COMMENT

ELECTRONIC COMMERCE, HACKERS, AND THE SEARCH FOR LEGITIMACY: A REGULATORY PROPOSAL

By Michael Lee, Sean Pak, Tae Kim, David Lee, Aaron Schapiro, and Tamer Francis[†]

ABSTRACT

The escalation of electronic commerce offers a wealth of opportunity for businesses. This technological revolution may be undermined by consumers wary of the increased threat of online invasions of privacy through hacking. The authors detail the various types of security infiltrations—both beneficial and detrimental—that hackers can perpetrate. After examining the current state of federal laws governing hacking, namely the Consumer Fraud and Abuse Law of 1984, the authors posit their recommendations for a realistic regulatory proposal based on an understanding of current technological capabilities.

TABLE OF CONTENTS

[†] Michael Lee, Sean Pak, Tae Kim, Aaron Schapiro, and Tamer Francis are third-year law students at Harvard. David Lee is an associate with the law firm of Shearman & Sterling.

This comment was the second-place winner of the 1998 *Berkeley Technology Law Journal* Comment Competition.

> You bring me a select group of 10 hackers and within 90 days, I'll bring this country to its knees.[1]
>
> — Jim Settle, Former Director, FBI Computer Crime Squad

> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.[2]
>
> — the "Mentor"

According to many experts in academia and industry, cyberspace will one day replace real space as the preferred medium for conducting busi-

[1] Chris O'Malley, *Information Warriors of the 609th (The Air Force's 609th Information Warfare Squadron)*, POPULAR SCIENCE, July 1997, at 74.

[2] The Mentor, *The Mentor's Last Words* (visited Apr. 16, 1999) <http//:insane.bloodline.com/mentor.html>.

ness.[3] Indeed, 1998 was a record year for electronic commerce,[4] with more than nine billion dollars of retail online sales.[5] The sudden increase in the volume of electronic commerce has prompted many experts to adjust upward their forecasts for the growth of electronic commerce.[6]

Underlying this optimistic picture for electronic commerce, however, is the basic assumption that consumers and companies will be able to establish what Peter Denning has termed "trust" in the exchange transaction between buyers and sellers in cyberspace.[7] Despite the theoretical advantages of conducting commerce in cyberspace[8] and the exponential expansion of the Internet,[9] many consumers continue to have little confidence in

[3] For example, the theory of friction-free markets once posited that Bertrand competition would necessitate pure price competition on the Internet, such that Internet markets would have lower prices than real space markets. *See* Joseph Bailey & Erik Brynjolfsson, In Search of "Friction-Free Markets": An Exploratory Analysis of Prices for Books, CDs and Software Sold on the Internet, at 3-5 (1998) (unpublished manuscript) (on file with authors).

[4] Although Internet-based commerce is the most visible form of electronic commerce, the former is clearly a subset of the latter. As used in this paper, the term "electronic commerce" encompasses all commercial transactions involving the exchange of "bits" as opposed to "atoms."

[5] *See Commerce Department to Measure Online Sales' Impact* (visited Feb. 5, 1999) <http://www.internetnews.com/ec-news/article/0,1087,archive_4_65111,00.html>. There exists a wide variation in estimates of online shopping due to differences in terminology and methodology. *See* Maryann Jones Thompson, *Spotlight: Why E-commerce Forecasters Don't Get It "Right,"* THE INDUSTRY STANDARD, Mar. 1, 1999, *available at* <http://www.thestandard.com/metrics/display/0,1283,850,00.html>.

[6] *See* Thompson, *supra* note 5.

[7] *See* Peter J. Denning, *Electronic Commerce, in* INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS 385-86 (Dorothy E. Denning and Peter J. Denning eds., 1997). Denning argues that cyberspace "trust" would be less difficult to establish with reliable authentication technology, i.e., that current cyberspace code precludes a social norm of "trust." According to Denning, "If human coordination, rather than information exchange, had been at the center of attention of protocol designers, it would be exceedingly difficult today to spoof an e-mail or Internet address or to forge a signature on a document." *Id.* Indeed, building trust online is the focus of many Internet-related companies and consultancies. *See* Maryann Jones Thompson, *E-commerce Spotlight: Building Trust Online,* THE INDUSTRY STANDARD, Jan. 25, 1999, *available at* <http://www.thestandard.com/metrics/display/0,1283,829,00.html>.

[8] Critics have argued that electronic commerce on the Internet reduces overall transaction costs (e.g. search costs, negotiation, and delivery costs) and facilitates connectivity so as to eliminate considerations of real space time and distance. *See, e.g.*, Denning, *supra*, note 7, at 377-78.

[9] According to a 1997 Robertson & Co. report, the total number of U.S. Internet users is expected to reach 102 million by the year 2000. See ComputerWorld, *Commerce*

the ability of sellers to deliver goods and services without compromising the security of sensitive information.[10] In fact, retail purchasers on the Internet still represent only a tiny fraction of all consumer spending.[11] The most visible agents of distrust have been individuals loosely described as "hackers."[12] Under constant media and governmental scrutiny, hackers have come to occupy a prominent and often mythical role in the popular discourse on electronic commerce.[13]

Surprisingly, however, academic discourse has failed to adequately address the challenges and opportunities posed by hackers for the regulation of cyberspace and electronic commerce. Some critics[14] of regulation have simply cited hackers to further the ambitious claim that attempts to regulate the Internet and its activities are "futile" in general.[15] Others have taken the contrary position that cyberspace actually facilitates effective regulation and that technological solutions will ultimately eliminate the threat to electronic commerce posed by hackers.[16] Somewhere between these opposite ends of the spectrum, Lawrence Lessig has posited that hackers pose little threat or relevant disorder to a regulatory scheme in

by Numbers (visited Apr. 9, 1999) <http://www.computerworld.com/home/Emmerce.nsf/All/pop>.

[10] In a 1999 national survey conducted by Netzero, more than 53 percent of the respondents cites "privacy and security" as their biggest concerns regarding online shopping. *See* Beth Cox, *Security, Privacy Remain Top Consumer Concerns*, (visited Apr. 9, 1999) <http://www.internetnews.com/ec-news/article/0,1087,4_95031,00.html>.

[11] *See* Greta Mittner, *E-commerce Companies Rejoice*, RED HERRING, Jan. 4, 1999, *available at* <http://www.redherring.com/insider/1999/0104/news-shopping.html>.

[12] *See* discussion *infra* Part I.B.

[13] *See* discussion *infra* Part I.

[14] These critics can be characterized either as optimists or pessimists, depending on how one views the broader implications of the advent of electronic commerce. *See* discussion *infra* Part V.C.

[15] *See, e.g.*, David G. Post, *Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. ART. 3 (visited Jan. 20, 1998), *available at* <http://www.law.cornell.edu/jol/post.html>. *See also* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[16] For example, Jeffrey Schiller, a computer security expert at M.I.T., claims that encryption technology such as PGP ("Pretty Good Privacy") can provide security against most hacking attacks and that "at this early stage, the insecurity of the Internet is primarily a result of human error and lack of user security education initiatives." Catherine Therese Clarke, *From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191, 231-32 (1996) (internal quotations omitted).

which the "code" or the architecture of the Internet permits *ex ante* constraints on the vast majority of the inhabitants of cyberspace.[17]

Although several distinct models for analyzing the regulation of cyberspace and electronic commerce have emerged with the development of the academic debate, these models, along with current legislation, share an undue emphasis on and reverence for the unique implications of Internet technology. All the models described above gauge the threat posed by hackers—indeed, their very relevance in the regulation debate—solely in terms of the technology or code by which hackers operate. Unfortunately, this (mis)understanding of new technology has precluded analyses of issues equally relevant to an informed discussion on the optimal regulation of cyberspace for the purposes of promoting electronic commerce. Issues meriting further study include: (1) the precise nature of the threat to electronic commerce posed by hackers and their tools, (2) the failure of current and proposed legislation to regulate hackers, and, finally, (3) the broader political nature of cyberspace code and its implications for regulating hackers.

[17] According to Lessig:

> We live life subject to the code [in cyberspace], as we live life subject to nature. Just as we do not choose whether to see through a wall or not, we don't choose whether to enter America Online without giving our password. Superman might choose whether to see through a wall; and hackers might be able to choose whether to enter AOL with a password. But we are neither supermen or hackers (if such a distinction exists). We live life subject to the constraints of the code; however (and by whomever) these constraints have been set.

Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMMLAW CONSPECTUS 181, 184 (1997) [hereinafter *Constitution of Code*]. In defense of his claim that code-based solutions for regulating cyberspace are effective despite hacking, Lessig has further stated:

> But from the fact that 'hackers could break any security system,' it no more follows that security systems are irrelevant than it follows from the fact that 'a locksmith can pick any lock' that locks are irrelevant. Locks, like security systems on computers, will be quite effective, even if there are norm-oblivious sorts who can break them.

Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 896 n.80 (1996) [hereinafter *Constitution in Cyberspace*]. Admittedly, Lessig does not claim that hackers do not pose any threat to electronic commerce. Rather, his discussion of hackers is limited to their effect on the long-term architectural development of the Internet, apart from their role in electronic commerce.

I. THE THREAT TO ELECTRONIC COMMERCE

Hacking via the Internet is currently a significant problem, with trends indicating cause for alarm. The business losses from such intrusions can be massive: MCI lost over fifty million dollars when hackers downloaded more than 50,000 credit card numbers,[18] and Citibank lost ten million dollars when its computer network was compromised by a crime group in Russia.[19] The service, repair, and restoration costs from such intrusions are also extensive. For example, in *United States v. Morris*,[20] the labor costs to eradicate a computer virus and monitor the computer systems' recovery was estimated at up to $186 million.[21]

Although these highly publicized cases illustrate the enormous power that a single hacker or a group of hackers may yield, the economic threat posed by hackers is not confined to a handful of Fortune 500 companies. A recent survey by Ernst & Young found that of 1,290 businesses, nearly half had been the victims of information security breaches in the past two years,[22] and at least twenty of these companies had suffered losses exceeding one million dollars.[23] According to a Senate report, major banks and corporations lost $800 million due to hacker intrusions in 1995 alone.[24] Moreover, businesses are continually under attack from multiple sources. For instance, Rockwell International, Inc., claims that hackers attempt to break into the company's computers via the Internet on a "regular basis."[25]

Yet the problem is almost certainly much more extensive than suggested by the available statistics, as many businesses are reluctant to admit that their computers have been successfully attacked by hackers.[26] According to William J. Cook, author of the Justice Department's manual on computer prosecution, "[O]rganizations often swallow losses quietly rather than notifying the authorities and advertising their vulnerability to

[18] *See* David L. Gripman, *The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 169-70 (1997).

[19] *See* Marc D. Goodman, *Why the Police Don't Care About Computer* Crime, 10 HARV. J.L. & TECH. 465, 472 (1997).

[20] 928 F.2d 504, 505-07 (2d Cir. 1991).

[21] *See* Gripman, *supra* note 18, at 171.

[22] *See* Marc S. Friedman & Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway*, 9 No. 5 J. PROPRIETARY RTS. 2, 7 (1997).

[23] *See* Goodman, *supra* note 19, at 472.

[24] *See* Friedman & Bissinger, *supra* note 22, at 7.

[25] *Id.*

[26] *See id.* at 2.

shareholders and clients."[27] Federal law enforcement officers estimate that over ten billion dollars worth of data is stolen in the United States annually,[28] and that reports of computer intrusion from government agencies and private businesses jump seventy percent every year.[29] According to Dennis Hughes, the FBI's senior expert on computer crime, "[T]he hackers are driving us nuts. Everyone is getting hacked into. It's out of control."[30]

Careful review of the empirical evidence suggests that hackers pose a significant threat to the future of electronic commerce in two significant ways. First, they *directly* endanger electronic commerce by increasing the risk that private and financial information transmitted over the Internet will be intercepted and used for illegal purposes. Second, they *indirectly* stifle the growth of electronic commerce by undermining the public's confidence in the safety of conducting financial online transactions. This indirect effect stems largely from the way that consumers, as well as policy makers, perceive hackers. Because hackers are typically characterized as "super-criminals" with extraordinary powers and malicious intent, many consumers may still be afraid to buy and sell goods and services over the Internet, even with adequate safeguards. Thus, the full extent of the economic threat posed by hackers can only be understood by analyzing the phenomenon of hacking from both technological (i.e., code-based) and sociological (i.e., norms-based) perspectives.

II. THE STRUGGLE FOR CODE

The history of the Internet and computer networks in general may be viewed as a story of a continuing arms race between those who seek to erect barriers of protection and those who seek to circumvent these barriers. This story pits governmental organizations, law enforcement officials, and computer professionals against a diverse and ever-expanding group of "[h]ackers, crackers, snoops, spoofers, spammers, scammers, shammers, jammers, intruders, thieves, purloiners, conspirators, vandals, Trojan horse dealers, virus launchers, and rogue program purveyors."[31] The object of

[27] *Id.*

[28] *See id.* at 7.

[29] *See id.* at 10.

[30] Gripman, *supra* note 18, at 173.

[31] Dorothy E. Denning & Peter J. Denning, *Preface* to INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS at vii (Dorothy E. Denning & Peter J. Denning eds., 1997).

the struggle is the power to control the "code" (i.e., the underlying architecture) of the Internet.

A. The Arsenal

In *Cyberspace Attacks and Countermeasures,* Dorothy Denning uses the following table to categorize the known methods, tools of attack, and safeguards for protecting against such attacks. The countermeasures are labeled according to their primary purpose: to prevent attacks (P), to detect their occurrence (D), or to facilitate recovery after an incident (R).[32]

	Encrypt. (secrecy)	*Authen. (includ. Crypto)*	*Access Control, Monitor*	*Audit, Intrusion Detect.*	*Virus Scan & Disinf.*	*Backup*	*Design, Implem., Operat.*
Eavesdropping	P						P
Snooping Storage	P		P	D			P
Snooping Memory			P	D			P
Tampering		D	P	D		R	P
Spoofing		PD		D			P
Jamming			P	D			P
Injecting Code		PD	P	D	PD		P
Cracking							P
Exploiting Flaws			P	D			P

Although the categories used above were not meant to be definitive or comprehensive, they do provide a useful framework for discussing the arsenal of weapons available to hackers and anti-hackers. It is important to note, however, that some of the new Java-based attacks may not fit neatly into any of the above categories.

[32] *See id.*

B. Methods and Tools of Attack

When attacking a secure Internet site, a hacker may use one or more of the following methods and tools, serially or in combination, to identify security holes and gain unauthorized access.[33]

1. *Eavesdropping and Packet Sniffing*

The Internet, like most networks, is susceptible to eavesdropping (i.e., "the passive interception of network traffic").[34] The preferred method of eavesdropping on the Internet is installing a program packet (commonly referred to as a "packet sniffer") for monitoring network on a local workstation, an Internet gateway, or router machine, which directs and relays network traffic. According to the Computer Emergency Response Team ("CERT") Coordination Center, following their initial discovery in 1993, sniffer attacks have allowed hackers to gain unauthorized access to more than 100,000 host machines in the United States alone.[35]

Once installed (either by a user with legitimate access or by a hacker posing as a legitimate user), packet sniffers can be used to intercept login IDs and passwords, as well as credit card information and private e-mail messages.[36] Intercepted login IDs and passwords then can be used to access other secured sites. Empirical evidence indicates that once hackers have logged into a secured system through sniffer attacks, their actions can vary.[37] In some cases, the hackers moved on to other systems without damaging or otherwise altering any systems or files. In other cases, however, they engaged in malicious activities, including denial of service, unauthorized possession, compromise of integrity, and destruction of data.

[33] For example, after cracking a password, a malicious hacker might pose as a legitimate user, browsing through files to gain confidential and financial information. If root access is acquired, the hacker may also leave a destructive logic bomb or alter login records to conceal his tracks. *See* Dorothy E. Denning, *Cyberspace Attacks and Countermeasures, in* INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS 29, 32 (Dorothy E. Denning & Peter J. Denning eds., 1997).

[34] *Id.*

[35] This estimate is likely to be very conservative. *See id.*

[36] Upon installation, a packet sniffer places the /dev/nit interface (a widely installed network utility tool) into "promiscuous mode" and logs the first 128 bytes of all TCP (i.e. Internet) sessions being routed through the compromised host machine. The hacker then periodically accesses the host machine to collect the intercepted information. For a more detailed description of packet sniffers, see E. Eugene Schultz & Thomas A. Longstaff, *Internet Sniffer Attacks*, PROCEEDINGS OF THE NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE 534-541 (Oct. 1995).

[37] *See id.* at 141.

2. *Snooping and Downloading*

Other methods for acquiring information without altering it include snooping and downloading data without authorization.[38] Rather than monitoring and intercepting network traffic, a hacker can obtain unauthorized access to a secured site by using a cracked password and obtain confidential and financial information by browsing through documents, e-mail messages, password files, and other data stored on disk or memory.[39] The hacker will often download data to his or her computer before browsing through them. Snooping and downloading can also be done by insiders, especially ex-employees.

3. *Tampering or Data Diddling*

Instead of just downloading data, a hacker, upon obtaining unauthorized access, can alter or delete files and programs stored on secured systems (commonly referred to as data "tampering" or "diddling").[40] The potential threat can be especially serious if the hacker is able to obtain root access.[41] An extreme form of tampering attack is the placement of logic bombs, which "detonate" in response to a predefined event.[42] Upon detonation, a logic bomb may crash the entire system or wipe out entire file systems. Another dangerous form of tampering is replacing system programs with their Trojan horse versions, which "look and feel" like the original program, but execute hidden and often malicious code.[43] A popular Trojan horse attack involves a modified login program, which operates normally but has the added function of storing copies of login IDs and passwords in a hidden file. As with snooping, data tampering can also be done by insiders.

4. *Spoofing*

In a "spoofing attack," the hacker deceives the victim into disclosing security or financial information by impersonating other users or computers. This form of attack can be analogized to a con game where "the at-

[38] As noted earlier, a hacker can combine packet sniffing and snooping attacks to infiltrate a large number of secured sites.

[39] In 1996, two hackers were convicted of downloading 1,700 credit card numbers from a Tower Records computer system that they had infiltrated. *See* Dorothy E. Denning, *supra* note 33, at 33.

[40] *See id.* at 33-34.

[41] Root access enables the hacker to modify system files and programs and to access personal files of every user on the system.

[42] *See* Dorothy E. Denning, *supra* note 33, at 33-34.

[43] *See id.*

tacker sets up a false but convincing world around the victim."[44] Common forms of spoofing attacks include e-mail forgery and looping, where a hacker uses one system as a "springboard" to log into another system in order to conceal his or her identity and location.[45]

5. *Jamming or Flooding*

Otherwise known as "denial-of-service" attacks, jamming or flooding attacks aim to disable or to tie up system resources.[46] Two common forms of this attack are: (1) consuming all available memory or disk space by flooding the target system with large volumes of e-mail, and (2) tying up network connection resources by sending multiple SYN messages requesting Internet connections. Both methods involve using fake return addresses or anonymous remailers to conceal the identity of the attacker. Jamming or flooding attacks can be used to target commercial websites or individual users. The motivation for these types of attack are often personal.

6. *Injecting Malicious Code*

Injecting malicious code (commonly referred to as "viruses") is another type of hacking attack with potentially devastating effects.[47] As a general rule, the malicious code is transmitted through an external device (e.g., a floppy disk) or through the network (e.g., e-mail attachments) and is activated when the file or data stream is loaded into memory and executed. Typically, the malicious code is designed to be self-replicating (hence the label "virus"), and consequently it may be difficult to predict or control the extent and scope of the damage.[48] To avoid detection, virus writers often incorporate encryption or self-modifying code into their viruses. In an interesting twist, cryptoviruses, which encrypt rather than destroy the victim's data, have been employed in Britain for extortion purposes.[49]

[44] Edward W. Felten et al., *Web Spoofing: An Internet Con Game* (last modified Feb. 1997) <http://www.cs.princeton.edu/sip/pub/spoofing.html>.

[45] *See* Dorothy E. Denning, *supra* note 33, at 35.

[46] *See id.* at 36.

[47] *See id.* at 37-38.

[48] A highly publicized example is the Internet Worm program released by Robert Morris. For a detailed account of the Worm program, see KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER 280-81 (1991).

[49] *See* Michael McCormack, *Europe Hit by Cryptoviral Extortion*, COMPUTER FRAUD & SECURITY BULLETIN, June 1, 1996, at 3.

7. *Cracking Passwords, Codes, and Keys*

Systems that employ password security schemes or encryption algorithms are susceptible to attacks aimed at guessing or finding (commonly referred to as "cracking") a valid password or encryption key.[50]

8. *Exploiting Flaws in Design, Implementation or Operation*

In addition to obtaining passwords by any of the above methods, hackers can also gain unauthorized access by exploiting undetected security flaws in the design, implementation, or operation of secured systems.[51] These security flaws can arise for a number of reasons, including "software bugs, lack of attention to security, and poor configuration."[52] New operating systems or architectures, such as Java, are especially susceptible to these types of attack.[53] Although many security holes are eventually detected and corrected, new ones inevitably arise, sometimes in the new code designed to fix existing flaws.[54]

C. Countermeasures

As with the various forms of hacking attacks and tools, the following categories of countermeasures are interrelated in that the effective operation of a countermeasure may ultimately depend on the success of other related countermeasures.[55]

1. *Encryption (Secrecy)*

Cryptography, defined as the science of using mathematical algorithms to disguise messages and information, is a powerful tool for protecting against various forms of hacking attacks. When used for purposes of secrecy, cryptographic algorithms can serve as effective countermeasures

[50] "Cracking" a password or encryption key (i.e., finding or guessing) should be distinguished from "cracking" a software application (i.e., disabling protection features). *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution,* 143 U. PA. L. REV. 709 (1995).

[51] A real-life example is the Network File Service ("NFS") and sendmail programs for the UNIX operating system, both of which originally contained bugs allowing regular users (and hackers posing as users) to obtain root access. *See* Dorothy E. Denning, *supra* note 33, at 38-39.

[52] *Id.* at 38.

[53] *See* discussion *infra* Part II.F.

[54] *See* Dorothy E. Denning, *supra* note 33, at 39.

[55] *See id.* at 41.

against eavesdropping and snooping.[56] Encryption, the subset of cryptography dealing with achieving and maintaining secrecy, involves applying a scrambling function to a given set of data so that only those who possess the right "key" can restore (or "decrypt") the encrypted data to its original ("cleartext") form. The strength of an encryption system is usually measured by the amount of effort (in terms of computing time) that would be required to "crack" it (i.e., to derive the original data from its encrypted form) by an outsider who knows the algorithm but not the key (or keys) used.

Two of the most popular encryption schemes are the Data Encryption Standard ("DES") promulgated by the National Bureau of Standards and the RSA system named after its inventors Ronald Rivest, Adi Shamir, and Leonard Adleman. The DES system is a single-key ("symmetric") system in which a common secret key is used to both encrypt and decrypt data.[57] The RSA system, by contrast, is a dual-key ("asymmetric" or "public key") system in which one key is used to encrypt and a second key is used to decrypt.[58]

The effectiveness of both the DES and the RSA systems has been challenged by critics in recent years. Theoretically, there are three ways to crack an encryption system:[59] (1) hackers can steal the key or suborn a key-holder; (2) hackers can hope to find a mathematical weakness in the cryptographic algorithm; or (3) hackers can use a "brute-force" method of trying all possible keys until the message is decrypted. While all cryptographic systems are susceptible to the first attack, it appears that current implementations of the DES and RSA systems are also vulnerable to attacks exploiting mathematical weaknesses and those utilizing brute-force methods.[60] As a result, there is a growing demand within the academic and

[56] Cryptographic algorithms can be used for two distinct purposes: secrecy and authenticity. The term "encryption" is generally used to refer to cryptographic systems used only for secrecy. *See id.*

[57] Typically, an encryption DES system is implemented by requiring a different session key for each communication and providing a different long-term key used for authenticating the user and for distributing session keys.

[58] As noted in the following subsection on authentication, public key systems can be used for authentication as well as encryption purposes.

[59] *See* Froomkin, *supra* note 50, at 752.

[60] In 1996, a 130-digit RSA key was cracked. RSA Laboratories recommends that keys be at least 230 digits (or more than 768 bits). In June 1997, a 56-bit DEC key was broken after four months of trial and error. According to cryptography experts, the DES algorithm is nearing the end of its useful lifetime. *See* Dorothy E. Denning, *Encryption*

business communities to strengthen existing encryption systems by using longer keys or to adopt alternative systems that are inherently more difficult to crack.[61] In the past the government has resisted these demands for change on the grounds of law enforcement and national security.[62]

Recently, the government offered a compromise solution based on key-escrow systems, which enable government agencies to keep a copy of the key needed to decrypt all encrypted communications.[63] Key escrow systems, in theory, satisfy both the demand for stronger encryption and the need for governmental monitoring of personal communications. These proposals, however, have been criticized on constitutional and technical grounds and have yet to be approved by Congress.[64]

2. *Authentication (Password Systems)*

In addition to maintaining secrecy, cryptographic algorithms also can be used for authentication purposes (i.e., to validate that the user is actually who he or she claims to be). If implemented properly, cryptographic systems can prevent against tampering, spoofing, and malicious code attacks.

Public-key encryption systems, such as the RSA scheme, are especially useful as authentication tools.[65] A user can validate his or her identity by encrypting the message with his or her private key. Upon receipt, the receiver will attempt to decrypt the encrypted message by using the sender's public key, which is freely accessible to all.[66] If the message has been altered or sent by an impostor, the verification will fail.

3. *Access Control and Monitoring (Firewalls)*

As a countermeasure against snooping and tampering, system designers can incorporate various methods and tools for monitoring and control-

Policy and Market Trends, in INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS 458 (Dorothy E. Denning & Peter J. Denning eds., 1997).

[61] *See id.* at 457-60.

[62] *See* Froomkin, *supra* note 50, at 711.

[63] *See id.* at 711-17.

[64] *See id.* at 717-51.

[65] An example of an RSA-based authentication scheme is the Pretty Good Privacy ("PGP") developed of Phil Zimmerman of MIT. For a more detailed analysis of public-key encryption systems, see Thomas Y.C. Woo and Simon S. Lam, *Authentication for Distributed Systems, in* INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS at 319-56 (Dorothy E. Denning & Peter J. Denning eds., 1997).

[66] The authenticity of the public key can be guaranteed by a trusted third party (e.g., a certification authority or a member of "a web of trust").

ling access to their secured systems.[67] For instance, UNIX systems only allow users with root accounts to access certain systems programs and data files. In addition, every program or file on UNIX can be configured with an access control list that specifies which accounts can read write, execute, or search that program or file.

Another example of an access and monitoring system is a firewall, which is placed between an organization's internal network (e.g., Intranet) and the Internet. By using a combination of password, packet filtering and encryption methods, firewalls can be designed to keep out unwanted intruders, exclude undesirable content, and prevent viruses.

4. *Auditing (Logging) and Intrusion Detection*

Most forms of hacking attacks (except for eavesdropping and cracking methods) can be detected by the use of auditing and intrusion detection systems. Auditing systems, which keep records of login activities, can serve as a valuable resource for detecting possible security breaches and for gathering evidence in support of an investigation or prosecution. Intrusion detection systems ("IDS") can provide greater security by enabling real-time detection of intrusion attempts.[68] IDS systems generally fall into two main categories:

1) Anomaly detection systems: Based on the assumption that all intrusive activities are necessarily anomalous, system designers can detect intrusion attempts by comparing current account activities against a "normal activity profile." Commonly used methods of comparison are statistical analysis, predictive pattern generation, and neural networks.

2) Misuse detection systems: Similar to virus scanners, misuse detection systems seek to detect intrusion attempts by searching for known attack patterns. The challenge is to distinguish legitimate account activities from known "bad" behavior.

[67] For a detailed description of monitoring systems, *see* Dorothy E. Denning, *supra* note 33, at 45-47.

[68] For an in-depth analysis of intrusion detection systems, *see* Aurobindo Sundaram, *An Introduction to Intrusion Detection* (visited Apr. 16, 1999) <http://www.cs.purdue.edu/coast/archive/data/author3.html>.

5. *Virus Scanners and Disinfectors*

Virus scanners are designed to detect the presence of malicious code by looking for signs or patterns of known viruses.[69] These programs can be configured to scan floppy disks, system memory, or network connections for virus signatures. Once detected, viruses can be removed by disinfectors. Virus scanners and disinfectors are ineffective against newly introduced or custom designed viruses.

6. *Backup*

Because it is difficult to detect and prevent hacking attacks in real time, backing up system data is essential to recovery from accidental and intentional data tampering (e.g., file deletions, virus programs, and logic bombs).[70] Backup systems, however, cannot prevent the unauthorized downloading and distribution of confidential and financial information.

7. *Secure Design, Implementation, and Operation*

Although no system can be made perfectly secure, all of the hacking attacks discussed above can be countered by making security a top priority in designing, implementing, and operating network systems. Useful tools and methods include good software engineering practices, formal methods, testing, and vulnerability analysis, configuration management, human practices, and user training.[71] Designers and users of secured systems would do well to heed Andy Grove's advice: "Only the paranoid survive."[72]

D. Related Activities: Cracking, Phreaking, Social Engineering

Most of the so-called "hackers" also engage in a wide range of other activities, including cracking, phreaking, and social engineering. Understanding the tools and methods of these activities is important for two reasons. First, many of the publicized attacks on government and corporate sites have involved a combination of hacking, phreaking, and social engineering tactics. Thus, protecting against hacking attacks alone may not be sufficient to secure an Internet site. Second, from a policy perspective, any regulatory framework designed to control hacking may have an unexpected impact on the ability to control other types of activities. For in-

[69] For a discussion of virus scanners and disinfectors, *see* Dorothy E. Denning, *supra* note 33, at 48-49.

[70] *See id.* at 49.

[71] *See id.* at 49-50.

[72] Andy Grove, ONLY THE PARANOID SURVIVE (1996).

stance, an effective ban on hacking tools and methods may encourage hackers to employ other means (e.g., cracking, phreaking, or social engineering) in their pursuit of thrills or profit.[73]

1. Cracking

To prevent unauthorized copying and use, software developers have incorporated various protection features into their programs. Some of the more common protection features include:[74]

1) Password protection: The user must supply a password before using the program.

2) Serial number protection: The user must supply a valid serial number before using the program.

3) Use limitation: The user can only use the program a given number of times without paying.

4) Time limitation: The user can only use the program for a fixed period of time without paying.

5) Disabling some of the functions: The user can only invoke all of the functions of the program upon payment.

6) Disk access / token protection: The user must insert a special disk into the floppy drive or attach a special device (i.e., token) to an input/output port before using the program.

7) CD access limitation: The user can only use the program if it is stored on a read-only CDROM.

8) Any of the above protection features disguised through encryption, "junk" instructions, or self-modifying code.

[73] A useful analogy is an underground water reservoir with vertical pipelines. Applying pressure on one of the pipelines will cause water levels to rise in the remaining pipelines. Similarly, applying regulatory pressure on hacking activities may cause incidents of related activities (e.g., cracking, phreaking, and social engineering) to rise.

[74] *See* +ORC ("the old red cracker"), *How to Crack, A Tutorial—Lesson 1* (visited Mar. 13, 1999) <http://www.geocities.com/Athens/Agora/1948/Crack/howto1.txt>. The old red cracker, a hacker, has authored one of the many "how-to" manuals on hacking available on the Internet. *See infra* note 76.

All of the above features are designed to make it difficult, if not impossible, for most users to use the protected program without payment or authorization.

"Cracking" is the act of eliminating or suspending one or more protection schemes inside a software application to facilitate unauthorized copying and use.[75] The most useful tool for a cracker is the "debugger," a software tool designed to assist software developers in identifying and correcting flaws in a computer program. A debugger allows the user to execute a computer program one instruction or one set of instructions at a time. Another useful tool is the "memory dump analyzer," which enables the user to examine in detail the memory space of a computer system. By employing these readily available tools in conjunction, a cracker can identify and isolate protection features of a software application and disable them by altering its object code.[76]

Once a protection feature has been disabled, the cracker can automate the process by writing an executable software patch, which can be downloaded and executed by anyone. Cracking patches (commonly referred to as "cracks" or "crackz") as well as pirated software (commonly referred to as "warez") can be downloaded from publicly accessible websites.[77] Valid serial numbers for various software applications are also available on the Web.

By all accounts, cracking activities pose a significant threat to the software industry.[78] According to a study conducted by the Business Software Alliance ("BSA") and Software Publishing Association ("SPA"), nearly one of every two new business applications used globally were pi-

[75] *See id.* (defining cracking as "understanding, broadly individuating, locating exactly and eliminating or suspending or deferring one or more protection schemes inside a software application you do not possess the source code of").

[76] "How-to" manuals vary in quality and accessibility. An example of a well-written and widely-read manual is the *How to Crack, A Tutorial*, *supra* note 74, written by "the old red cracker." This manual gives step-by-step instructions on how to crack various types of software applications, including those written for the Windows operating system.

[77] *See, e.g.*, Kurupt Technologies, *Kurupt Warez* (visited Apr. 16, 1999) <http://www2.ipeg.com/>.

[78] The provision of cracker utilities and serial numbers that are intended to circumvent the copyright protections in software, when used by a direct infringer, may constitute contributory infringement under copyright law. *See Software Publishers Association Policy Statement on Contributory Infringement* (visited Feb. 5, 1999) <http://www.spa.org/piracy/contrib.htm>.

rated in 1996, resulting in an estimated $11.2 billion of lost revenue for the software industry.

2. *Phreaking*

Before the advent of the World Wide Web, hackers communicated with one another via Bulletin Board Systems ("BBS"). BBSs are privately owned and privately operated networks that can be accessed through a dial-up modem connection. As PCs and modems became readily available, various hacking groups began to operate their own underground BBSs, which served as forums for sending messages to other hackers, exchanging information on newly discovered hacking attacks, and sharing pirated software. By the early 1990s, hundreds, if not thousands, of hacker BBSs were in operation across the United States and Europe.

To gain access to a BBS outside the local exchange area, a hacker had to establish a long-distance modem connection, thus giving rise to "phreaking." Phreaking is "a subset of computer hacking and involves hacking of telephone systems to make fraudulent phone calls, or manipulating telephone systems."[79] By building various devices from off-the-shelf components and by making use of confidential information regarding telephone systems, phreakers are able to make long-distance calls, install calling features like caller-ID or call waiting, and make conference calls—all for free. Some of the more popular phreaking devices include:[80]

1) Red Box: Built from a modified Radio Shack tone dialer or a Hallmark greeting card, a Red Box allows the user to make free phone calls by simulating a quarter tone for public telephones.

2) Blue Box: Built from the same components as a Red Box, a Blue Box allows the user to convince the telephone system that he or she is actually a telephone operator.

3) Black Box: Built from a 10k ohm resistor, a Black Box prevents the phone company equipment from detecting that the user has answered an incoming call. People who call the user's number will not be billed for the call.

[79] Jim Christy, *Rome Laboratory Attacks: Prepared Testimony of Jim Christy, Air Force Investigator, before the Senate Governmental Affairs Committee, Permanent Investigations Subcommittee, May 22, 1996, in* INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS 64 (Dorothy E. Denning & Peter J. Denning eds., 1997).

[80] For a more detailed listing of various phreaking devices, see Voyager, *#hack Frequently Asked Questions (FAQ)* (visited Feb. 5, 1999) <ftp://rtfm.mit.edu/pub/usenet-by-group/alt.2600/alt.2600_FAQ>.

In addition to calling long-distance for free, hackers often employ phreaking tools and methods to disguise their calling location, thereby making it difficult, if not impossible, for law enforcement officials to trace suspected hackers back to their origin in real time. It is especially difficult to trace hacking attacks made through multiple paths across multiple systems in multiple countries, as was the case in the highly publicized attacks on the Rome Laboratory of Griffiss Air Force Base during 1994.[81]

3. *Social Engineering*

As the least discussed category of hacking-related activities, social engineering may also be the most important. "Social engineering" is a term used within the hacking community for hacking techniques that rely on "weaknesses in wetware [i.e., people] rather than software."[82] The aim is to trick or deceive people into revealing passwords or other information that may compromise the security of a target system or organization.[83] Classic social engineering methods include phoning a "mark" (usually a user or an employee) who has the desired information and posing as a field service technician or a fellow employee with an urgent access problem.[84]

A more sophisticated method is to design and send promotional material (e.g., a fake entry form for a mass-mail sweepstakes) via regular mail to be filled out by the mark or group of marks. One of the entries should be a password for verification (usually associated with a prize) based on the assumption that the mark will enter the same password that he or she uses to gain access to his or her network account. The hacker can then use this password to gain unauthorized access to secured accounts. Other methods include posing as a system operator ("SYSOP") to an unwitting user in an online chat room or going through someone's trash, commonly referred to as "dumpster diving."

Social engineering tactics are often used to complement other methods of hacking and, in some cases, may prove to be the most effective and time efficient way to gain unauthorized access to secured systems.[85] As a

[81] *See* Christy, *supra* note 79, at 57-65.

[82] *See* bernz, *The Complete Social Engineering FAQ §1.1* (visited Feb. 4, 1999) <http://members.tripod.com/~bernz/socenfaq.txt>.

[83] *See id.*

[84] *See id.*

[85] For a real-life account of social engineering, see *The New York Newsday Interview with Ice Man and Maniac: Inside the Underworld of "Hacking,"* N.Y. NEWSDAY, July 22, 1992, at 83.

general rule, it is easier to find lapses in security by the people who use the systems, rather than in the systems themselves.[86]

E. Password Systems: An Arms Race of the Past

In the preceding analysis, various hacking attacks and their countermeasures were described without reference to their related histories. Most security systems, however, are the result of many years of competition between those responsible for maintaining security and those seeking to attack it. Thus, at any given point in time, the design of these systems reflect the ongoing arms race between the system designers and the hackers. For this reason, it is often instructive to trace the history of various security systems in addition to analyzing their present strengths and weaknesses.

One illustrative example is the development of the password security scheme used in the UNIX operating system.[87] The UNIX system was initially implemented with a password file containing the actual passwords of all the users. This scheme was quickly proven to be "excessively vulnerable" to lapses in security.[88] The vulnerability stemmed from the fact that there was no way to prevent privileged users from making copies of the password file. Thus, once a hacker had access to a password for privileged user status, he or she had access to all the passwords for the system. In addition, accidental disclosures of the password file jeopardized the security of the entire system. Experiences with earlier remote-access systems indicated that such disclosures occurred with alarming frequency.[89]

In order to remedy these flaws, the UNIX designers added an encryption component to the password system. Before each user password was stored in the password file, it was first encrypted using a modified version of the M-209 cipher scheme used by the U.S. Army during World War II.[90]

[86] For instance, the most sophisticated password system can be circumvented by deceiving one of its users to disclose his or her password unwittingly.

[87] The following discussion on the history of password security systems is based on Robert Morris & Ken Thompson, *Password Security: A Case History* (visited Jan. 21, 1998) <http://www.securezone.com/Information_Sources/Papers/>.

[88] *See id.*

[89] *See id.*

[90] The problem with the original M-209 scheme was that, with a given key, encrypted messages (or "ciphers") were trivial to invert. It was much more difficult to reverse engineer the key given the cleartext input and the encrypted messages. Thus, the UNIX designers decided to use the password not as the text to be encrypted, but as the

Theoretically, the encrypted password system was very difficult to penetrate because brute force methods for inverting the encryption algorithm used were prohibitively slow. The system, however, proved to be vulnerable to so-called "key search" attacks. This class of hacking attacks is based on the fact that people tend to choose relatively short passwords that are easy to remember, such as words, names or birth dates. Using this insight, hackers were able to gain unauthorized access to secured systems with encrypted password schemes by comparing the encrypted entries in the password file against a collection of trial passwords that have been encrypted using the same algorithm as the one used by the target system. The success of this method depended on the hacker's ability to decrease the required amount of computing time by carefully choosing the collection of trial passwords. The most successful approaches employed trial passwords derived from a dictionary or list of names.[91]

In response to the unexpected success of key search attacks, the UNIX designers adopted the following countermeasures:

1) Slower encryption: To increase the amount of computing time required to conduct key search attacks, the M-209 algorithm was replaced with the slower DES encryption algorithm approved by the National Bureau of Standards.

2) Less predictable passwords: The password entry program was redesigned to encourage users to adopt longer and more obscure passwords.

3) Salted Passwords: To reduce the likelihood of finding a match using a large collection of encrypted password files, the password system was modified to append a randomly generated 12-bit number (called the "salt") to the password typed in by the user before being encrypted and stored in the password file.

With these countermeasures in place, the UNIX operating system is considered to be one of the more secure operating systems on the market. It is important to note that the development of these countermeasures were made possible by the decision (on the part of the UNIX designers) to pub-

key to encrypt a predetermined constant. The encrypted result was then stored in the password file.

[91] Some "profitable" entries to include as trial passwords are: (1) the dictionary with the words spelled backwards; (2) a list of first names, last names, and street names; (3) all valid license plate numbers; (4) social security and telephone numbers.

licize the design of the password system and to invite attacks on its security, rather than "playing the customary make-believe game in which weaknesses of the system are not discussed no matter how apparent."[92]

At the same time, the system is not perfect and remains vulnerable to unanticipated hacking attacks made possible by exploiting a flaw in the implementation or by capitalizing on rapid advances in technology. For instance, brute force methods for inverting the DEC algorithm may become more feasible as the computing power available to the general public continues to increase exponentially.[93]

F. Java-Based Security Holes and Safeguards: The Arms Race of the Future

As the battle for control of the password system continues, the advent of the World Wide Web and the Java programming language has spawned a new arms race between those seeking to erect barriers of protection and those seeking to circumvent them. Although this new battle is being fought with some of the same weapons used to attack and protect password systems of the past, the unique characteristics of the World Wide Web and the Java language in particular have created new opportunities for hackers.

One of the most powerful features of the Java programming environment is the ability to develop and distribute executable content (commonly referred to as "applets") across heterogeneous platforms.[94] In effect, Java has transformed the Web from a static collection of mostly textual pages to an interactive and animated world of mini-applications that can be downloaded and executed on any machine on the Internet. With Java applets at their disposal, content providers on the Web now possess unprecedented levels of programming power and expressive potential.

Unfortunately, the very properties that make Java so exciting also make it the greatest threat to Internet security.[95] If a Java-compatible Web browser is not carefully configured, it can provide a malicious applet with the ability to delete files on the user's personal computer and to send private information over the network surreptitiously.[96] The solution, how-

[92] Morris & Thompson, *supra* note 87, at 5.

[93] *See* discussion *supra* Part II.C.1.

[94] For a detailed discussion of the Java programming language and executable content in general, see Joseph A. Bank, *Java Security* (Dec. 8, 1995) <http://swissnet.ai.mit.edu/~jbank/javapaper/javapaper.html>.

[95] *See id.*

[96] *See id.*

ever, is not as simple as completely preventing Java applets from accessing resources on the host machine. Without access to certain resources, Java applets would be of limited value.[97] For instance, a word processor that cannot save files is useless.[98] The challenge is to identify the resources required by a particular Java applet and to provide controlled access to those resources without jeopardizing the security of the host machine.

Although the Internet community is only beginning to appreciate fully the dangers posed by uncontrolled Java applets, experts have long recognized the security threats posed by the Java programming environment.[99] Known Java-based attacks can be organized into five categories:

1) Data tampering attacks: Hackers can exploit various implementation flaws in Java to create and distribute malicious applets that modify or delete files and memory locations.[100]

2) Denial-of-service attacks: Malicious applets can also tie up system resources and crash host machines by consuming processor cycles and misallocating memory resources.[101]

3) Disclosure attacks: Malicious applets can transmit private information stored on the host machine by accessing user files and establishing covert channels with an undisclosed third-party site on the Internet.[102]

4) Annoyance attacks: Malicious applets can project offensive video and audio data on the host machine without the user's consent or authorization.[103]

5) Web spoofing attacks: Malicious applets can also deceive the user into thinking that he or she is communicating with a trusted site through a secure connection when in fact all submitted information

[97] *See id.*

[98] *See id.*

[99] *See, e.g., id.*; Gary McGraw & Edward Felten, *Understanding the Keys to Java Security—the Sandbox and Authentication,* JAVA WORLD, May 1997, *available at* <http://www.javaworld.com/javaworld/jw-05-1997/jw-05-security.html>; Drew Dean et al., *Java Security: Web Browsers and Beyond, in* INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS 241-71 (Dorothy E. Denning & Peter J. Denning eds., 1997).

[100] *See* Bank, *supra* note 94.

[101] *See id.*

[102] *See id.*

[103] *See id.*

> is being forwarded to an undisclosed third-party site on the Internet.[104]

While Netscape and Microsoft have redesigned their Java-compatible browsers to protect against many of the known attacks, effective countermeasures have not been developed for others, including denial-of-service and Web-spoofing attacks.[105] Although denial-of-service attacks may cause at worst inconvenience for an individual user, Web-spoofing is a dangerous and nearly undetectable security attack that can pose a significant threat to conducting electronic commerce on the Internet.[106]

The potential dangers of spoofing attacks on the Web were vividly illustrated by a team of computer science researchers at Princeton University, who created a "shadow copy" of the entire World Wide Web.[107] The researchers placed a spoofing program on one of the servers linking the victim to the rest of the Web (referred in the following discussion as "the hacker's server"). Upon installation, the spoofing program first rewrites all of the URLs on a selected Web page so that they point to the hacker's server rather than to a real server on the Web. If the victim requests a Web page through any of the rewritten URLs, the spoofing program fetches the real page from the Web and modifies the page before forwarding it to the victim. The requested page can be modified to store hidden copies of form entries, passwords, or other information submitted by the victim. To complete the illusion, JavaScript programs can be used to hide all evidence of the spoofing attack from the victim.

One particularly troublesome property of this attack is that it is effective even when the victim believes that he or she is requesting a Web page through a "secure" connection.[108] Because the spoofing program is acting as a hidden intermediary between the victim's computer and the Web, the secure connection is established to the hacker's server, rather than the intended server. Thus, any information transmitted over this connection, whether encrypted or not, is visible to the spoofing program.

As the Princeton researchers noted in their paper, there appears to be no fully satisfactory countermeasure to Web-spoofing attacks, short of disabling the Java feature entirely.[109] Until an effective countermeasure is

[104] *See* Felten et al., *supra* note 44.

[105] *See* Bank, *supra* note 94, at 10.

[106] *See* Felten et al., *supra* note 44.

[107] For a detailed description of Web spoofing attacks, see *id.*

[108] *See id.*

[109] *See id.*

discovered, users conducting secured commercial transactions on the Web are forced to choose between risking undetected disclosures of their financial information and foregoing Java compatibility altogether.

In addition to the security threat posed by Web-spoofing attacks, new and unanticipated Java-based attacks are being discovered on a regular basis. For instance, in February of 1997, anonymous hackers (using the pseudonyms "Major Malfunction" and "Ben Laurie") exposed two new Java-based attacks that "crack a 'secure' client machine wide open."[110] The first attack enables a hacker to discover the real identity of any client machine despite the use of precautionary measures such as firewalls, proxies, and SOCKS hosts.[111] The second and more dangerous attack allows a hacker to scan any TCP/IP port on a client machine.[112] Using this attack, a hacker can copy sensitive information transmitted over the compromised port and surreptitiously transmit this information back to his or her machine through a covert channel. In response, Netscape and Microsoft have since released patches to prevent against these types of attacks.[113]

The arms race between hackers and Java designers has just begun. No one can predict when the race will end or who will win. What is clear, however, is that Java will play an increasingly larger role in the development of the World Wide Web as "marketspace."

G. Implications for Regulating Hackers

The preceding analysis suggests that problems posed by hackers cannot be solved by technological means alone. History and experience have shown that no system can be made perfectly secure. "Secured systems" employing code-based solutions will always remain vulnerable to unexpected attacks exploiting overlooked flaws in design, implementation, or operation. Moreover, new technologies, such as Java, create new opportunities for users and hackers alike. Often the very properties that make these new technologies exciting and valuable will also give rise to new and unexpected security threats.

[110] Although the hackers had employed the newly discovered attacks to hack their way through firewalls in January of 1997, they had decided to give Netscape and Microsoft ample time to address the problem before they publicly disclosed their methods. *See* Gary McGraw, *Is Your Browser a Blabbermouth? Are Your Ports Being Scanned?*, JAVA WORLD, Mar. 1997, *available at* <http://www.javaworld.com/javaworld/jw-03-1997/jw-03-securityholes.html>.

[111] *See id.*

[112] *See id.*

[113] *See id.*

The insufficiency of code-based solutions is best expressed by Peter and Dorothy Denning in their book Internet Besieged: Countering Cyberspace Scofflaws, an anthology of leading experts on Internet security:

> We believe that the [problems caused by hacking attacks] are a serious threat to information infrastructures everywhere. Until they are addressed satisfactorily, all the widely touted boons of the Internet—from tele-work to distance education to electronic commerce—will not be realized ... We also believe that the solutions to these problems cannot be achieved solely by technological means. The answer will involve a complex interplay among law, policy, and technology.[114]

III. THE STRUGGLE FOR NORMS

As hackers battle against system designers for control of the code, they find themselves battling one another for control of the internal norms governing the hacking community. Initially, hackers were a homogeneous and tightly knit community, united by a common desire to learn and a strong code of ethics.[115] They viewed themselves as "learners and explorers who want to help rather than cause damage, and who often have very high standards of behavior."[116] In fact, they were generally scornful of those who employed hacking methods and tools for malicious or profit motives.[117]

The so-called "hacker ethic" included the following principles[118]:

[114] Dorothy E. Denning & Peter Denning, *Preface*, *supra* note 31, at x-xi (emphasis added).

[115] *See generally* Dorothy E. Denning, *Concerning Hackers Who Break into Computer Systems,* at 13 (visited Jan. 23, 1998) <http://www.cpsr.org>.

[116] *Id.* at 1.

[117] Dorothy Denning, in her 1990 survey of the hacking community, stated that, according to all of the hackers she spoke with, malicious hacking was considered morally wrong. They also said that most hackers were not intentionally malicious, and that they were concerned about causing accidental damage. *See id.* at 10.

[118] In *A Novice's Guide to Hacking*, the "Mentor," one of the members of the Legion of Doom hacking group, presents the following set of guidelines for beginning hackers:

> Do not intentionally damage any system.
>
> Do not alter any system files other than ones needed to ensure your escape from detection and your future access.
>
> Do not leave your real name (or anyone else's) real name, real handle, or real phone number on any system that you access illegally.
>
> Be careful who you share information with.

1) Access to computers—and anything which might teach you something about the way the world works—should be unlimited and total."[119]

2) "All information should be free."[120]

3) "Thou Shalt Not Destroy."[121]

Surprisingly, the above principles mirror the ethical standards adopted by many computer security professionals. Where the two groups differ is that hackers did not consider the act of breaking into secured systems as inherently unethical.[122] They believed that hacking was not the same as stealing, but was in fact beneficial because hackers were able to uncover latent design flaws and security deficiencies.[123]

For the most part, these ethical principles were shared by leaders of the earlier generation of hackers. Most hacker organizations at the time operated by the rule of mutual teaching and learning: If a hacker wanted to learn from other hackers in the group, he or she had to contribute to the knowledge base.[124] Accordingly, those who accomplished the most and discovered the most creative hacking methods naturally became the leaders. Conversely, those who did not possess the drive to learn were precluded from benefiting from the knowledge of other hackers.

More importantly, these leaders also possessed the means to enforce the "hacker ethic." Prior to the Internet, hacker organizations existed

> Do not leave your real phone number to anyone you don't know.
> Do not hack government computers.
> Don't use codes unless there is no way around it.
> Don't be afraid to be paranoid.
> Watch what you post on boards.
> Don't be afraid to ask questions.
> Finally, you have to actually hack.

A Novice's Guide to Hacking—1989 Edition (visited Apr. 16, 1999) <http://insane.bloodline.com/mentor.html>.

[119] *Id.* at 5.

[120] *Id.* at 5.

[121] *Id.* at 10.

[122] *See id.* at 10-11.

[123] *See id.* at 11. *But see* Eugene H. Spafford, *Some Musings on Ethics and Computer Break-ins* (visited Jan. 19, 1998) <http://www.cs.purdue.edu>.

[124] *See The New York Newsday Interview with Ice Man and Maniac: Inside the Underworld of "Hacking," supra* note 85. In an interview with a Newsday reporter, Joshua Quittner, a well-known hacker by the pseudonym of "Maniac" stated: "[Hacking] is an organized hobby. You do these things for us and you get a little recognition for it." *Id.*

largely through closed networks such as bulletin board systems ("BBSs").[125] Because these BBSs were privately owned and privately managed, the leaders of hacking organizations had the power to accept only those who pledged to the existing norms and to remove from membership those that violated them. As a result, the original hacking community was a hierarchy based on expertise and knowledge, rather than profit or criminal intent. Moreover, this hierarchy based on accomplishment ensured that those who became the most technologically proficient—and thus had access to the most potentially dangerous knowledge—were those who had gone through the norm-reinforcing process.

Although some critics have questioned whether the so-called "hacker ethic" was the exception rather than the rule within the hacking community,[126] it is undisputed that such norms did exist and that they did have a profound effect on the way hackers viewed themselves and their activities. It is equally clear, however, that "the hacker ethic is fading fast with the advent of the Internet."[127]

The Internet drastically changed the internal dynamics of the hacking community in several different but related ways. First of all, the Internet's open architecture and its increasing accessibility have created huge opportunities for large businesses and individual entrepreneurs alike. As explained in the previous section on electronic commerce, online companies must obtain, transmit, or place commercially valuable information, such as credit card numbers, on the Internet.[128] With more commercial transactions being conducted on the Internet everyday, the potential profit for malicious hacking activities has grown dramatically. Consequently, the hacking community is increasingly attracting profit-driven and criminally-minded outsiders who do not follow the hacker code of ethics.[129]

Market forces aside, the very architecture of the Internet has made it difficult to maintain the hacker code of ethics. Many hackers have moved away from private and closed networks, such as bulletin board systems, onto the Internet. Whereas BBS-based hacking groups could easily exclude non-members or norm-violators, Internet-based hacking groups do not necessarily have such self-selecting mechanisms. It is now possible for a norm-breaking hacker to distribute his or her knowledge on the Internet

[125] *See* discussion *supra* Part II.D.2.

[126] *See* Benjamin J. Fox, *Hackers and the U.S. Secret Service* (visited Jan. 20, 1998) <http://www.gse.ucla.edu//iclp/bfox.html>.

[127] *Id.*

[128] *See* discussion *supra* Part I.

[129] *See* Fox, *supra* note 126.

users by simply posting a Web page. Criminals who want to take advantage of such information are finding it increasingly easier to gain access to dangerous hacking tools and methods without ever contributing to the mutual learning process or being subject to the norms that once governed the pre-Internet hacker community.

Although the Internet has certainly resulted in the dilution of norms within in the hacking community, it would be incorrect to say that norms no longer exist. Rather, the hacker community now consists of different sectors with different and often conflicting norms. Thus, the internal struggle for norms is critical to the future of the hacking community and the threat that it may pose to electronic commerce.

IV. CURRENT AND PROPOSED LEGAL REGIMES

The proliferation of various means by which hackers now manipulate the architecture of cyberspace and the growing visibility of hackers willing to misuse these means have not gone unnoticed by lawmakers. Unfortunately, however, existing attempts to regulate malicious hackers have produced dismal results by any standard. Although the sources of such failure are many, perhaps the most debilitating is that the regulatory approach underlying these attempts to control hackers betrays a cursory understanding of the dynamics of a community of social dissidents whose growth and danger have been fueled by the very laws attempting to extinguish it. Indeed, while direct regulation may have proven satisfactory for two centuries of real space regulation, a critical examination of both current laws and existing proposals for reform reveals that an entirely different form of regulation is appropriate for cyberspace.

A. Hacking as Crime: The Computer Fraud and Abuse Law of 1984

Congress has treated computer-related crimes as distinct federal offenses since its enactment of the Computer Fraud and Abuse Law of 1984 ("CFAA"), a seminal piece of legislation embodying the predominant approach to regulating hackers. As mentioned above, the types and sheer number of computer crimes have expanded considerably in a rather short span of time, and the CFAA has since been amended to cover new strains of computer crime facilitated by emerging technologies. Despite numerous amendments, however, the history of the CFAA and attempts to enforce its ever expanding provisions highlight severe inadequacies symptomatic of all current approaches to regulating hackers.

1. *The Text of the CFAA*

The CFAA prohibits "knowingly, and with intent to defraud, access[ing] a protected computer without authorization."[130] The text of the statute defines all relevant terms broadly. A "protected computer" is one

> exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer.[131]

However, a "protected computer" as defined by the CFAA is also one that is used in interstate or foreign commerce or communication.[132] As a result, any computer with Internet access qualifies as a "protected computer" for purposes of the CFAA.

2. *Access Denied—Access as Crime*

In theory, the CFAA does not prohibit all unauthorized, intentional access to such computers. Unauthorized, intentional access is proscribed only if such access is gained:

1) to obtain information relating to national defense or foreign relations. The *mens rea* requirement is that the offender knowingly access a computer without authorization or exceeding authorized access.[133]

2) to obtain information in a financial record of a financial institution or consumer reporting agency, any information from any department or agency of the United States, and information from any protected computer if the conduct involves an interstate or foreign communication.[134]

[130] 18 U.S.C. § 1030(a)(4) (1998).

[131] 18 U.S.C. § 1030(e)(2) (1998).

[132] *See id.*

[133] *See* 18 U.S.C. § 1030(a)(1) (1998). To be prosecuted under § 1030(a)(1), the actor must have reason to believe that such information will be used to the injury of the United States or to the advantage of any foreign nation. Further, the section is violated regardless of whether the actor communicates the information to another person or simply retains it. This crime is treated as a felony.

[134] 18 U.S.C. § 1030(a)(2) (1998). A "financial record" is defined as "information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution." 18 U.S.C. § 1030(e)(5) (1998). Under this section, ob-

3) to manipulate information on any computer that is exclusively for the use of the Government, or in the case of a computer not exclusively for such use, is used by or for the Government, such that the actor's offense adversely affects the use of the computer by or for the Government.[135]

4) to access a protected computer, without or in excess of authorization, with the intent to defraud and obtain anything of value, unless the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.[136]

5) to intentionally without authorization access a protected computer, where such access alters or damages program, information, code or command.[137]

taining information of minimal value ($5,000 or less) results in a misdemeanor, whereas obtaining valuable (more than $5,000) information or misusing information for financial or commercial gain or to commit a criminal or tortious act constitutes a felony.

[135] 18 U.S.C. § 1030 (a)(3) (1998). Section 1030(a)(3) criminalizes electronic trespasses on Federal Government computers. If the computer is not exclusively used by the Government, a violation is found if the trespasser's conduct affects the use of the computer by the Government.

[136] 18 U.S.C. § 1030(a)(4) (1998). This section contains a "computer use" exception where the intent to defraud consists only in making use of the computer.

[137] 18 U.S.C. § 1030(a)(5) (1998). Section 1030(a)(5) contains three provisions covering both outsider hackers and insiders who cause intentional, reckless or negligent damage. Violating the first two provisions is a felony, violating the third provision is a misdemeanor, with penalties based on the intent and authority of the actor.

The first provision prohibits unauthorized access to a protected computer where the actor knowingly transmits any program, information, code, or command which *intentionally* causes damage, covering both insiders and outsiders. The second provision prohibits unauthorized, intentional access to a protected computer, where such trespass *recklessly* causes damage, covering only outside hackers. The third provision prohibits the same action, but where such trespass causes damage, covering outside hackers. *See* S. Rep. No. 104-357, at 7-8 (1996).

Thus, insiders authorized access to a protected computer face criminal liability only for causing intentional damage, whereas outside hackers who break into a computer can be held liable for intentional, reckless, or negligent damage. This distinction between outsiders and insiders stems from the doctrine of trespass:

> To provide otherwise is to openly invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause, it is no crime unless that damage was either intentional or reckless. Rather than send such a dangerous message (and deny victims any relief), it is better to ensure that § 1030(a)(5) criminalizes all computer trespass, as well as intentional damage by insiders, albeit at different levels of severity.

6) to "knowingly and with intent to defraud," without authorization, "traffi[c] in any password or similar information through which a computer may be accessed" if "such trafficking affects interstate or foreign commerce; or such computer is used by ... the Government."[138]

7) to extort from any legal entity anything of value, transmitting in interstate or foreign commerce any communication containing any "threat to cause damage to a protected computer."[139]

Nevertheless, the aggregate effect of these qualifications has been to criminalize all unauthorized, intentional access to protected computers. Of particular significance in the history of the CFAA has been the willingness of Congress to reduce the requisite level of *mens rea* required for prosecution under the statute.[140] Whereas the 1994 amendment classified the requisite *mens rea* as "intentional, knowing, and reckless," the latest amendment enacted in 1996 eliminated the *mens rea* requirement altogether by imposing strict liability in addition to the requisite *mens rea* as enacted in 1994.[141] In short, Congress has criminalized unauthorized access into computer systems, regardless of whether the computer user actually intended to cause damage.[142]

Courts have also interpreted the *mens rea* requirement under the CFAA to facilitate the prosecution of hackers. In *United States v. Mor-*

Id.

The term "damage" is broadly defined to include any impairment to the integrity or availability of data, a program, a system, or information that (A) causes loss aggregating at least $5,000 in any one-year period to one or more individuals; (B) either modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals; (C) causes physical injury to any person; or (D) threatens public health or safety. *See* S. Rep. No. 104-357, at 8 (1996).

However, it is unclear whether there is a loss if, for example, a virus does not destroy files, but simply overloads the network, thus slowing down processing speed or using up some of a system's underutilized capacity. What is clear is that this section was added to address the threat posed by hackers. *See* S. Rep. No. 104-357, at 9 (1996) (describing § 1030(a)(5) as a measure that protects computers from hackers).

[138] 18 U.S.C. § 1030(a)(6) (1998).

[139] 18 U.S.C. § 1030(a)(7) (1998).

[140] *See* S. Rep. No. 104-357, at 10-11(discussing changes in *mens rea* level).

[141] *See* S. Rep. No. 104-357, at 9-12 (1996) (discussing effect of different *mens rea* requirements and intended effect from using different *mens rea*).

[142] *See id.* at 10 (indicating Congress's desire to punish hackers who unintentionally cause damage to computer systems).

ris,[143] the court "accepted the government's view that 1986 amendments to the [Computer Fraud and Abuse Act] eliminated any distinction between a break-in that damages files or steals money and what Morris was found guilty of, intentional unauthorized access that prevented authorized use."[144] More recently, the court in *United States v. Sablan*[145] ruled that the government does not have to prove intentional damage to a computer file but only intentional access without authorization.

3. *A Critical Evaluation*

The regulatory model justifying such *expansion* of the CFAA is flawed. The most immediate weakness is that the CFAA attempts to regulate "hacking," a particular type of computer crime without recognizing the important distinction between computer technology and the individuals responsible for its application. As described above, hacking is only one expression of computing prowess for the hacker who is equally technically proficient to engage in cracking and phreaking. Thus, to the extent that hackers engage in hacking either to express their computer prowess or to exploit structural deficiencies for monetary purposes, aggressive enforcement of hacking is unlikely to reduce the overall number of incidents of information-related crime. At best, a crackdown on hacking will prompt a shift in hackers from hacking to phreaking, cracking, or other related activities.

At worst, the crackdown on hacking represented by the CFAA is likely to prove counter-productive when analyzed from the perspective of other sources of behavioral constraint in cyberspace. For example, the public perception effectuated by the recent criminalization of all forms of hacking exacerbates the tense divide between hackers, law enforcement, and the general Internet public.[146] Inasmuch as laws affect the development of social norms, the average Internet user can be expected to view all forms of hacking as criminal and as undermining the consumer trust necessary for electronic commerce.

The application of public law is also allocatively inefficient in this context. The vigorous regulation of hackers through governmental law enforcement externalizes the costs of enforcing such norms to individuals

[143] 928 F.2d 506 (2nd Cir. 1991).

[144] Harold L. Burstyn, *Computer Whiz Guilty*, 76 A.B.A. J. 20, 20 (1990).

[145] 92 F.3d 865, 865 (9th Cir. 1996).

[146] For an insightful critique of current law enforcement along these lines, see Catherine Therese Clarke, *From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191 (1996).

who do not participate in electronic commerce. This unnecessary cost externalization, in turn, suggests that some form of indirect regulation through the market might best regulate hackers, at least from the perspective of allocative efficiency.[147]

Finally, the CFAA is no different from any other example of direct regulation that has proven highly ineffective in cyberspace.[148] For instance, jurisdiction is problematic: foreign hackers might not be within the reach of state and federal laws,[149] and the complexity of Internet routing creates jurisdictional conflicts among the localities, states, and countries that wish to exercise jurisdiction over transient information packets.[150] In short, the myriad problems that have plagued this statute from its inception justify a wholesale rejection of its approach to regulating hackers.[151]

[147] *See* discussion *infra* Part IV.B. Moreover, the CFAA does not provide an incentive for anyone to adopt adequate anti-hacking security measures. In fact, network security remains at an shockingly low level and is virtually nonexistent in many companies despite the severity of the hacking threat. A 1996 survey revealed that 58 percent of companies do not have a written policy on how to deal with network intrusions. *See* Gripman, *supra* note 18, at 174 n.21. This lack of security obviously facilitates Internet hacking. According to security expert Clifford Stoll, "The security weaknesses of both systems and networks, particularly the needless vulnerability due to sloppy systems management and administration, result in a surprising success rate for unsophisticated attacks." *Id.* at 177. This is not to say, of course, that allocative inefficiency or cost externalization is in and of itself sufficient justification for cyberspace regulation. *See* discussion *infra* Part V.C.

[148] See Lessig, *Constitution of Code, supra* note 17, for a detailed discussion of Lessig's theory of indirect regulation through code as the most effective means of regulation in cyberspace.

[149] *See id.* at 184.

[150] *See* Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475, 489 (1997).

[151] Some proposals have suggested piecemeal reforms to existing legislation. *See, e.g.*, Clarke, *supra* note 146. Catherine Clarke has proposed a scheme for law enforcement on the Internet that employs the technical expertise of hackers to improve Internet security while promoting self-regulation of the Internet through code solutions such as PGP. Although Clarke recognizes the importance of tailoring law enforcement techniques to match more closely available demographic data on the different subsets of the hacking community, implementing the proposals set forth thereafter are difficult to envision under the current legal regime. For instance, there is no reason to believe that convicted ex-hackers will serve as effective community educators as she suggests, particularly since the social divide between hackers and the rest of the Internet community is imposed by the law itself, irrespective of how such law is enforced. Moreover, as Clarke concedes, "cultural barriers exist between young hackers ... and police officers. Law enforcement officers may be hesitant to seek out the advice of persons who could be their teenage

B. Hacking as Tort: The Internet Service Provider ("ISP") Solution

Some academics have advanced a critique of public law solutions that implies a promising regulatory scheme based in tort negligence theory.[152] These critics maintain that even if jurisdictional issues are solved, "the infrastructure of cyberspace is evolving too rapidly for governments to regulate efficiently."[153] Also, anecdotal evidence suggests that the poor enforcement record of existing criminal law will deter companies from going online. Tom Peltier, the corporate information protection coordinator for Detroit Edison Power Company, predicts that "because of the risk of online crime is so great, there will be a mass exodus of corporate users of the Internet when they realize their vulnerability."[154] Pointing to such deficiencies in current criminal law, proponents of a negligence regime frame their regulatory model on the following: (1) how to provide an incentive for Internet participants to increase security; (2) how to deter hacking; and (3) how to provide a financial remedy to those harmed by hacker intrusions,[155] both as a means to achieve the basic tort end of compensating victims and as a means of promoting online participation.

1. The Decisive Advantages of a Negligence Regime

Tort law does provide a more efficient means of achieving such goals. The primary purposes of tort law are: (1) to deter wrongful conduct; (2) to encourage socially responsible behavior; and (3) to compensate injured parties.[156] Imposing tort liability on larger market actors for losses caused by hacking encourages them to adopt socially valuable security measures (i.e., those whose expected benefits outweigh their costs); imposing tort liability on (non-judgment-proof) hackers deters them from infiltrating

children. The Generation-X young men ... may also be unenthusiastic about assisting law enforcement agencies." Clarke, *supra* note 146, at 233. Clarke must ultimately reduce her claim to the proposition that "existing institutional and procedural measures may force some level of cooperation." *Id.* Re-examination of the laws creating these harmful social norms (i.e., the social divide) suggest that existing institutional and procedural measures should be jettisoned altogether.

[152] *See, e.g.*, Gripman, *supra* note 18.

[153] Gibbons, *supra* note 150, at 509.

[154] Gripman, *supra* note 18, at 170 n.14.

[155] *See id.* at 175. Gripman suggests imposing tort liability on corporations for injuries incurred by third parties as a result of hackers' using the corporations' networks to hack into third parties' computers. As explained below, however, such an approach would raise the cost of online participation for corporations, thereby deterring many companies—particularly small ones—from going online.

[156] *See id.* at 176.

companies because of the threat of monetary sanctions.[157] Tort liability would prompt these market actors to exercise reasonable care in providing network security.[158] Parties injured by a breach of this duty are compensated for their injuries and are restored "to their original condition, insofar as the law can do this."[159] In this way, tort law provides incentives for such market actors to erect security measures that will lower the cost of going online to potential and current Internet participants, thereby allowing the individual expected benefits accruing to corporations from online participation to exceed the expected cost.[160]

Numerous reasons may be cited for the proposition that ISPs should be jointly liable for the tortious hacking activities of those who use their services. As explained above, hackers are generally judgment-proof,[161] so victims of hacking intrusions are usually left without financial remedy, thereby deterring online participation due to the high expected costs stemming from such intrusions.[162] Also, hackers are difficult to detect, much less identify. Third, the jurisdictional problems discussed above render hackers very unattractive defendants. Fourth, many Internet participants also may be judgment-proof due to thin capitalization, given the low

[157] *See id.* Given the difficulties associated with identifying the perpetrators of tortious hacking, the primary goal of the model of tort law proposed here is not the deterrence of socially undesirable activity (i.e., hacking), which tort law is traditionally concerned with, but rather the growth of the Internet as facilitated by greater network security.

[158] *See id.*

[159] *See id.* at 176 (quoting John W. Wade, et al., PROSSER, WADE AND SCHWARTZ'S TORTS 1 (9th ed. 1994)).

[160] Corporations take only individual, not social, costs and benefits into account when they make business decisions. However, online participation has strong positive externalities due to such phenomena as network effects that augment the utility of other users. Thus, the social benefit of an individual corporation's online participation exceeds its individual benefit, and should therefore be encouraged. Hacking imposes a cost on online companies; compensation via tort liability reduces this cost, thereby raising the expected net benefit (benefit less cost) of going online. Thus, the tort system can raise online participation to the socially-optimal level by transferring a portion of the expected cost of going online—i.e., costs imposed by hackers—from corporations to ISPs.

[161] *See* Victoria A. Cundiff, *Trade Secrets and the Internet: A Practical Perspective*, COMPUTER LAW., Aug. 1997 at 6, 14 ("Internet tortfeasors and infringers are likely to include a high percentage of students and others who may not have the resources to satisfy large judgments.").

[162] ISPs may also be judgment proof in some instances. This problem could be solved by requiring ISPs to maintain a minimum level of assets.

barriers to entry on the Internet,[163] so they may be a weak source of compensation for hacking losses if they are the means by which hackers intrude into third parties' computers. Fifth, ISPs are the least cost avoiders, i.e., it is more efficient for ISPs to secure their entire systems than for each online corporation to do so, and ISPs could spread the cost of security among their subscribers. Sixth, absent liability for abuse by their subscribers, ISPs have a financial incentive to tolerate such abuse, in order that they may attract and maintain such subscribers as customers. Seventh, if corporations are forced via tort liability to provide their own security protections, the private expected cost incurred by many individual corporations on the Internet—from invoking security measures as well as from non-recoverable hacking losses—would exceed the expected gain derived from being online, thereby deterring online participation—a socially suboptimal outcome.[164] This analysis is particularly applicable to small companies for whom security costs would make up a large proportion of total costs; while large corporations might be able to afford to hire security experts to constantly update their computer systems, many small companies would not. These small companies would therefore either choose not to go online (because the expected costs would outweigh the expected benefits), or would go online (e.g., if they were judgment-proof) without adequate security and threaten the security of third parties' networks with whom such companies are linked. If, however, ISPs are held liable, such costs of online activity will be transferred to the ISP, thereby increasing the private net gain of going online. Only under this regime would there exist an adequate incentive to adopt security measures without sacrificing online participation and growth.

The negligence rule[165] thus provides an allocation of incentives, deterrence, and remedies as it fulfills three primary objectives: (1) the provision

[163] *See* Ian C. Ballon, *The Law of the Internet: Developing a Framework for Making New Law*, 482 PLI/PAT 9, 20-21 (1997).

[164] One might argue that a corporation's knowing placement of confidential information in a database accessible on the Internet constitutes an effective assumption of risk that would vitiate third party tort liability. However, unlike other risky activities (e.g., skiing), online activities have positive externalities and should be encouraged, given the network effects of online participation and the efficiency of electronic commerce. Tort liability imposed on ISPs largely removes such risk from corporations' net benefit calculus and therefore increases their expected net benefit from online participation, thereby increasing total expected online participation.

[165] Strict liability is another regime that could be possibly erected to deal with the hacking problem. Applying strict liability to ISPs for all damages incurred as a result of hacking has its advantages, given that (1) ISPs are the party in the best position to detect

of an incentive for ISPs to augment their security levels; (2) the deterrence of (non-judgment-proof) hackers from illegally breaking into computer networks because even unintentional harm may make them liable; and (3) the provision to injured corporations or persons a financial remedy for their injuries.[166]

2. *A Critical Evaluation*

Although a tort-based model of regulation is more efficient than the status quo, an examination of the process by which an ISP liability system would seek to regulate hackers suggests several compelling bases for nevertheless rejecting such a scheme. Cost-benefit analysis in such a legal regime would arguably create incentives for Internet participants to deter hacking at the level of Internet technology or architecture. In fact, proponents of a tort-based model of reform criticize inadequate network security[167] and suggest that a minimum security standard for determining the duty of reasonable care would include the adoption of architectural or code solutions[168] such as encryption technology and Internet Protocol next generation ("IPng"), widely touted as "the future version of IP used on the Internet ... [providing] support for authentication, data integrity, and confidentiality."[169] In short, the ISP liability model advocates a shift in the form of behavioral constraint from "direct" regulation of hacking activity to "indirect" regulation through Internet code or architecture.[170]

and eliminate defects in security, (2) ISPs are best able to absorb and spread the risk or cost of injuries through insurance or price increases, and (3) the strict liability rule avoids costly and burdensome requirements of proof. However, the problem with such an approach is that it limits online corporations' incentives to establish security systems of their own that exceed the security levels imposed on ISPs by a due care standard, since corporations would be compensated for all losses regardless of whether the ISP maintained the level of due care or not. Under the negligence rule, this would not be a problem. If a corporation felt that the level of due care was too low for its purposes (say, because it had unusually highly sensitive and valuable information exposed), it would have an incentive to erect higher security levels than those required under due care, since the corporation would not be compensated for losses if the ISP maintained the level of security mandated under the due care standard.

[166] *See* Gripman, *supra* note 18, at 179.

[167] *See id.* at 171-77.

[168] *See id.* at 184-91.

[169] William A. Hodkowski, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 SANTA CLARA COMPUTER & HIGH TECH. L.J. 217, 220 (1997).

[170] *See generally* Lawrence Lessig, *Constitution of Code*, *supra* note 17.

However, such reliance on technology-based solutions is problematic in two important respects. First, although most "live life subject to the constraints of code ... however (and by whomever) these constraints have been set,"[171] hackers do not. To be sure, technological constraints on hackers may have some impact on network security, but the regulatory implication drawn from the history of Internet technology is clear: any such impact will be temporary and inadequate for the purposes of securing electronic commerce.[172] In this instance, the government cannot accomplish indirectly that which technology precludes it from doing directly.

Second, and perhaps more importantly, proponents of the ISP liability scheme have failed to consider the broader policy implications of regulation that has the effect of altering cyberspace code. As Lessig has argued, the architecture of the Internet has the potential to enable and disable behavior with a level of "efficiency" and "compliance" impossible to achieve in real space.[173] The ability to raise such powerful ex ante mechanisms of control, in turn, raises public policy concerns even though imposing ISP liability would permit the market to determine changes in code. The ISP model does empower consumers to approve or reject changes in the code, but any such change would be

> the result of a collection of choices made at an individual level, [with] no collective choice made at a collective level. It is the product of the market. But individual choice might aggregate in a way that individuals collectively do not want. Individual choices are made within a particular architecture; but they may yield an architecture different from what the collective might want.[174]

Particularly since no code-based solution is likely to regulate hackers effectively, the danger posed by making uninformed changes in code premised on the regulation of hackers may indeed be greater for the vast majority of Internet users than any of the current dangers posed by hackers.

[171] *Id.* at 184.

[172] *See* discussion *supra* Part II. The proposition that hackers will evade architectural constraints and therefore pose a threat to electronic commerce is distinct from the claim that hackers point to the general inefficacy of code-based solutions in cyberspace, an argument which is not made here.

[173] *See* Lessig, *Constitution in Cyberspace, supra* note 17, at 869.

[174] Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1411 (1996) [hereinafter *Zones*].

V. A HEURISTIC MODEL FOR REFORM

This critical survey of federal legislation and academic scholarship has attempted not only to expose the critical problems with current models for regulating hackers, but also to deconstruct the current discourse so as to expose the underlying sources of widespread regulatory failure. Such an approach has produced insights that inform the development of a regulatory framework perhaps better equipped to address the threat posed by hackers to electronic commerce. This framework, in turn, should provide the basis for a fruitful discussion of the broader respects in which cyberspace has transformed social dynamics.

A. Consider All Relevant Modalities of Regulation

Although several distinct forms of regulation have emerged in the context of cyberspace, neither current legislation nor the academic literature on hacking has produced a regulatory model that fully comprehends the effects of multiple feedback loops between the several sources of constraint through which social behavior may be regulated, both in real space and in cyberspace. Professor Lessig has labeled these sources of behavioral constraint "the modalities of regulation" and identified the primary modalities as "code" (or architecture/geography), "law," "social norms" and the market.[175] According to Lessig:

> [L]aw, norms and code regulate cyberspace just as law, norms and nature (or what I call "real space code") regulate real space. But there is an important difference between these two regimes. In real space, constraints are changed by changing law; in cyberspace, constraints will be changed by changing code. This will follow because of two features of these two different worlds: First: In real space, it is law that is plastic; in cyberspace, it is code that is plastic. And second: In real space, it is relatively hard to escape the constraints of law; in cyberspace, it is much easier. The effect of both differences will be to shift the locus of regulatory change from law to code. In real space, law is at cen-

[175] *See* Lawrence Lessig, *Constitution of Code*, *supra* note 17. Although Lessig makes explicit reference only to code, law, and social norms, he does not claim "that there are no other constraints. Psychology or the market, for example, are constraints which are related to these three primary constraints in complex ways." *Id.* at 181 n.1. Explicit mention of market forces above is consistent with Lessig's inclusion of the market as a primary constraint in his more recent lectures in his course *The High Tech Entrepreneur*.

> ter stage, and code is an afterthought. In cyberspace, the game is code. Law is a side-show.[176]

Viewed through the lens of Lessig's framework, recent criticisms of the CFAA and even more recent proposals for imposing tort liability on market actors are part of a broader paradigm shift in cyberspace regulation. The CFAA is an attempt to regulate hackers directly through law, and recent scholarship advancing the "indirect regulation" of code through market manipulation in lieu of the CFAA confirms Lessig's theory that "the locus of regulatory change" is changing. Indeed, governmental adaptation of such proposals may not be far behind.[177] And yet, any such "indirect regulation" would be misguided insofar as it attempted to regulate hackers. In Lessig's terms, "Hackers define for themselves a certain anarchy, by devoting themselves to finding the holes in the existing code."[178]

It does not necessarily follow, however, that hackers are impossible to regulate. Lessig's articulation of the primacy of code-altering regulation in cyberspace is a predictive model to facilitate critical analysis of a general trend, not a prescriptive model for how to regulate cyberspace effectively in every instance. In fact, the very process of modality-interplay by which code becomes "the game" suggests that code does not have to be the sole conduit of cyberspace regulation. As Lessig points out, "Architectures don't come in natural kinds."[179] Rather, Internet architectures reflect choices, ones that have been encoded with the values informing those choices—and vice versa. In this respect, code operates not only as an *ex*

[176] *Id.* at 183-84 (footnotes omitted).

[177] *See id.* at 184.

> [G]overnment will shift to a different regulatory technique. Rather than regulating behavior directly, government will regulate indirectly. Rather than making rules that apply to constrain individuals directly, government will make rules that require a change in code, so that code regulates differently. Code will become the government's tool. Law will regulate code, so that code constrains as government wants.

Id.

[178] Lessig, *Zones*, *supra* note 174, at 408 n.18. Lessig's contention that indirect regulation through code is the most effective regulator in cyberspace in no way competes with the contention that such code is a poor means for regulating hackers. Lessig's fear is that cyberspace code will develop in undesirable ways despite the existence of hackers, not as a consequence of eliminating hackers. ("I don't think one need believe hacking impossible to believe it will become less and less significant. People escaped from concentration camps, but that hardly undermines the significance of the evil in concentration camps."). *Id.*

[179] Lessig, *Constitution of Code*, *supra* note 17, at 1411.

ante constraint on socially undesirable behavior, but also by way of its relation to social meaning—as a code of ethics or social norms.[180]

This process in turn exposes a powerful framework for applying the interplay between modalities for prescriptive purposes. In this respect, the strength of Lessig's model is the ease with which modalities may be viewed for their effects on each other. Such interplay points to alternative modalities of regulation for hackers, who cannot be regulated as others in cyberspace are. Admittedly, direct regulation through law (e.g., the CFAA) has been as unsuccessful as code-altering solutions. Nevertheless, examining the effect of law in general, particularly through its interplay with other modalities, may yield answers, whereas exhaustive exploration of the nature of Internet technology has yielded none.

B. Analyze the Political Consequences of Inducing Changes In Code

Equally, if not more important, than which modalities regulate social behavior is the issue of who controls those modalities, whether in real space or cyberspace. In cyberspace, code takes on many of the characteristics that make law effective in real space. With respect to its power to alter social behavior, then, the architecture of the Internet (i.e., the regulation thereof) is more properly the analog of real space law than real space geography or architecture. Yet real space law and cyberspace code also differ in ways that suggest the need for careful scrutiny of code-altering regulation.

The most striking difference between real space law and cyberspace code is that law regulates "through the threat of ex post sanction, while code, in constructing a social world, regulates immediately."[181] However, the most visible instances of code's immense regulatory power take the form of "zoning" technologies,[182] or commercial alterations of code designed to create "a perfect technology of choice"[183] for Internet users (e.g., by making each inhabitant of cyberspace "a market of one"). That government might indirectly regulate the market to induce such changes for its regulatory purposes is less clear to individual users. Yet government can easily transform commercially designed code into "a perfect technology of justice," one that allows policymakers to select a social end, and

[180] Initially, these ethics reflected the values of Internet architects. This is certainly not the case today. *See* discussion *supra* Part IV.B.

[181] Lessig, *Constitution of Code*, *supra* note 17, at 184.

[182] *See* Lessig, *Constitution in Cyberspace*, *supra* note 173, at 901.

[183] Lessig, *Zones*, *supra* note 174, at 1410.

then assure compliance by individuals to that end.[184] It is in this profound sense that code is of great political consequence in and of itself, regardless of whether the government or the market is shaping its development:

> "[S]tructures of [code-altering] regulation entail important value choices. Whether information will be kept private, whether encrypted speech is allowed, whether anonymity is permissible, whether access is open and free—these are policy choices made by default by a structure of code that has developed—unaware at times, and, generally, uncritically of the politics that code entails."[185]

Thus, code in cyberspace possesses regulatory power far beyond the reach of law in real space, and yet alterations of code currently do not undergo any scrutiny resembling the democratic process by which laws are legitimated in real space.[186] Of course, commercial code developers and scholars alike continue to propose changes, such as imposing tort liability on market actors as an "efficient" form of inducing changes in the code to advance the goal of Internet security. Such proponents fail to see the broader issue of choice:

> We could imagine allowing efficiency to rule this new space, by allowing liberties protected by imperfections to fall away; or we could imagine recreating spheres of liberty to replace those created by imperfections in technology. These are our democratic choices, and real choices they are.[187]

That market actors fail to address these choices is acceptable, perhaps inevitable; that policymakers and academics do so is irresponsible.

VI. A PROPOSAL FOR OPTIMAL REGULATION

The preceding heuristic model suggests that state and federal governments should immediately decriminalize all forms of non-malicious hacking. Non-malicious hacking should be defined as obtaining unauthorized access to a protected computer without causing intentional or reckless damage. Successful incidents of unauthorized access should be presumed by law to be non-malicious if the actor makes a good-faith effort

[184] *Id.* at 1408.

[185] Lessig, *Constitution of Code*, *supra* note 17, at 184.

[186] *See* Lessig, *Zones*, *supra* note 174, at 1410.

[187] Lessig, *Constitution in Cyberspace*, *supra* note 173, at 909.

to report the incident to the proprietor of the accessed system immediately upon obtaining access.

All existing state and federal statutes governing computer-related activities, including the Computer Fraud and Abuse Act ("FCAA"), 18 U.S.C. § 1030 (1994), should be amended to reflect this change in policy. In particular, Section 1030(a)(5)[188] of the FCAA should be modified to repeal the third provision criminalizing acts causing negligent damage by outside actors.

A. Advantage One: Promotes Self-Regulation Through Market Forces

The proposed change in legislation enables market actors to draw upon the resources of non-malicious hackers to increase the security level of the Internet and otherwise to mitigate the economic threat posed by malicious hackers. Currently, all hackers are treated by the law and viewed by the public as dangerous criminals who must be stopped at all costs. This overgeneralization discourages companies and law enforcement agents from enlisting the help of hackers in identifying latent security flaws and collecting information on acts of malicious hacking. Moreover, the sweeping criminalization of all hacking activities has bred within the hacking community a strong distrust and resentment of computer security professionals and government agents.[189]

A clear legal distinction between malicious and non-malicious hacking will revive the positive and self-regulating norms (i.e. the "hacker ethic") within the hacking community and promote market-based initiatives aimed at enlisting the help of non-malicious hackers.[190] Existing literature indicates that many within the hacking community would be willing to cooperate with companies and government agencies if monetary rewards and public recognition were offered for their skills and knowledge.[191] Such market-based initiatives may include the following:[192]

[188] *See* discussion *supra* Part IV.A.

[189] Hackers felt that system managers treat them like enemies and criminals, rather than as potential helpers in their task of making their systems secure. *See* Dorothy E. Denning, *Concerning Hackers Who Break into Computer Systems* (visited Apr. 24, 1999) <http://www.cpsr.org/cpsr/privacy/crime/denning.hackers.html>.

[190] "Frank Drake," an editor of the now defunct cyberpunk W.O.R.M., suggested in 1990 that making a legal distinction between malicious and non-malicious hacking would lead to a "kinder, gentler" relationship between hackers and computer security people. *See id.* at 16.

[191] According to Dorothy Denning in her 1990 survey, several hackers said that they would like to be able to pursue their activities legally and for income: "Hackers say

1) Companies can offer monetary rewards and public recognition for hackers who voluntarily report their successful break-ins and give suggestions for correcting latent security flaws.[193]

2) Companies and government agencies can offer monetary rewards for hackers who provide useful information about acts of malicious hacking.[194]

3) Companies can hire hackers as security consultants or members of "tiger teams."[195]

By tapping into the expertise and knowledge base of hackers, who are often in the best position to identify security holes, companies can receive invaluable assistance in detecting and correcting latent security flaws before they are exploited for malicious purposes. In addition, the public will have a more positive view of hackers in general, increasing consumer trust

they want to help system managers make their systems more secure. They would like managers to recognize and use their knowledge about design flaws and the outsider threat problem." Also, the hackers felt that it would help if system managers and the operators of phone companies and switches could cooperate in tracing a hacker without bringing in law enforcement authorities. *See id.* at 15.

[192] As the following footnotes will illustrate, some companies are turning to market-based initiatives already. With the decriminalization of non-malicious hackers, more and more companies will feel comfortable with trusting hackers and relying on them for their expertise.

[193] For example, consider Crypto-Logic. This company has developed a new type of encryption software for sending secure e-mail messages. It is currently staging a contest in which it challenges hackers to decode an encrypted message sitting on its Web site. *See Ultimate Privacy* (visited Feb. 8, 1999) <http://www.ultimateprivacy.com>.

[194] For instance, in the famous case of Rome Laboratory Attacks, the Government was able to identify one of the hackers through an intelligent network of informants after failed attempts to trace back the origin of attack using phone taps and packet tracing tools. *See* Christy, *supra* note 79, at 59-60.

[195] Although the information security community is in principle reluctant to hire hackers to work for them, some will admit to hiring, or at least consulting with, ex-hackers. Among them are the National Computer Crime Information Center, part of the Federal Bureau of Investigation, and the operator of the system that is hacking's Holy Grail: the National Security Agency ("NSA"). A highly regarded Information Services security consultant confirmed that both institutions, along with several major defense contractors, have occasionally used hackers at least as informants in the past.

In another instance, Price Waterhouse's elite group of computer experts—the Tiger Team—spends its waking hours breaking into their client's security systems. The team, part of the firm's Enterprise Security Solutions Practice, simulates "enemy" break-ins to help clients defend themselves against computer hackers.

in the safety of conducting commercial transactions online.[196] Finally, government agencies can make better use of law enforcement resources by focusing on deterring and prosecuting malicious hackers.

B. Advantage Two: Facilitates Democratization of Architectural Developments

In addition to mitigating the economic threat posed by malicious hackers, the proposal also facilitates an informed discussion of the political nature of code or the "governance" issue implicit in code-altering regulation. As mentioned above, changes in code are currently implemented without any formal institution or process for review, recommendation, or legitimization. Governmental and commercial code developers, whose interests are often aligned in this respect, thus possess potentially unchecked discretion in their development of Internet architecture. However, the decriminalization of non-malicious hacking presents an opportunity to place a check on corporate and governmental interests and initiate a scheme for the democratization of Internet code development.

Just as the free flow of market forces in a proposed regime of decriminalization would forge the necessary "trust" between consumers and retailers to promote the growth of electronic commerce, decriminalization of non-malicious hacking also bridges the cultural gap between hackers and the vast majority of Internet users. Without the force of law to create a widespread societal norm against the activities of non-malicious hacking, both hackers and ordinary Internet users are likely to find their interests aligned. Should a group of hackers organize for the purposes of promoting open discussion of the policy implications of adopting various changes in code, there is no reason to believe consumers would hesitate to pay attention, particularly where the advice of hackers was contrary to that offered by corporate and governmental forces. In this respect, hackers could become at the very least a loosely organized coalition of consumer advocates who could provide a forum, however informal, for the discussion and implementation of code at a collective level. In fact, many existing hacker organizations could fulfill such a function; nor does one organization have to operate in such a capacity to the exclusion of others.[197] Consumers may ultimately make the same "choice" they would have made without the quasi-institutional role played by hackers. But under the presence of their

[196] *See* discussion *supra* Part I.

[197] In fact, many hackers are members of consumer advocate and civil liberties organizations such as Electronic Frontier Foundation ("EFF"), the League for Programming Freedom ("LPF"), and SotMesc.

watchful eyes, the process of implementing architectural changes in cyberspace will more likely reflect the democratic principles that govern this nation in real space.

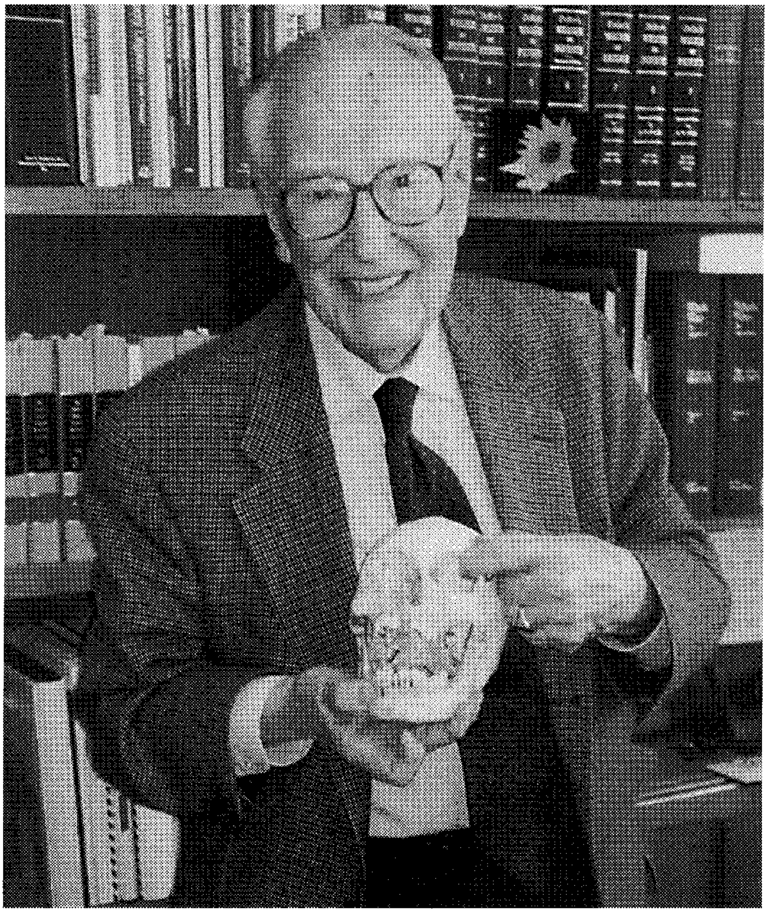

Photo Courtesy of Janice Mueller

JUDGE GILES S. RICH

1904–1999

IN MEMORIAM
JUDGE GILES S. RICH

Judge Giles S. Rich, considered by many scholars to be the father of modern patent law, passed away on June 9, 1999. Judge Rich was a historical and active force in shaping this country's intellectual property system, both in the legislature and on the bench. A member of the Drafting Committee of the Coordinating Committee of the National Council of Patent Law Associations, he co-authored the 1952 Patent Act, which remains the basis of the current patent law.

Judge Rich was also active in reform from the bench. During his lifetime, Judge Rich had the distinction of being the oldest active federal judge in the history of the United States, serving on the United States Court of Customs and Patent Appeals from 1956 to 1982 and then on the Federal Circuit from its inception in 1982 until his death this past year. He was the author of many major panel and en banc decisions, including *In re Alappat* and *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, two decisions primarily responsible for opening up the patent system to software and Internet business methods.

The Berkeley Technology Law Journal is pleased to present the following memorials: one from Judge Paul R. Michel, a long-time Federal Circuit colleague of Judge Rich, and two from former law clerks of Judge Rich, Neil A. Smith and Janice M. Mueller. As patent law moves forward into the 21st century, the legacy of Judge Rich will move with us, guided by his efforts during over fifty-plus years of legislative and judicial scrutiny.