[465] *Nationalizing Tort Law*, *supra* note 393.

in cyberspace. A strong tort regime in cyberspace will teach Internet wrongdoers that "tort does not pay."[466]

[466] Michael L. Rustad & Thomas Koenig, *Crimtorts As Corporate Just Deserts*, 31 U. MICH. J.L. REFORM 289, 315 (1998).