Research Publication No. 2004-07
4/2004

Computer Hacking: Making the Case for a National Reporting Requirement

(Working Paper)

Jason V. Chang

JEL Classification: K20, K42, O33, O38

COMPUTER HACKING: MAKING THE CASE FOR A NATIONAL REPORTING REQUIREMENT

Jason V. Chang*

ABSTRACT

The incidences of computer hacking have increased dramatically over the years. Indeed, the current federal laws, including the Computer Fraud and Abuse Act, have done very little to deter potential computer hackers. This article finds that only a small percentage of computer hackers are ever caught and prosecuted. The biggest problem is that most victimized companies regrettably choose to hide the problem from the public due in part to negative publicity concerns. As a result, this article proposes that a mandatory reporting requirement imposed by Congress, which forces companies to disclose intrusions, will be salient to the problem of computer hacking in several regards. First, individuals who are affected by the intrusions will receive advance warning that their personal information was stolen by hackers. This will allow these affected individuals to take precautions in securing their identities. Secondly, the mandatory reportings will assist law enforcement in investigating and prosecuting a greater percentage of computer hackers. As more prosecutions of computer hackers are publicized, this should reduce the future incidences of computer hackings. Moreover, on July 1, 2003, California became the first state to enact a reporting requirement for computer hackings. This could provoke other states to pass similar reporting requirements. Because computer hacking is a national (and international) problem, Congress needs to consider enacting a reporting requirement before an untenable piecemeal state-by-state solution occurs.

Keywords: computer, hacking, hacker, intrusion, software security, cybercrime, identity theft

---

* J.D. Candidate, 2004, Harvard Law School; B.S. Electrical Engineering, 2001, Georgia Institute of Technology. I wish to acknowledge the support and guidance of Professor John Palfrey of the Berkman Center for Internet & Society at Harvard Law School.

COMPUTER HACKING: MAKING THE CASE FOR A NATIONAL REPORTING REQUIREMENT

Jason V. Chang

Table of Contents

COMPUTER HACKING: MAKING THE CASE FOR A NATIONAL REPORTING REQUIREMENT

I. INTRODUCTION

Computer hackings have grown at an alarming rate and the effects are widespread and costly. Each year hackers steal millions of dollars worth of proprietary information from companies and organizations. A survey by the Computer Security Institute indicated that for the year 2002, theft of proprietary information by hackers cost companies and organizations over $70 million.[1] The cost to insure against these hackers is staggering— the market for hacker insurance is expected to increase from $100 million in 2003 to $900 million by 2005.[2] In addition, hackers can cause severe damage to computer systems by altering or deleting data files and disabling software.

In addition to proprietary information, hackers also steal personal information from these organizations and corporations including their customers' credit card numbers, account numbers, and social security numbers. For example, in 2000, hackers stole 55,000 credit card numbers from creditcards.com and 300,000 credit card numbers from CDUniverse.com.[3] The theft of personal information such as credit card numbers raises serious concerns relating to both identity theft and privacy.

---

[1] COMPUTER SECURITY INSTITUTE, CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 20 (2003), *available at* http://www.security.fsu.edu/docs/FBI2003.pdf. The respondents to this survey included 17% from high-tech companies, 15% from the financial sector, and 15% from government agencies. *Id.* at 2. Further, more than half of the organizations taking part in the survey had more than 1,000 employees while approximately 28% had more than 10,000 employees. *Id.* at 3.

[2] Jon Swartz, *Firms' hacking-related insurance costs soar*, USA TODAY, Feb. 9, 2003, *available at* http://www.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm. Worse yet, many general-liability policies have now eliminated the hacking-related portion of the coverage because of the number of claims filed within the last two years. *See id.* Thus, companies are being forced to choose between paying $5,000 to $30,000 a year for $1 million in stand-alone hacking coverage or not being insured against hackers at all. *See id.*

[3] Associated Press, *Extortionist Puts Credit Card Data on Web*, CBSNEWS.COM, Dec. 14, 2000, *at* http://www.cbsnews.com/stories/2000/12/14/archive/technology/main257200.shtml. In the creditcard.com incident, the hackers who stole the credit card numbers demanded $100,000 ransom. *Id.* When the extortion payment was not made, the hackers retaliated by posting the stolen credit card numbers on a public webpage. *Id.*

Even more disconcerting than the theft of proprietary and personal information is the fact that most companies and organizations are not reporting hacking incidents to law enforcement.[4] According to surveys from 1999 to 2003, only about 30% of hacking intrusions are ever reported.[5] Further, Internet technology presents high hurdles for law enforcement to trace the hacking intrusions back to the hacker. This means that the vast majority of hackers have very little chance of being caught and prosecuted.

Because tackling the area of computer hacking requires an understanding of the technical issues involved, an Appendix is included, which will introduce the numerous tools that hackers use to accomplish their intrusive hacking attacks. Knowledge of this is necessary to appreciate the applicability of the current laws to these tools. Some readers may find it helpful to reference the Appendix before beginning Part II of the paper, which covers the scope of several federal laws commonly used against hackers.

Part III of the paper will evaluate the technical, societal, and legal failures that result in hackers not being caught or prosecuted. Against this background, Part IV of this paper proposes a national reporting requirement to tackle the problem of computer intrusions with respect to the computer networks of organizations and corporations. The national reporting requirement framework will propose one set of reporting requirements when privacy is at stake and another set of reporting requirements aimed at deterring property damage by hackers. Part V will then illustrate how such a framework for a national reporting requirement could help bridge the current technical, societal, and legal shortcomings discussed in Part III and thus reduce the number of computer intrusions in business and organizational computer networks as a whole. Finally, Part VI anticipates and responds to several major arguments against a reporting requirement.

While there is also the problem of hacking into personal computers, this paper does not intend to address that problem. However, as will be discussed in Part III of the paper, many hackers take control of personal computers for the purpose of launching hacking attacks on corporate computers. Accordingly, it is conceivable that reducing the number of corporate and organizational hacking intrusions will result in a proportionate decline in the number of personal computers attacked.

---

[4] *See* COMPUTER SECURITY INSTITUTE, *supra* note 1, at 17.

[5] *See id.*

II. CURRENT FEDERAL LAWS AGAINST COMPUTER HACKING

This section covers the federal approaches applicable to computer crimes that may be relevant to the problem of computer hacking. The author realizes that some states may have their own laws tailored toward various computer crimes, like the variations of the proposed Federal Computer Systems Protection Act.[6] Further, many practitioners have been creative in applying common law approaches along with other state laws (such as trade secrets law) to the area of cybercrime.[7] However, because of the numerous jurisdictional limitations of state laws[8] and because computer hacking is not limited by state borders, this paper focuses on the two main federal laws relevant to computer hacking—the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.

A. Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 ("ECPA") was Congress's patchwork attempt to fit new crimes into the existing laws.[9] Title I of the ECPA amended the Federal Wiretap Act, 18 U.S.C. §§ 2510 et al., to include not only wire or oral communications, but also electronic communications.[10] Title II of the ECPA created the Stored Communications Act.[11] The coverage of both the Federal Wiretap Act and the Stored Communications Act is described below.

1. Federal Wiretap Act, 18 U.S.C. §§ 2510 et al.

Title I of the ECPA amended the Federal Wiretap Act to cover not only wire and oral communications, but also electronic communications.[12] The current

---

[6] See, e.g., the Georgia Computer Systems Protection Act at O.C.G.A. § 16-9-90 (2002).

[7] As an example, in *Ebay, Inc. v. Bidder's Edge, Inc.*, Bidder's Edge, an auction aggregation site, used an unauthorized robot to collect auction listings from eBay's site. *See* 100 F. Supp. 2d 1058, 1062-63 (N.D. Cal. 2000). Based on eBay's claim that Bidder's Edge's activities constituted trespass to chattels, the court granted a preliminary injunction against Bidder's Edge's use of robots to collect information from eBay's site. *See id.* at 1072.

[8] The author also realizes that computer hackings often originate from foreign countries—China is one such example. *See, e.g.*, Daniel M. Creekman, Comment, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 Am. U. Int'l Rev. 641, 675 (2002) (stating that the "lack of an agreement with China, whether a bilateral extradition treaty or a multilateral international agreement, prevents an action to seek legal redress from a lone Chinese citizen-hacker, regardless of the importance of the victimized computer system."). This raises international jurisdictional issues that, while important in certain circumstances, are beyond the scope of this undertaking.

[9] *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (stating that the "existing statutory framework is ill-suited to address modern forms of communications").

[10] *See id.* (reviewing S. Rep. No. 99-541, at 3 (1986)).

[11] *See id.*

[12] *See id.* (stating that the Wiretap Act was amended to "address[] the interception of . . . electronic communications"). Congress gave "electronic communications" an expansive definition. An electronic communication is "any transfer of signs, signals, writing, images,

version of the Wiretap Act prohibits intentionally intercepting (or endeavoring to intercept) any wire, oral, or electronic communication.[13] In addition, the Wiretap Act punishes disclosing or using the contents of any wire, oral, or electronic communication with knowledge that the information was obtained through the prohibited interception of a wire, oral, or electronic communication.[14]

A large blow to the effectiveness of the Wiretap Act against computer hackers was the judicially-interpreted requirement of an "acquisition contemporaneous with transmission."[15] This means that hackers that obtain information through their intrusive attacks do not violate the Wiretap Act unless they capture the information while it is being transmitted from one computer to another.[16] Presumably, the Wiretap Act applies to hackers who install network packet sniffers ("sniffers") to intercept real-time communications. This is because sniffers capture network data packets while they are in transmission, and thus the acquisitions of the data packets by the sniffers are contemporaneous with their transmission from one computer to another. Unfortunately, the case law is absolutely devoid of examples of prosecutions in such cases.

---

sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include-- (A) any wire or oral communication . . . ." 18 U.S.C. § 2510(12).

[13] *See* 18 U.S.C. § 2511(1)(a) (prohibiting "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication"). A violation of 18 U.S.C. § 2511(1) may result in a fine or imprisonment for not more than five years, or both. *See* 18 U.S.C. § 2511(4). Notwithstanding possible criminal punishment, the Wiretap Act generally authorizes recovery of civil damages. *See* 18 U.S.C. § 2520(a) (stating that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter . . . may in a civil action recover from the person or entity . . . which engaged in that violation such relief as may be appropriate").

[14] *See* 18 U.S.C. § 2511(1)(c) (prohibiting "intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection"); 18 U.S.C. § 2511(1)(d) (prohibiting "intentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection").

[15] The word "intercept" as used in the Wiretap Act has been interpreted to mean an "acquisition contemporaneous with transmission." *See U.S. v. Steiger*, 318 F.3d 1039, 1048 (11th Cir. 2003), *cert. denied*, 123 S. Ct. 2120 (2003). The Fifth, Ninth, and Eleventh Circuit have all required such an interpretation of the word "intercept." *See Theofel v. Farey-Jones*, 341 F.3d 978, 986 (9th Cir. 2003); *Steiger*, 318 F.3d at 1048; *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878-89 (9th Cir. 2002) (withdrawing contrary panel opinion at 236 F.3d 1035 (9th Cir. 2001)); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 460 (5th Cir. 1994).

[16] *See id.*

2. Stored Communications Act, 18 U.S.C. §§ 2701 et al.

The Stored Communications Act ("SCA") was created by Title II of the ECPA.[17] Title 18 U.S.C. § 2701(a) of the SCA punishes "whoever—(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to wire or electronic communication while it is in electronic storage in such system . . . ."[18]

The SCA only applies if the target of the attack is an "electronic communication service."[19] An electronic communication service is defined as "any service which provides to users thereof the ability to send or receive wire communications."[20] An email server would clearly fit this definition as would Internet Service Providers.[21] However, courts have determined that personal computers are not electronic communication services within the purview of the SCA.[22] Unfortunately, this means that if the hacker breaks into a computer that is not a qualifying electronic communication service, then the SCA does not apply. This limitation has curbed the effectiveness of the SCA against computer hackers.

B. Computer Fraud and Abuse Act (18 U.S.C. § 1030)

1. Overview

Title 18 U.S.C. § 1030, otherwise known as the Computer Fraud and Abuse Act ("CFAA"), is currently the most targeted and comprehensive federal law directed towards computer-related criminal conduct. The premise behind the enactment of the CFAA was to "deter and punish those who intentionally access

---

[17] See *supra* note 11.

[18] 18 U.S.C. § 2701(a). Violations of the SCA may result both fines and imprisonment (if offense was for commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortuous act, then imprisonment for not more than 5 years for first offenses or not more than 10 years for a subsequent offense). *See* 18 U.S.C. § 2701(b). In addition, in certain circumstances, civil causes of action are authorized. *See* 18 U.S.C. § 2707 (stating that "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of the [Stored Communications Act] in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a devil action, recover from the person or entity . . . which engaged in that violation such relief as may be appropriate").

[19] *See* 18 U.S.C. § 2701(a).

[20] 18 U.S.C. § 2510(15) incorporated by 18 U.S.C. § 2711(1) (stating that "the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section").

[21] See *Theofel*, 341 F.3d at 984-85 (finding that email stored at an Internet Service Provider is within the scope of the SCA); *Steiger*, 318 F.3d at 1049 (noting that "the SCA may apply to the extent the source accessed and retrieved any information stored with [the] Internet service provider").

[22] *See Steiger*, 318 F.3d at 1049 (stating that ordinarily a personal computer does not meet the requirements of an electronic communication service).

computer files and systems without authority and cause harm."[23] The CFAA contains seven substantive provisions. Each of the seven provisions will be introduced according to its statutory order.

First, section 1030(a)(1) prohibits knowingly accessing a computer without authorization or exceeding authorization, thereby obtaining and subsequently transferring classified government information.[24]

Next, section 1030(a)(2), which is highly applicable to intrusive computer hackers, proscribes intentionally accessing a computer without authorization or exceeding authorization and obtaining information from a financial institution, any department or agency of the United States, or any protected computer[25] involved in interstate or foreign communication.[26]

Section 1030(a)(3) makes it a crime to intentionally, without authorization, access a nonpublic computer of a department or agency of the United States.[27]

Section 1030(a)(4) prohibits knowingly and with intent to defraud, accessing a protected computer without authorization (or in excess of authorization) and thereby obtaining anything of value greater than $5,000 within any 1-year period.[28]

Section 1030(a)(5)(A) is the main anti-hacking provision and contains three types of offenses. Subsection 1030(a)(5)(A)(i) proscribes knowingly causing the transmission of a program, information, code, or command, and as a result, intentionally causing damage without authorization to a protected computer.[29] Prior to the amendment by the USA PATRIOT Act of 2001 ("PATRIOT Act"), the CFAA defined damage as "any impairment to the integrity or availability of data, a program, a system, or information that-- (A) causes loss

---

[23] *Doe v. Dartmouth-Hitchcock Med. Ctr.*, 2001 DNH 132 (D. N.H. 2001) (reviewing S. Rep. no. 104-357 (1996), pts. II, III).

[24] *See* 18 U.S.C. § 1030(a)(1).

[25] The definition of a "protected computer" is very inclusive. "[T]he term 'protected computer' means a computer—(A) 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 that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commence or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2). It is not difficult to imagine that most computers connected to the Internet are involved in interstate commerce. Indeed, over 50 million American computers that are connected to the Internet can be classified as "protected computers." *See* Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 Geo. L.J. 171, 172 (2000).

[26] *See* 18 U.S.C. § 1030(a)(2).

[27] *See id.* § 1030(a)(3).

[28] *See id.* § 1030(a)(4).

[29] *See id.* § 1030(a)(5)(A)(i).

aggregating at least $5,000 in value during any 1-year period to one or more individuals."[30] Following the amendments by the PATRIOT Act, the CFAA eliminated the $5,000 jurisdictional requirement in criminal cases and damage is now broadly defined as "any impairment to the integrity or availability of data, a program, a system or information."[31] While subsection 1030(a)(5)(A)(i) focuses more on intentionally causing damage (without regard to authorization), subsection 1030(a)(5)(A)(ii) focuses on intentionally accessing a protected computer without authorization.[32] Subsection 1030(a)(5)(A)(ii) proscribes intentionally accessing a protected computer without authorization and thereby recklessly causing damage. Finally, subsection 1030(a)(5)(A)(iii) proscribes intentionally accessing a protected computer without authorization and thereby causing damage.[33]

Section 1030(a)(6) prohibits the trafficking of passwords through which a computer may be accessed without authorization.[34]

Finally, section 1030(a)(7) makes it a crime for someone to transmit a communication in interstate or foreign commerce that threatens damage to a protected computer for the intent of extorting money or other things of value.[35]

2. The CFAA as applied to intrusive computer hackers

Of the seven prohibitions listed in the CFAA, two of these are particularly important to the prosecution of intrusive computer hackers—namely sections 1030(a)(2) and 1030(a)(5).

As stated above, section 1030(a)(2) applies to a hacker who intentionally accesses a computer without authorization or exceeds authorization and obtains information from a protected computer involved in interstate communication.[36] For example, a hacker may violate section 1030(a)(2) by obtaining unauthorized access to an Internet computer through war dialing or through a Trojan horse[37] and then obtaining sensitive personal information such as social security numbers or credit card numbers from the hijacked computer.

In addition, section 1030(a)(5) applies to a hacker that causes damage to a protected computer. If the damage was caused by the transmission of a program, information, code, or command, then subsection 1030(a)(5)(A)(i) is applicable.[38]

---

[30] *Id.* § 1030(e)(8) (1994 & Supp. IV 1998).
[31] *Id.* § 1030(e)(8).
[32] *See id.* § 1030(a)(5)(A)(ii).
[33] *See id.* § 1030(a)(5)(A)(iii).
[34] *See id.* § 1030(a)(6).
[35] *See id.* § 1030(a)(7).
[36] *See supra* note 26 and accompanying text.
[37] See parts C and E in the Appendix for discussions regarding war dialing and Trojan horses.
[38] See 18 U.S.C. § 1030(a)(5)(A)(i).

Therefore, a Trojan horse (and also other viruses and worms) would be such a "program, information, code, or command" invoking the prohibition of subsection 1030(a)(5)(A)(i). Alternatively, if the damage was caused from unauthorized access, then either subsection 1030(a)(5)(A)(ii) or subsection 1030(a)(5)(A)(iii) would apply.[39] Once the hacker obtains access to the computer, either through a Trojan horse or other unauthorized means such as war dialing or buffer overflow attacks,[40] damage can result from altering or deleting existing files or otherwise impairing "the integrity or availability of data, a program, a system or information."[41]

A violation of any of the seven prohibitions of the CFAA can result in criminal sanctions.[42] However, for civil damages, a violation of the CFAA must include at least one of the five factors listed in section 1030(a)(5)(B).[43] The most relevant of these five factors is the requirement of a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[44] This often presents a hurdle for victims who sometimes find it difficult to prove a loss of $5,000 in value.

III. FAILURES PREVENTING REDUCTION IN INTRUSIVE COMPUTER HACKING

As described in the Appendix, intrusive computer hackers have a variety of tools available for them to breach the security of computer systems. Indeed, many hackers themselves freely share the tools and methods they have developed or acquired.[45] Hackers, in addition, also utilize several additional tools to help conceal their tracks. It is estimated that at most, only ten percent of successful intrusions are ever detected.[46] Even if an intrusion is successfully detected, a rough estimate is that only between one and seventeen percent of these detected intrusions are ever reported to law enforcement.[47] Finally, of the successful intrusions reported to law enforcement, only a small percentage of these cases are

---

[39] *See id.* § 1030(a)(5)(A)(ii) and (iii).

[40] See part D of the Appendix for a discussion regarding buffer overflow attacks.

[41] 18 U.S.C. § 1030(e)(8).

[42] See *id.* § 1030(c) (describing the punishments for violations of § 1030(a) or § 1030(b)).

[43] *See* 18 U.S.C. § 1030(g) (stating that "[a] civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)").

[44] *See* 18 U.S.C. § 1030(a)(5)(B)(i).

[45] There is actually a hacker code of ethics that is generally followed by some in the hacking underground. Among these rules are to "always be willing to freely share and teach your gained knowledge and methods" and to "respect knowledge and freedom of information." *See* Brian Matheis, *Hacker Ethics: Part II*, Nov. 25, 2003, *at* http://www.geocities.com/brian_matheis/hacker_ethics/part2.html (last visited Mar. 26, 2004).

[46] *See* Jamila Harrison Vincent, *Cyberterrorism*, *at* http://gsulaw.gsu.edu/lawand/papers/fa01/harrisonvincent/ (last visited Mar. 26, 2004).

[47] *See id.* However, these numbers are not beyond dispute. Surveys by the Computer Security Institute have found that approximately 30% of its respondents have reported their incidents to law enforcement. *See supra* note 5.

successfully prosecuted.[48] A 1999 study by David Banisar ("Banisar"), who was involved with the Electronic Privacy Information Center, found that in 1998, of the 419 cases of computer fraud referred to federal prosecutors, only 83 cases were prosecuted.[49] Moreover, of these 83 cases, only 57 cases reached disposition— with 47 ending in convictions and the remaining 10 ending unsuccessfully for prosecutors.[50] Surprisingly, the average sentence was only five months and half of the defendants who were convicted received no jail time at all.[51] Against this background, this paper will now discuss the technical, societal, and legal failures that contribute to the unsuccessful prosecution of computer hackers.

A. Technical Failures

The federal laws discussed in Part II— the ECPA and CFAA— are only effective against computer hackers if they are apprehended. In this section, the various tools and methods that computer hackers use to conceal their activities and evade law enforcement will be discussed.

1. Tracing difficulties

All computers communicating on the Internet are assigned an Internet Protocol ("IP") address.[52] This IP address uniquely identifies a computer and is similar to how a street address identifies a particular home.[53] Because malicious hackers want to make it more difficult for law enforcement to find them, they will oftentimes mask their activities. These hackers may utilize intermediate computers, delete log files, or utilize anonymous proxy servers as described below.

a. Utilization of intermediate computers

If a hacker has compromised a computer, the hacker may utilize this compromised computer as a "launching pad" for attacks on other computers.[54] By launching their attacks from intermediate computers, computer hackers can make it more difficult for law enforcement to trace their attacks.

---

[48] *See* Kevin Poulsen, *Study: Cybercime cases up 43 percent*, ZDNET NEWS, Aug. 4, 1999, *at* http://zdnet.com.com/2100-11-515355.html?legacy=zdnn.

[49] *See id.*

[50] *See id.*

[51] *See id.*

[52] For a short and simple introduction on IP addresses, see Russ Smith, *The IP Address: Your Internet Identity*, CONSUMER.NET, Mar. 29, 1998, *at* http://consumer.net/IPpaper.asp.

[53] *See id.*

[54] *See* VERISIGN, INC., HACKING AND NETWORK DEFENSE 10 (2002), *available at* http://www.securitytechnet.com/resource/rsc-center/vendor-wp/verisign/hacking.pdf (last visited Mar. 26, 2004) (stating that "[r]ather than use his or her own system to launch an attack, the hacker decides to use [the compromised computer]").

For example, the hacker can utilize compromised Computer A to connect to compromised Computer B, which is then used to attack the target computer. In this example, this means that law enforcement must penetrate two additional layers of anonymity (Computers A and B) before discovering the hacker's computer.[55]

As a first step, law enforcement will investigate the log file of the target computer (and its Internet Service Provide ("ISP")). The log file of the target computer (or its ISP) will indicate the IP address of Computer B. Investigators must then travel to Computer B and obtain its log file. The log file of Computer B (or its ISP) may point to the IP address of Computer A. Investigators must then go to Computer A (or its ISP) to obtain its log file, and, if lucky enough, will obtain the IP address of the hacker's own personal computer. Further, law enforcement will likely have to obtain subpoenas and court orders to obtain access to Computers A and B (or the ISP's of Computers A and B).[56]

b. Problems with log files

In the above example, tracking a computer hacker from the target computer to the hacker's personal computer requires that the log files at intermediate Computers A and B (or their respective ISP's) be intact. Several problems may occur with respect to these log files: (1) some victim computers do not keep log files; (2) the hackers sometimes alter or delete log files upon gaining entry into the compromised computer; (3) or the ISP's log files have been routinely cleared before law enforcement sends the retention letter to the ISP.[57] If any of these three events occur, then the chain from the target computer to the hacker has been broken and law enforcement will have to turn to traditional investigative techniques.[58] Unfortunately, these traditional investigative techniques are oftentimes inadequate to identify the hacker.[59]

2. Existence of anonymous proxy servers

Most users access the Internet through legitimate proxy servers provided by reputable companies such as AOL or Earthlink. These legitimate proxy servers keep logs of the activities of their users. However, the existence of

---

[55] Sometimes these compromised computers are misconfigured proxy servers. When a hacker connects to target computer through a proxy server, the proxy's IP address, rather than the hacker's IP address, is recorded on the target computer's logs. *See* Chris Prosise and Saumil Shah, *Hackers' Tricks to Avoid Detection*, SECINF.NET NETWORK SECURITY LIBRARY, Oct. 16, 2002, *at* http://secinf.net/info/misc/tricks.html.

[56] *See* DANIEL A. MORRIS, US ATTORNEYS' BULLETIN: TRACKING A COMPUTER HACKER (2001), *at* http://www.cybercrime.gov/usamay2001_2.htm (last updated July 10, 2001) (stating that "[s]ubpoenas and court orders to each bounce point may be necessary to identify the hacker").

[57] *See id.* (discussing that a victim that has no record of the IP address of the attacking computer may leave investigators to traditional investigation techniques that may be inadequate).

[58] *See id.*

[59] *See id.*

anonymous proxy servers[60] make it much more difficult for law enforcement to find hackers because anonymous proxy servers intentionally do not keep *any* log files at all. Utilizing the same example above, this means that at best, the log file of Computer A (or its ISP) will give the IP address of the anonymous proxy server, which is insufficient to uniquely identify a hacker out of the perhaps thousands of people who connect to the Internet through the anonymous proxy server.

B. Societal Failures

Sometimes hackers are never caught because companies never alert law enforcement to the hacker's intrusive activity. At other times, even cases that are referred to law enforcement and prosecutors (assuming the hacker-defendant can be identified) result in relatively low prosecution rates. This subsection explains why companies fail to report and why prosecutors fail to prosecute.

1. Failure to report

The 2003 CSI/FBI Computer Crime and Security Survey ("2003 CSI/FBI Survey") found that in 2002, only thirty percent of the companies and organizations surveyed reported computer intrusions to law enforcement.[61] Some of their reasons for not reporting include competitive advantage concerns, negative publicity concerns, and lack of knowledge that anything could be done.[62]

a. Competitive advantage concerns

When asked why their organization did not report intrusions to law enforcement, sixty-one percent of the respondents to the 2003 CSI/FBI Survey indicated that they feared that their competitors would use this information advantageously.[63] For example, competitors may advertise that they are not subject to the same security loopholes as the hacked company. These competitors may then be able to divert customers from the hacked company.

In addition, once federal law enforcement gets involved, they oftentimes move at a painfully slow rate.[64] Further, federal agents may freeze, and thus make unavailable for an extended period of time, the resources that were

---

[60] For an example of an anonymous proxy server, see http://www.multiproxy.org or http://www.anonymizer.com.

[61] *See* COMPUTER SECURITY INSTITUTE, *supra* note 1, at 18. Previously, the 2002, 2001, 2000, and 1999 surveys indicated reporting rates of 34%, 36%, 25%, and 32% respectively. *See id.*

[62] *See id.* at 19.

[63] *See id.* (only 45% of the total respondents answered this question).

[64] *See* Thomas C. Greene, *Is prosecuting hackers worth the bother?*, THE REGISTER, Aug. 21, 2001, *at* http://www.theregister.co.uk/content/6/21184.html (discussing how deliberately the Feds conduct their investigation).

compromised by the hacker.[65] The company may also have to expend additional resources in providing Federal agents with information about its business, in attending interviews, and in making employees available as witnesses for trial.[66] Thus, many companies are concerned that if a substantial amount of their resources are diverted towards the investigation, their competitors may gain the competitive advantage and manage to outmaneuver them in the marketplace.

Perhaps a good example of this occurred after hackers penetrated the systems of Egghead.com[67] ("Egghead") in December 2000. Immediately after the intrusion, Egghead spent substantial resources hiring the "world's leading computer security experts" to investigate the extent of the security breach and to analyze the current security measures.[68] While Egghead had expected to learn the extent of the security breach within 5 days, the investigation required 20 days, perhaps because a full forensics investigation had to be done.[69] Further, law enforcement was simultaneously pursuing a criminal investigation.[70] Shortly after the hacking incident, Egghead's business took a turn for the worse.[71] Egghead blamed the shortfall in expected sales in the following fourth quarter (February 2001) on "softening of consumer demand for personal computers and related technology products."[72] Perhaps Egghead, consumed with dealing with the hacking incident, was not able to recognize and respond quickly enough to the intense competition within the computer and software marketplace. Egghead's inability to respond quickly enough to the marketplace was permanently marked on October 15, 2001.[73] On that day, Egghead filed for bankruptcy, citing an unexpected sharp drop in sales during the preceding several weeks.[74] Egghead's fate was sealed when Amazon.com successfully purchased the assets of Egghead through a bankruptcy auction.[75]

---

[65] Once the Federal agents get involved, many restrictions on what information can be collected and how it is to be collected will kick in. *See id.*

[66] *See id.*

[67] Egghead.com previously sold computers, software, and consumer electronics on its web site.

[68] *See* Lori Enos, *Egghead Hacked and Cracked*, E-COMMERCE TIMES, Dec. 22, 2000, *at* http://www.ecommercetimes.com/perl/story/6286.html.

[69] *See* Robert Lemos, *Lengthy Egghead investigation costs banks millions*, CNET NEWS.COM, Jan. 9, 2001, *at* http://news.com.com/2009-1017-250745.html?legacy=cnet (discussing the steps Egghead took after the hacking incident was discovered).

[70] *See id.*

[71] *See* Carol King, EGGHEAD.COM SALES SOFT IN Q4, INTERNETNEWS.COM, Jan. 26, 2001, *at* http://www.internetnews.com/ec-news/article.php/571601 (reporting that Egghead's sales revenue in the fourth quarter would not meet analysts' expectations).

[72] *See id.*

[73] *See* Michael Mahoney, *Egghead Files for Bankruptcy, Sells Assets*, E-COMMERCE TIMES, Aug. 16, 2001, *at* http://www.ecommercetimes.com/perl/story/12841.html (discussing Egghead's bankruptcy proceedings).

[74] *See id.* (discussing that the initial plan under bankruptcy was to sell most of its assets to Fry's Electronics, a California brick-and-mortar retail chain).

[75] Amazon.com purchased Egghead's Web address, customer data, trademarks, and other related intellectual property for $6.1 million in cash. *See* Ana Letícia Sigvartsen, *Egghead reborn*

b. Negative publicity concerns

The potential negative publicity that may come from reporting computer intrusions can be quite damaging and therefore can also be a contributing factor to the non-reporting of intrusive computer attacks.[76] For example, the CDUniverse.com ("CDUniverse") hacking incident in 2000, where 300,000 credit card numbers were stolen by a hacker, was widely publicized by the media.[77] Undoubtedly, CDUniverse lost many sales during the time that its web site was unavailable to potential customers. More importantly, however, many potential customers declined making purchases from CDUniverse for fear that their own credit card numbers would be stolen by hackers.[78]

Indeed, "most companies believe that the public relations ('PR') costs of being identified with weak security are far greater than the damage most malicious hackers can inflict."[79] Seventy percent of the respondents in the 2003 CSI/FBI indicated that negative publicity was a factor in not reporting intrusions to law enforcement.[80] Accordingly, most large companies tend to handle the problem in-house rather than risk the potential costs of negative publicity.[81]

c. Lack of knowledge by victims that anything can be done

Fifty-three percent of respondents in the 2003 CSI/FBI Survey indicated that they did not know they could report these incidents.[82] The survey narrates a highly probable explanation about the low rates of reporting:

> While [the lack of reporting] may seem strange, . . . it makes more sense in that it isn't always obvious who to turn to when someone has been hacking, say, your Web storefront's customer database. Should you turn to the local police? By and large, you won't get much help there. Should you turn to the FBI? In some cases they can help you and in others, they

---

through Amazon, Nov. 5, 2001, INFOSATELLITE.COM, *at* http://www.infosatellite.com/news/2001/12/a051201egghead_amazon.html.

[76] *See* COMPUTER SECURITY INSTITUTE, *supra* note 1, at 19 (indicating that in 2003, 70% of respondents cited negative publicity concerns as a reason for not reporting intrusions).

[77] *See Extortionist Puts Credit Card Data on Web*, *supra* note 3.

[78] *See* Maria Atanasov, *The truth about Internet Fraud: Merchants Pay the Price*, ZDNET AUSTRALIA, Mar. 13, 2001, *at* http://www.zdnet.com.au/news/business/0,39023166,20208623,00.htm ("As CDUniverse . . . can attest, fraud's most devastating effects are not the material costs associated with chargebacks or bank fees. What's often worse is the resulting damage to a merchant's reputation, erosion of consumer trust, and, ultimately, lost sales.").

[79] *See* Greene, *supra* note 64.

[80] *See* COMPUTER SECURITY INSTITUTE, *supra* note 1, at 19 (only 45% of the total respondents answered this question).

[81] San Diego Supercomputer Center Security Manager Tom Perrine, speaking at the tenth annual (2001) USENIX security Symposium in Washington, indicated that "[i]f you're a Fortune 500, there's about a 99.995 percent chance that you're going to cover up and go on." *See id.*

[82] *See id.* (reporting that only 45 percent of the total survey respondents indicated why they didn't report the intrusions, and of these 45 percent, 53 percent stated that they did not know that they could report these incidents).

can't (but it sure doesn't hurt to call).[83]

This lack of knowledge that anything can be done is not surprising given the low number of prosecutions of other hackers. Thus, the result is that many hackers that could be prosecuted if only reported are not being held accountable for their intrusive attacks.

2. Failure to prosecute

Notwithstanding the failure in reporting hackers, the failure in prosecuting hackers also creates a situation in which hackers are not being held accountable for their intrusive attacks. In this subsection, two factors for why hackers are not being prosecuted will be explored—a lack of understanding by law enforcement and the fact that computer crimes are difficult to prove.

a. A lack of understanding in hacking cases

Law enforcement has struggled with prosecuting hackers because the technology is complex and difficult to understand.[84] The result is that the vast amount of evidence presented along with the lack of understanding by police and prosecutors oftentimes leads to unnecessary searches, arrests, and court delays.[85] Thus, it is not surprising that in 1998, just under twenty percent of referred cases were prosecuted.[86] Moreover, this twenty percent is slim compared to the overall federal prosecution rate in 1998, which was approximately sixty-one percent.[87]

b. "Computer crime is terribly hard to prove"[88]

In the 1999 Banisar study discussed above, of the 419 cybercrime cases referred to prosecutors, 336 were dismissed.[89] The majority of these cases were dismissed for lack of supporting evidence.[90]

The lack of supporting evidence can result from either concealment by the hackers themselves (as discussed in Part III.A) or by delayed or improper actions by others. For example, as discussed above, Internet Service Providers may have routinely cleared their log files before receiving the retention order by law

---

[83] *See id.* at 17.

[84] Rob Apgood, *The Difficulty of Prosecuting High Tech Crimes*, WASHINGTON STATE BAR ASSOCIATION, Nov. 1999, *at* http://www.wsba.org/media/publications/barnews/archives/1999/nov-99-crimes.htm (stating that "the world of high-tech crime is frequently too complex for police and prosecutors to handle properly").

[85] *See id.*

[86] The actual percentage was 19.8% (83 of 419 referred cases). *See* Poulsen, *supra* note 48.

[87] In 1998, of the 132,772 referred cases, 82,071 of these were prosecuted. *See id*.

[88] This statement was made in 1999 by then FBI spokesperson Debbie Weierman. *See id.*

[89] *See* Apgood, *supra* note 84.

[90] *See id.*

enforcement.

All too often, companies that have been hacked into have not taken the proper steps to preserve evidence. Sometimes the hijacked computers remain in use, thereby overwriting all traces of the hacker's footprints.[91] Or at other times, companies may inadvertently destroy the traces of the hacker as they try to ascertain the damage to the hijacked computer system. Indeed, proper preservation of evidence requires that deliberate and laborious steps be taken, including making a byte-stream copy of the hijacked computer's hard-drive and employing forensic software to uncover changes on the hijacked computer.[92]

C. Failures in the ECPA and CFAA

Finally, there are some failures in the current federal laws that allow the problem of intrusive computer hacking to continue. This includes loopholes in the ECPA and the lack of deterrence by the CFAA.[93] Moreover, the CFAA fails to hold software manufacturers liable for the negligent design of software.[94]

1. Judicial exceptions to the ECPA

The courts themselves have conceded the shortcomings of the ECPA, which includes the Wiretap Act and the Stored Communications Act ("SCA") as described above in Part II.A. For example, in *United States v. Steiger*, the 11th Circuit stated that "our reading of the Wiretap Act to cover only real-time interception of electronic communications, together with the apparent non-applicability of the SCA to hacking into personal computers to retrieve information stored therein, reveals a legislative hiatus in the current laws purporting to protect privacy in electronic communications."[95]

As previously explained, the Wiretap Act applies only to acquisitions contemporaneous with transmission and, thus, typically would only apply to the hacker's use of network packet sniffers.[96] However, other hacking tools described in the Appendix such as buffer overflow attacks and Trojan horses are not prohibited by the Wiretap Act (although may be prohibited by other federal and state laws).

In addition, the SCA mainly applies against intrusive hackers whose

---

[91] For example, some of the evidence may be contained in a computer's temporary swap file. If the computer is rebooted, this temporary swap file is cleared.

[92] *See* Scott Grace, Computer Incident Response and Computer Forensics Overview, SANS INSTITUTE, *at* http://www.giac.org/practical/gsec/Scott_Grace_GSEC.pdf (last visited Mar. 26, 2004) (discussing how the computer expert will use forensic software to discover, to the extent possible, affected files and any attempts to hide, delete, protect, or encrypt information).

[93] *See infra* Part III.C.2.a.

[94] *See* 18 U.S.C. § 1030(g) (discussed *infra* in Part III.C.2.b)

[95] 318 F.3d 1039, 1049 (11th Cir. 2003) (emphasis added).

[96] For a discussion on network packet sniffers, see part F of the Appendix.

attacks are against Internet Service Providers, email servers, and other electronic communication services.[97] But, many computers that contain highly sensitive information would be more akin to a personal computer and not be considered an electronic service within the purview of the SCA.[98] Hackers could obtain access to these non-electronic communication service computers by either using a launch-pad style attack[99] (by utilizing a company's computer that is visible on the Internet to access a company's internal computer that is not accessible on the Internet) or through war dialing as described in Part C of the Appendix.

2. Failures in the CFAA

While the ECPA provides only limited assistance to the problem of intrusive computer hacking, the current version of the Computer Fraud and Abuse Act (including changes made by the PATRIOT Act) has covered many of the deficiencies of the ECPA.[100] Despite overcoming the deficiencies of the ECPA, the main problem with the CFAA is that it does not appear to be deterring intrusive computer hackers.[101] In addition, the CFAA does not hold software manufacturers liable for the negligent design of their software.[102]

a. Lack of deterrent effect of the CFAA

Twenty years have passed since the enactment of the first version of the CFAA in 1984, and the incidences of intrusive computer hacking have not declined but rather increased.[103] The 2003 CSI/FBI survey indicated that system penetrations for respondents increased from fifty-two in 1999 to one hundred thirteen in 2002 and eighty-eight in 2003.[104]

A possibility is that computer hackers may not know of the seriousness of penalties for certain violations of the CFAA. There is some support for this proposition. Some of the broadening amendments, including the definitions of damage and protected computers have only occurred recently.[105] Other provisions such as the strong protection of government computers have stood the test of time. Indeed, the CFAA was initially enacted in 1984 to protect government computers (and financial computers) from hackers. In 2002, a modern day hacker named *HeX* compiled a revised code of ethics for the hacking

---

[97] *See supra* Part II.A.2

[98] *See Steiger*, *supra* note 22.

[99] See Part III.A.1.a for how intermediate computers may be used to access the target computer.

[100] *See* 18 U.S.C. § 1030(a)(2) and (a)(5).

[101] *See infra* note 104.

[102] *See supra* note 94.

[103] See COMPUTER SECURITY INSTITUTE, CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 11 (2003), *available at* http://www.security.fsu.edu/docs/FBI2003.pdf.

[104] From 1999 to 2003, respondents reported 52, 68, 70, 113, and 88 system penetrations, respectively. *See id.*

[105] *See supra* Part II.B.1 for a discussion about how the PATRIOT Act broadened the definition of damage.

underground.[106] Included among his revised code of ethics was to never take "stupid" risks such as trying to connect to a government computer.[107] Undoubtedly, this was a recognition of the strong protection for government computers that has endured every revision of the CFAA.[108] Not surprisingly, this revised code of ethics did not include a prohibition against hacking into personal or corporate computers.[109]

Another possibility is that these hackers are overly optimistic about their chances of not being caught or prosecuted. Some experts have indicated that a significant number of hackings are committed by young people who believe that "they are untouchable."[110] Given the statistics compiled by Banisar regarding the actual number of prosecutions in 1998, these computer hackers may be justified in being overly optimistic.

b. Software manufacturers explicitly excepted from liability under the CFAA

Prior to the 2001 PATRIOT Act amendment of 18 U.S.C. § 1030(g), several courts had expanded the reach of CFAA to include not only damages resulting from unauthorized computer use, but also damages resulting from software manufacturers who distributed faulty software.[111] However, the last part of 18 U.S.C. § 1030(g) now explicitly states that "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."[112] This means that software manufacturers will not be held accountable for creating the security holes that allow computer hackers to hijack computer systems.

IV. MOVING TOWARDS A NATIONAL REPORTING REQUIREMENT FOR COMPUTER INTRUSIONS

Having established the technical, societal, and legal problems that contribute to the escalating problem of intrusive computer hacking, this paper now proposes a solution in the form of a national reporting requirement. First, as background, California's reporting requirement will be introduced. California is

---

[106] *See* Matheis, *supra* note 45 (discussing the evolution of hacker ethics).

[107] *See id.*

[108] *See* 18 U.S.C. § 1030(a) (protecting computers of the United States government); 18 U.S.C. § 1030(c)(1) (imprisonment up to 10 years for first offense or 20 years if existing prior conviction).

[109] *See* Matheis, *supra* note 45.

[110] *See* Raju Chebium, *Experts say more laws won't stop computer hackers*, CNN.COM, May 8, 2000, *at* http://www.cnn.com/2000/LAW/05/05/love.bug/.

[111] *See, e.g., Shaw v. Toshiba Am. Info. Sys., Inc.*, 91 F. Supp. 2d 926, 941 (E.D. Tex. 1999) (holding in a class action lawsuit that defendant-manufacturers use of faulty microcode in floppy diskette controllers that eventually were incorporated into computer systems fell into the prohibition of 18 U.S.C. § 1030(a)(5) (for a transmission of a program, information, code, or command that intentionally causes damage)).

[112] *See* 18 U.S.C. § 1030(g).

the first and only state with a reporting requirement. Next, a description of the proposed national reporting requirement and the interests to be protected will be presented. An argument will be made that such a proposed national reporting requirement is not only beneficial, but also necessary to tackle the problem of intrusive computer hacking. More specifically, this paper will argue that inaction by the national government could lead to an unworkable situation with piecemeal state-by-state legislation. Further, this paper will explain how such a proposed national reporting requirement can overcome the technical, social, and legal failures described in Part III.

A. California's Reporting Requirement (2002 Cal SB 1386)

California's reporting requirement (2002 Cal SB 1386, which amended the California Civil Code and took effect on July 1, 2003) was the first of its kind in the nation.[113] In short, the reporting requirement means that businesses that store their customers' personal information in the form of computerized data must warn their customers when their personal information is stolen (or suspected of being stolen) by computer hackers or other criminals.[114] Such a law is an attempt to extend and protect the privacy of individuals that transact with such businesses.

1. Impetus behind the Reporting Requirement

The birth of the California reporting requirement was the result of a hacking intrusion that affected thousands of California's employees. On April 5, 2002, a hacker broke into a computer database housed at California's Stephen P. Teale Data Center in Rancho Cordova.[115] The computer database, a personnel database, housed the personal information of the state's 265,000 employees.[116] The personnel database included the names, Social Security numbers, and payroll information of the employees.[117] Among the information included in the personnel database was the personal information of then-Governor Gray Davis.[118] While the intrusion was discovered a month later on May 7, 2002, public disclosure of the intrusion did not occur until May 24, 2002.[119] This delay in the public reporting provoked criticism from the California Union of Safety Employees ("CAUSE").[120] The public outcry from this incident was the main

---

[113] *See* Associated Press, *Bill would require customer notification of hacks*, CNN.COM, June 30, 2003, *at* http://www.cnn.com/2003/TECH/biztech/06/30/hacker.bill.ap/.

[114] *See infra* Part IV.A.2.

[115] *See* Jaikumar Vijayan, *Recent breaches raise specter of liability risks*, COMPUTERWORLD, May 31, 2002, *at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,71609,00.html.

[116] *See id.*

[117] *See id.* (the employees affected ranged from office workers to judges).

[118] *See id.*

[119] *See id.*

[120] CAUSE President Alan Barcelona criticized the state controller's handling of the incident stating that "It is an outrage that the controller herself has been negligent in recognizing the peril posed by this high-tech invasion of privacy." *See id.*

impetus behind the enactment of California's reporting requirement.[121]

On a broader level, the enactment of California's reporting requirement recognizes the growing problem of identity theft in California. For instance, in 2000, the Los Angeles County Sheriff's department reported 1,932 identity theft cases, representing a 108 percent increase over the prior year.[122] The California law attempts to thwart the growth of such identity theft arising from personal information that is obtained from breaches into computer systems.[123]

2. Applicability

California's reporting requirement became effective on July 1, 2003. Section 1798.29 of the California Civil Code, applicable to agencies, requires that:

> (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[124]

Similarly, Section 1798.82 has a reporting requirement for businesses:

> (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[125]

Both provisions require that "[t]he disclosure shall be made in the most expedient time possible and without an unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore reasonable integrity of the data system."[126]

In addition, for purposes of both Section 1798.29 and 1798.82, the Civil

---

[121] *See* Patrick Thibodeau, *California leads way on ID theft legislation*, COMPUTERWORLD, Dec. 13, 2002, *at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,71609,00.html (stating that the new California law was prompted by the breach where hackers gained access to the state's Stephen P. Teale Data Center).

[122] See SECTION 1 of 2002 Cal SB 1386.

[123] *See id.*

[124] CAL. CIV. CODE § 1798.29(a) (Deering 2003).

[125] CAL. CIV. CODE § 1798.82(a).

[126] *See* CAL. CIV. CODE § 1798.29(a); CAL. CIV. CODE § 1798.82(a).

Code defines "personal information" as:

> an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[127]

The required notice under both of these provisions can be satisfied with written or electronic notification.[128] In the event that providing written or electronic notification would be too burdensome (because such notice would cost more than $250,000 or more than 500,000 persons would have to be notified), then substitute notice may be utilized instead.[129] Substitute notice includes email notice, conspicuous notice on the web site page of the person or business, if the person or business maintains one, or notification to major statewide media.[130] Through the allowance of substitute notice, California's law recognizes the potential heavy burden that individual notification places on agencies and businesses.

3. Remedies

Section 1798.84 of the California Civil Code expressly provides for damages for customers injured by violations of California's reporting requirement. More specifically, Section 1798.84 states that "[a]ny customer injured by a violation of this title may institute a civil action to recover damages."[131]

B. A National Problem Requiring Congressional Response

After California's reporting requirement went into effect on July 1, 2003, other states may be considering similar measures as well. If other states were to pass similar laws, an untenable piecemeal state-by-state regulatory scheme would result.[132] For example, consider a hypothetical Internet company, Ames Corp. ("Ames"), that sells products throughout all fifty states[133] and assume that each state has passed a modified version of California's reporting requirement. If

---

[127] *See* CAL. CIV. CODE § 1798.29(e); CAL. CIV. CODE § 1798.82(e).
[128] *See* CAL. CIV. CODE § 1798.29(g)(1); CAL. CIV. CODE § 1798.82(g)(1).
[129] *See* CAL. CIV. CODE § 1798.29(g)(3); CAL. CIV. CODE § 1798.82(g)(3).
[130] *See id.*
[131] See CAL. CIV. CODE § 1798.84(a).
[132] The Information Technology Association of America (ITAA) opposed the California reporting requirement because of the concern about piecemeal state-by-state regulation of the issue and because the ITAA believed it is best left to the purview of the federal government. *See Hearing on S.B. 1386 Before the Assembly Comm. on Appropriations*, 2002 Senate 2 (Cal. 2002).
[133] Amazon.com, Buy.com, and Ebay.com are examples of such companies.

hackers obtained access to one of Ames's customer databases, Ames would have fifty different reporting requirements to comply with. Not only would this result be burdensome and costly to Ames, but Ames could never be sure that it has fully complied with all of the requirements of each state. For example, while many states may have similarly-worded statutes, each state may have a slightly different interpretation of its own statutes.

As an initial matter, because Congress has not yet enacted a reporting requirement, California's reporting requirement does not conflict with any federal statute and thus is not preempted under the Supremacy Clause[134] of the U.S. Constitution. Further, while the positive aspects of the commerce clause[135] permits Congress to regulate in this area (as will be discussed immediately below), the negative aspect of it, the dormant commerce clause, does not nullify California's reporting requirement (and perhaps the reporting requirements of other states, if enacted) even though it imposes limitations on interstate commerce. The dormant commerce clause, operating under the balancing test under *Pike v. Bruce Church, Inc.*,[136] requires that California's interest in a reporting requirement outweigh the burden the law imposes on interstate commerce. Based on the discussion above regarding California's interest in stopping identity theft, the *Pike* test is likely to be met and California's reporting requirement most likely survives dormant commerce clause considerations.

On the other hand, Congress has the power to solve this piecemeal state-by-state regulatory scheme by adopting a unifying approach under the commerce clause. In *United States v. Lopez*, Chief Justice Rehnquist, in delivering the opinion of the Court, indicated three categories of activity that Congress may regulate under the commerce power: (1) the use of the channels of interstate commerce, (2) the instrumentalities of interstate commerce or persons or things in interstate commerce, even though the threat may come only from certain intrastate activities, or (3) those activities having a substantial relation to interstate commerce.[137] A computer connected to the Internet would be using a channel of interstate commerce or an instrumentality of interstate commerce. The result is that Congress would indeed have the power to regulate this area.

Thus, if Congress does not enact a reporting requirement similar to

---

[134] Article VI, paragraph 2 of the United States Constitution states that "This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the contrary notwithstanding."

[135] Article I, Section 8, clause 3 of the United States Constitution states that Congress shall have the power "[t]o regulate Commerce with foreign Nations, and among the several States, and with Indian Tribes."

[136] *See* 397 U.S. 137, 142 (1970) (stating that "[w]here the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits").

[137] *See* 514 U.S. 549, 558-59 (1995).

California's, then an unworkable state-by-state solution may evolve. As will be described below, the benefits of a single unified approach greatly outweigh such a state-by-state solution.

C. A National Reporting Requirement Should Be Adopted

In 2003, U.S. Senator Dianne Feinstein (D-California) proposed a national reporting requirement modeled after California's reporting requirement known as the *Notification of Risk to Personal Data Act* ("Feinstein proposal").[138] The Feinstein proposal would have required a business or government entity to notify an individual whenever there is a reasonable basis to conclude that a hacker has obtained unencrypted personal information.[139] Personal information would have included an individual's Social Security number, driver's license number, state identification number, bank account number, or credit card number.[140] Fines by the Federal Trade Commission for non-compliance with the Feinstein proposal would have been $5,000 per violation or up to $25,000 per day for continuing violations.[141] Unfortunately, the Feinstein proposal has been stalled in committee.[142]

1. The proposed reporting requirement

This paper now proposes a national reporting requirement ("proposed reporting requirement") for the problem of intrusive computer hacking. Two interests will be recognized here—first, the interest of each individual in his or her privacy and secondly, the interest in protecting property against damage by computer hackers. In short, this proposed reporting requirement recognizes not only that hackers should be deterred, but also that the ripple effect of their hacking attacks be minimized by allowing victims to take proactive action after receiving timely notice.

a. Interest in preserving privacy

In one aspect, the proposed reporting requirement recognizes the privacy of individuals in their personal information. This interest in privacy means that the affected individuals should have an opportunity to reduce and minimize the risks and effects of identity theft. Because this goal is similar to that of

---

[138] *See* Roy Mark, *Feinstein Seeks Hacker Notification Law*, INTERNETNEWS.COM, June 30, 2003, *at* http://www.internetnews.com/bus-news/article.php/2229261.

[139] *See id.*; Berkley D. Sells, *California's New Hacker Disclosure Law and its Potential Impact on Canadian Businesses*, THE LAWYERS' WEEKLY, Aug. 15, 2003, *available at* http://www.fasken.com/Web/fmdwebsite.nsf/0/ EEADB6E2707588B585256D87005103E2/ $File/HACKERDISCLOSURELAW.PDF?OpenElement.

[140] *See id.*

[141] *See id.*

[142] *See* Kevin Poulsen, *No effect seen in US hack disclosure law*, THE REGISTER, Oct. 28, 2003, *at* http://www.theregister.co.uk/content/55/33622.html (discussing how California's disclosure requirement has not yet seen enforcement action).

California's reporting requirement, the proposed reporting requirement largely follows from the California reporting requirement.

i. Applicability

The proposed reporting requirements would apply to all agencies, businesses, companies, and organizations that store unencrypted computer data containing personal information as defined below. Like the California reporting requirement discussed above, any agency, business, company, or organization that discovers a breach or is notified of such a breach shall report the breach to the affected individuals within a reasonable time. Further, a reasonable basis for belief of a breach should also result in notification to the potentially affected individuals.

Note that the proposed reporting requirement does not apply to agencies, businesses, companies, and organizations that encrypt the personal information using at least 128-bit encryption. By not making this proposed reporting requirement applicable to *encrypted* personal information, this gives agencies, companies, and organizations an incentive to secure the stored personal information and thus avoid the reporting requirement. Moreover, the customers greatly benefit from the 128-bit encryption, which would take hackers no less than a *quintillion* (10^18) years to decode using a single computer.[143]

ii. Definition of personal information

Like the California reporting requirement, personal information will be defined to include a name (either first and last name or first initial and last name) in conjunction with at least one of the following unencrypted data: (1) social security numbers, (2) state identification numbers such as drivers' license numbers, or (3) deposit account numbers, credit card numbers, or debit card numbers if obtained with any required security code, access code, or password that would permit access to an individual's financial account.

In addition, personal information will also include email addresses, whether or not stolen in conjunction with the corresponding name. However, as will be discussed below, the notice requirement for email addresses will be less burdensome than for the other personal information described above.

iii. Means of notice

The affected individuals would receive notice within a reasonable time after the personal information is found to be or suspected of being stolen. A reasonable time cannot be exactly specified, but will depend on factors such as the nature and scope of the hacking incident and whether the hacking incident is

[143] See Richard E. Smith, *Are Web Transactions Safe?*, NOVA, *at* http://www.pbs.org/wgbh/nova/decoding/web.html (last updated Nov. 2000).

isolated or continuing.

If the stolen personal information includes social security numbers, state identification numbers, deposit account numbers, credit card numbers, or debit card numbers, then notice should be given either in written or electronic form. If the number of people to be notified exceeds 50,000, then constructive notice can be given by alerting the media or by providing a notice on the business or organization web site. This is because giving notice to each individual may often be very costly to the agency, business, company, or organization. For example, under the California reporting requirement, written or electronic notice must be given unless the number of individuals to be contacted exceeds 500,000. At thirty seven cents per letter, the postage alone for contacting 500,000 individuals would cost a company $185,000.[144] Under the proposed reporting requirement, the postage for contacting 50,000 individuals would be $18,500, an amount believed to be more reasonable and less likely to cause ruinous liability for smaller agencies, businesses, companies, and organizations.

Further, if an email address is stolen, whether or not in conjunction with a name, then notice shall be given to those affected through an email notice (at the same email address that was stolen by the hacker). Only one email notification need be sent so long as the sender is not responsible for a returned email. For instance, if the email is returned for any reason not in control of the sender of the email (i.e. mailbox full or mailbox address not found), then no second notice need be sent. If the number of people to be notified exceeds 100,000, then constructive notice can be given by alerting the media or by providing a notice on the agency, company, business, or organization web site. This requirement does not seem to be unduly burdensome to companies. For instance, on October 27, 2003, Orbitz.com ("Orbitz"), a web-based travel pricing and reservation company, detected a security breach that allowed spammers to obtain access to its customers' email addresses, which could have been as many as 18 million email addresses.[145] Three days later, on October 30, 2003, an Orbitz spokesperson had made a statement to the media that an unknown party had used unauthorized and/or illegal means to obtain the email addresses maintained with Orbitz.[146] If this proposed reporting requirement had been in effect, Orbitz would have complied with it because with over 18 million users to notify, this substitute notice through the media would have been sufficient as constructive notice to the affected users.

---

[144] This amount is below California's ceiling of $250,000. *See* Cal. Civ. Code §§ 1798.29(g)(3) and 1798.82(g)(3). If the agency or business can demonstrate that the cost of providing notice would exceed $250,000, then it is entitled to use substitute notice (e-mail notification, a conspicuous web site posting, or notification to major statewide media).

[145] Associated Press, *Spammers steal e-mail addresses from Orbitz*, CNN.COM, Oct. 30, 2003, *at* http://www.cnn.com/2003/TECH/internet/10/30/orbitz.security.ap/index.html.

[146] *See id.* (Orbitz spokeswoman Carol Jouzaitis stated that a "small number of customers have informed us that they have received spam or junk e-mail from an unknown party that apparently used unauthorized and/or illegal means to obtain their e-mail addresses used with Orbitz.").

b. Interest in protecting property against damage by hackers

In addition, this proposed reporting requirement recognizes an interest in protecting property against computer hackers. Accordingly, this proposed reporting requirement seeks to maximize the likelihood that the responsible parties will be subject to investigation and prosecutions. Presumably, the increased numbers of investigations and prosecutions should deter other potential computer hackers from causing property damage through their intrusive attacks.

i. Applicability

The second aspect of the proposed reporting requirement requires agencies, businesses, companies, and organizations that experience damage (as defined below) from a computer intrusion to report the intrusion to federal law enforcement. The intrusion would be reported to federal law enforcement within a reasonable time after the agency, business, company, or organization either discovers or has a reasonable basis for believing that a computer intrusion has occurred.

A good example of how this proposed reporting requirement is designed to operate can be illustrated by the hacking intrusion that happened to VoteHere, Inc. ("VoteHere") in late 2003.[147] VoteHere is involved in creating the highly-controversial electronic voting technology. Sometime in late 2003, a hacker broke into VoteHere's internal computer systems and may have copied the sensitive software source code.[148] Shortly after the intrusion was detected, VoteHere contacted the FBI and Secret Service and assisted in their investigation by providing the FBI and Secret Service with megabytes of evidence relating to the intrusion.[149] By contacting law enforcement shortly after the incident, VoteHere would have complied with the proposed reporting requirement.

---

[147] A similar hacking incident occurred to Diebold Election Systems ("Diebold") earlier in 2003. In the Diebold incident, a hacker broke into a private Web server and obtained internal discussion-list archives, a software bug database, and sensitive software. Prior to this incident, unauthorized outsiders had been able to copy the source code and documentation for the proprietary voting software from an insecure Diebold FTP site. *See* Brian McWilliams, *New Security Woes for E-Vote Firm*, WIRED NEWS, Aug. 7, 2003, *at* http://www.wired.com/news/privacy/0,1848,59925,00.html. Both of these Diebold incidents open the possibility that hackers may obtain the information and opportunity to breach the security of Diebold's electronic voting software. *See* Paul Krugman, *Hack the Vote*, NEW YORK TIMES, Dec. 2, 2003, *available at* http://www.commondreams.org/views03/1202-02.htm.

[148] A hacker that has obtained a software's source code would be able to examine how the software was written and possibly determine vulnerabilities in the software. This source code is different than the final product that is sold to consumers in a "run-time" or "compiled" form. When compiled, the source code is transformed to machine code and is typically incomprehensible.

[149] *See* Associated Press, *Site of electronic voting firm hacked*, CNN.COM, Dec. 29, 2003, *at* http://www.cnn.com/2003/TECH/biztech/12/29/voting.hack.ap/index.html. Executives at VoteHere believe the hacker break-in was related to the rancorous debate over the security of casting ballots online. *See id.*

ii. Definition of Damage

Damage under this second aspect of the proposed reporting requirement is the monetary loss that arises from the computerized data, code, software, or other program that is obtained, altered, or deleted through unauthorized means. Some consideration should be given to direct economic effects flowing from computerized data, code, software, or other program that is obtained, altered, or deleted through unauthorized means.

In that regard, damage includes the cost of repairing or restoring the affected data, code, software, or other program. Damage also includes any costs necessary to ensure the security of copies of the proprietary program that have already been sold. In another instance, if hackers were to shut down the normal operation of a commercial web site by deleting, modifying, or altering data on the web servers, then damage could include the loss of expected sales for the amount of time that the web site was not operational. On the other hand, damage does not include the cost of investigating or tracking the hacker.

iii. Jurisdictional Amount

The second aspect of the proposed reporting requirement does not apply to all damage amounts. Indeed, every hacking incident results in some kind of monetary loss, however slight. However, this proposed reporting requirement recognizes that reporting all damages may be burdensome and costly[150] to businesses. Accordingly, only damage that results in at least $20,000 in monetary damages should be reported. This recognizes that while many smaller computer intrusions will go unreported, those intrusions that exceed $20,000 in damages will likely result in more successful prosecutions, because the amount of the damage will likely justify a company's efforts to investigate, to preserve evidence, and to cooperate with law enforcement. In addition, companies may also be willing to seek civil remedies under the CFAA because they are likely to be above the $5,000 CFAA jurisdictional amount.

c. Enforcement of both aspects of the proposed reporting requirement

Unlike the California reporting requirement, no private right of action would be available against agencies, businesses, companies, and organizations that fail to comply with the proposed reporting requirement. An important purpose of the proposed reporting requirement is to give the affected individuals notice so that they can protect themselves from the ripple effect of a hacking intrusion. However, because hundreds of thousands of people may be affected by a single hacking incident, a business, company, or organization that fails to comply with the reporting requirement may be presented with ruinous liability.

---

[150] For a discussion on why many companies are unwilling to report hacking incidents, see Part IV.B.1.

Such a result would be much too harsh. Accordingly, the alternative enforcement mechanism would be a statutory fine to be decided on a case-by-case basis. The same result would be true in the case of non-compliance of the second aspect of the proposed requirement (where significant property damage had been received).

In addition, companies should not be allowed to bypass the reporting requirement by not monitoring for intrusions or performing intrusion audits. Thus, the statutory fine should be reduced in cases where companies have implemented a monitoring or auditing plan. This would make it more worthwhile for companies and organizations to continue to monitor against computer hackers.

d. Exception to the proposed reporting requirement

In some circumstances, giving public notice, either to the affected individuals or to the public, would hinder investigation by law enforcement. For example, in 1995, the infamous Kevin Mitnick ("Mitnick") breached the security of a popular bulletin board.[151] The bulletin board could have shut down, which would have tipped off Mitnick (as well as the general public).[152] However, by not shutting down the bulletin board, law enforcement was able to track Mitnick's moves online.[153] The result was that Mitnick was caught in possession of 20,000 stolen credit card records.[154] Accordingly, in a situation such as this, agencies, businesses, corporations, and organizations should be given some latitude to delay giving public notice when working with law enforcement. This delay is usually reasonable because the interest in apprehending the hacker outweighs the slight delay in giving public notice.

V. BENEFITS OF THE PROPOSED REPORTING REQUIREMENT

In Part III, the contributing factors to the problem of intrusive computer hacking were presented. In the first instance, hackers can be difficult to track down.[155] At other times, hackers are not tracked down because the victims do not report the intrusions to law enforcement.[156] Even if the hackers are tracked down by law enforcement, there is a tendency not to prosecute them or to prosecute

---

[151] *See* ROBERT B. GELMAN & STANTON MCCANDLISH, PROTECTING YOURSELF ONLINE: THE DEFINITIVE RESOURCE ON SAFETY, FREEDOM, AND PRIVACY IN CYBERSPACE 141-45 (1st ed. 1998). The investigation into Mitnick began when he hacked into Netcom Internet Services and compromised the confidentiality of several thousand credit-card numbers. Within the same time frame, Mitnick stole some sensitive files from security expert Tsutomu Shimomura of the San Diego Supercomputer Center. After breaching the security of bulletin board Whole Earth 'Lectronic Link (WELL), Mitnick had hidden some the sensitive files on WELL's systems. *See id.*

[152] *See id.*

[153] *See id.*

[154] *See id.* at 144 (discussing how law enforcement used cellular frequency scanners to track down Mitnick, who was using a computer modem connected to a cellular telephone for his online activities).

[155] *See* Part III.A.1 *supra* for difficulties in tracing hackers.

[156] *See* Part III.B.1 *supra* for reasons why companies do not reporting intrusions.

them with minimal sentencing.[157] Moreover, the judicial exceptions to the ECPA tend to make it inapplicable to the problem of intrusive computer hackings.[158] Further, although the recently-amended CFAA may compensate for the shortcomings of the ECPA, the CFAA does not tend to deter computer hackers.[159] Finally, the CFAA fails to hold software manufacturers liable for the negligent design of software that is compromised by hackers.[160] This section now illustrates how the proposed reporting requirement tackles many of the technical, societal, and legal problems presented in Part IV.

A. Removing Traditional Societal Barriers to Reporting

Businesses have previously been reluctant to report computer intrusions because of competitive advantage concerns, because of negative publicity concerns, and because of lack of knowledge that anything can be done.[161] This means that given the choice, businesses overwhelmingly choose to forgo reporting computer intrusions. However, a mandatory reporting requirement levels the playing field for the following reasons.

First, a mandatory reporting requirement would mean that regardless of whether an agency or business believes that anything can be done, they will have to report computer intrusions. Secondly, a mandatory reporting requirement lessens negative publicity and competitive advantage concerns. If all businesses have to report when they have experienced a computer intrusion, then no single business will have to bear the entire burden of reporting an intrusion because its competitors are also likely to be experiencing intrusions as well.

For instance, consider two companies in similar markets that are both experiencing intrusions from hackers. If a mandatory reporting requirement were not in place, then the first company that reported the intrusion (or perhaps was leaked to the media) could lose its competitive advantage to the competing company. For example, the other company might advertise that it is not experiencing intrusions like that of its competitor (even though it actually is). However, if a mandatory reporting requirement were in effect, both companies would have to report the intrusions and neither would receive a competitive advantage could be obtained by either. In addition, the effect of negative publicity would likely be lessened because a company's reporting would be included with the multitude of other reportings.

In other words, because there is no present mandatory reporting requirement, the current reportings of intrusion carry with them a large amount of

---

[157] *See* Part III.B.2 *supra* regarding the low prosecution rates.

[158] *See* Part III.C.1 *supra* regarding judicial exceptions to the ECPA.

[159] *See* Part III.C.2.a *supra* regarding lack of deterrence of the CFAA.

[160] *See* Part III.C.2.b *supra* for information about the CFAA exceptions for software manufacturers.

[161] *See supra* Part III.B.

backlash because the general public views computer intrusions as an anomaly rather than a daily battle. This is because such a small percentage of the current intrusions are reported, and when they are reported, they are typically very large in scope and damage. However, if a mandatory reporting requirement were in effect, then the larger number of reportings and the regularity of the reportings would mean the general public would begin to see the scope of the problem and would shift away from blaming any single company or business for having weak security. Instead, the focus would shift to "what can we do about this hacking problem?"

B. Public Notice and Awareness of the Problem

"Software consumers . . . fail to prevent security-related software failure because of imperfect information. Some customers misjudge the threat [because] intrusions are for the most part largely undetected and unreported. Others exhibit an 'it can't happen to me' mentality."[162]

As stated above, one of the hurdles to reducing the number of computer intrusions is the imperfect information that software consumers often have. However, the problem is not limited to imperfect information by software consumers, but also imperfect information by software manufacturers, the general public, and even law enforcement.

On a broader level, the problem is that we cannot tackle the problem of intrusive computer hacking until we actually understand the problem in the first place. Take for instance a House subcommittee hearing in September 2003 where IT vendors generally recommended more money in lieu of new laws to tackle the problem of cybercrime.[163] A troubled conversation evolved as the subcommittee's chairman, Representative Adam Putnam (R-Florida), questioned John Malcom, assistant attorney general at the Criminal Division of the U.S. Department of Justice:

> [Putnam] questioned why John Malcolm, deputy assistant attorney general at the Criminal Division of the U.S. Department of Justice could only name a handful of cyber criminals who've been caught.…'There are hundreds of viruses released every year ... but you can recall two arrests, two convictions,' Putnam said to Malcolm. 'I asked what was the source of the threat. "We really don't know." Was it foreign or domestic? "We

[162] Kevin Pinkney, Article, *Putting blame where blame is due: software manufacturers and customer liability for security-related software failure*, 13 Alb. L.J. Sci. & Tech. 43, 67 (2002).

[163] *See* Grant Gross, *Feds Search for Cybersecurity Solutions*: *More money, not new laws, are the key to security, most experts agree*, PC WORLD.COM, Sept. 11, 2003, *at* http://pcworld.shopping.yahoo.com/yahoo/article/0,aid,112419,00.asp (stating that only 3 of the 12 experts hinted at new legislation). Putnam is also considering legislation that would require companies to fill out a cybersecurity checklist in their reports to the Securities Exchange Commission ("SEC"). *See id.*

really don't know." That seems to re-enforce a premise that cybercrime is treated vastly different than some other crimes that caused significant damage.'[164]

Increasing the number and frequency of reportings will increase the knowledge base of the problem of computer hacking. This knowledge will assist software consumers in taking proactive actions to secure their systems. Moreover, software manufacturers will be able to respond to the problem by: (1) developing anti-hacking software, (2) fixing existing security holes, and (3) improving the security of future software. Further, the additional information gained from the reported hackings will provide evidence of the adequacy or inadequacies of the current laws such as the CFAA. Without this data, the discussion about the adequacy of the current laws is moot because these laws have largely remained untested in the case of intrusive computer hackers. The conclusion to be drawn is that we just do not know enough about the problem to tackle it efficiently and effectively. However, a reporting requirement will help provide the necessary information required to effectively tackle the computer hacking problem.

C. Deterrence

Some experts have posited that more laws will not deter hackers. These experts point to the public awareness of high-profile hacking cases (such as the prosecution of Kevin Mitnick) and yet the number of computer hackings has not decreased, but rather increased. Other experts have argued that "most hacking is committed by young people seeking attention and believing themselves to be mere high-tech pranksters . . . and laws will do little to deter them."[165] Still another expert has argued that "[he doesn't] know what good more laws can do. The fix to this is technical."[166]

Despite the scattered high-profile cases, the problem continues because the law at this stage not made a statement about the act of computer hacking itself but only about the possibility of being caught. Indeed, most computer hackers have always realized, whether consciously or not, that law enforcement tracking down a skilled hacker is not the norm.

A mandatory reporting requirement should increase the number of reported computer intrusions. Increasing the number of reported computer intrusions will also result in a higher number of computer hackers being tracked down by law enforcement (and thus being prosecuted). As more hacking cases become reported and as more hackers are prosecuted, the number of hackers willing to take the risk of a being prosecuted should also decrease. Thus, this proposed reporting requirement would provide an enhanced level of deterrence

---

[164] *See id.* (emphasis added).
[165] *See* Chebium, *supra* note 110.
[166] *See id.*

against computer hacking.

Consider for example when the Recording Industry Association of America ("RIAA") began cracking down on MP3[167] file-sharing in 2003. In early 2003, the RIAA began targeting individuals who maintained servers that allowed users to download MP3's.[168] Four university students were sued by the RIAA, thereby resulting in a substantial amount of publicity. These four students eventually settled with the RIAA in May 2003, with each student agreeing to pay between $12,000 and $17,000 each.[169] The RIAA also announced that it would go after individual file traders utilizing file-sharing tools such as Kazaa and Grokster.[170] Shortly after the announcement, online file swapping of MP3's began to drop sharply.[171] According to a 2003 report by The NPD Group ("NPD"), the number of households acquiring music fell from 14.5 million in April to 12.7 million in May to 10.4 million in June.[172] NPD stated "[w]hile we can't say categorically that the RIAA's legal efforts are the sole cause for the reduction in file acquisition, it appears to be more than just a natural seasonal decline."[173] Even more recently, a telephone survey indicated that the percentage of Americans downloading music from the Internet fell to 14% over the four week period ending December 14, 2003.[174] Previous telephone surveys in March, April, and May 2003 had indicated that approximately 29% of Americans were downloading music during that time frame.[175] Thus, preliminary evidence indicates that the RIAA's targeting of individuals who participate in file-swapping is deterring others from participating in online file-swapping. Similarly, a mandatory reporting requirement should increase the number of prosecuted hackers, and thus deter potential computer hackers. The result should be a reduction in hacking intrusions over time.

D. Market Correction

As previously discussed in Part III.C.2.b, the CFAA fails to hold software manufacturers liable for creating software that contains security vulnerabilities.

---

[167] An MP3 is a highly compressed file-format that usually contains audio. The MP3 format can generally be used to covert uncompressed audio files into MP3 data files that are less than 1/10th the size of the original.

[168] *See* Lisa M. Bowman, *Labels aim big guns at small file swappers*, CNET NEWS.COM, June 25, 2003, *at* http://zdnet.com.com/2100-1105_2-1020876.html.

[169] *See id.*

[170] *See id.*

[171] *See* Lisa M. Bowman, *File-swappers put off by lawsuits*, CNET NEWS.COM, Aug. 22, 2003, *at* http://news.zdnet.co.uk/internet/0,39020369,39115873,00.htm.

[172] Music acquisition included obtaining songs from paid sites, ripping CDs, and through file-swapping tools. During the 3 month study, file-swapping accounted for 2/3's of the total amount of music acquisition. *See id.*

[173] *See id.*

[174] The telephone survey was conducted by the Pew Internet & American Life Project. *See* Lisa Baertlein, *Music downloads fall after RIAA lawsuits-study***,** FORBES.COM, Jan. 4, 2004, *at* http://www.forbes.com/personalfinance/retirement/newswire/2004/01/04/rtr1197410.html

[175] *See id.*

Although software manufacturers are likely to be in the best position to reduce the risk of computer intrusions, the CFAA exception ensures that they shoulder little of the hacking damage resulting from their faulty software.[176]

One might expect that if the law refuses to hold software manufacturers liable for their faulty software, then the market may punish these manufacturers for producing faulty software. Yet, the market response has been inefficient due to imperfect information. In other words, the market cannot correct for a problem that it does not know about. If computer intrusions are being substantially underreported, then the market does not realize which software programs are faulty. In addition, competitors will be hesitant to enter into a competing area without having knowledge of a specific need or demand (because the assumption is that the current software is adequately protected). A mandatory reporting requirement should be able to correct for these market deficiencies.

First, consumers will be less likely to purchase software that is known to be faulty. Accordingly, if the law refuses to punish manufacturers for faulty software, then the market surely will. Secondly, in order to maintain their competitiveness, software manufacturers will have to create more secure software or risk the negative publicity. Finally, where the reported intrusions indicate a need, the market will quickly fill that need. In essence, the mandatory reporting requirement is a catalyst for what the market would have done given enough time and information.

VI. CRITIQUE OF THE PROPOSED REPORTING REQUIREMENT

Critics of a national reporting requirement have stated several concerns about a national reporting requirement. First, critics state that a reporting requirement reduces incentives of companies to monitor in the first place. Indeed, why would a company implement a plan to increase the probability that they will have to report an intrusion (and therefore suffer the resulting damage to its reputation)? Further, if companies are not diligent in monitoring intrusions, this may only exacerbate the problem. Secondly, even if companies detect an intrusion, many critics believe that most large companies would rather risk the possibility of statutory fines of not reporting rather than risk negative publicity. These companies believe that the public disclosure of an intrusion may mean near-certain death for the company. However, the proposed national reporting does have the ability to induce the companies to comply with the reporting requirement. The reporting requirement does this by allowing enough flexibility and variance in the statutory fines to make it rational for companies to monitor.

[176] *See* Pinkney, *supra* note 162, at 46. "Software manufacturers rush to market with products full of foreseeable vulnerabilities. Due to the market power possessed by some manufacturers, software manufacturers directly affect how much hacker risk enters the system. Software manufacturers are the least cost avoiders for many types of hack-prevention, yet they shoulder almost none of the harm that results from hacking." *See id.*

For example, consider a company with a multi-billion dollar market capitalization that must decide whether it will implement a monitoring system or not. If the company does not monitor, it is likely that if an intrusion were detected, the damage (both actual and reputational) would be more severe than if they had detected the intrusion during routine monitoring (assume $30 million versus $10 million in damage). This might be the case because a company that does no monitoring is likely to discover the intrusion only after significant damage had already been done for an extended period of time, at which point the intrusion becomes obvious. In contrast, a company that has a periodic monitoring plan is more likely to be able to stop intruders before any significant damage is done. Therefore, a company that monitors is more likely to have less security vulnerabilities because it likely takes preventative action in updating its software and hardware. This difference alone may induce a company to monitor. However, remember that monitoring increases the probability that reporting will have to be done under the proposed reporting requirement (and therefore some reputational damage will be done). In order to equalize the difference between reporting and not reporting (and tilt the decision in favor of reporting), a discount in the statutory fine can be made for companies that monitor. Furthermore, the overall magnitude of the statutory fines can be varied to make it more expensive not to report (whether or not a company decides to monitor). The main benefit of a flexible statutory fine is that proper tailoring of the fine can incentivize a company to monitor and report intrusions.

The proposed reporting requirement also reduces the cost that each company bears through reporting by removing the prisoner's dilemma problem as illustrated in Table I. Removing the prisoner's dilemma problem should reduce the possibility that any company would suffer near-certain death from reporting an intrusion. This is because the overall damage would be spread among the companies such that no company alone bears the burden. Further, as will be illustrated below, the overall damage level should decrease because more reportings will result in increased prosecutions of hackers, which should deter other hackers from committing similar crimes.

Table I
Game Table: Prisoner's Dilemma for Reporting Intrusions

		Company A	
		Report	**Don't Report**
Company B	**Report**	$1X, $1X	$0, $12X
	Don't Report	$12X, $0	$7X, $7X

According to Table I, if Company A reports and Company B does not, then Company A suffers damage of $12X while Company B only suffers nominal damage in comparison (and vice versa). This is because Company B can gain the competitive advantage over Company A when Company A reports and Company B does not. However, if neither Company A nor Company B reports, then neither

company can gain the competitive advantage, but the intrusion problem remains and continues to cause $7X worth of damage to each company. On the other hand, if both Company A and B report their intrusions, both would suffer less damage than either of the schemes above ($1X each because more computer hackers will be tracked down, prosecuted, and deterred; in addition, software manufacturers will release better software and more security update patches). However, notice that without a reporting requirement, each company would decide not to report because the possibility of losing $12X (if their competitor does not report) would keep each company in a defensive mode. Thus, a mandatory reporting requirement means that if each company reports, then the overall damage to either company is reduced. This is indeed the most desirable and least costly solution.

VII. CONCLUSION

Hackers utilize a variety of tools to compromise the security of computer systems. More importantly, hackers do not usually limit their intrusive activities to any single business or organization. A single hacker may target multiple businesses or organizations. Moreover, these hackers have not been deterred because only a handful of hackers have been prosecuted in the twenty years since the enactment of the Computer Fraud and Abuse Act. These problems contribute to the growing problem of computer intrusions.

In addition, the damage caused by a computer intrusion is not limited to the target of the intrusion. In the case of a stolen database of credit card numbers, banks may spend hundreds of thousands, if not millions of dollars, just to replace the credit cards in the hands of their customers.[177] Additional costs include the customers' temporary loss of use of their credit cards and the costs resulting from actual identity theft.[178]

Currently, many businesses and organizations fail to internalize the externalities described above. A mandatory reporting requirement, as proposed in this paper, will motivate businesses and organizations to internalize these external costs. In addition, the benefits of the proposed reporting requirement as described above in Part V may be achieved. These benefits include minimizing competitive advantage concerns, increasing public awareness of the problem, deterring other hackers, and allowing market forces to correct for negligent software design.

The Feinstein proposal for a national reporting requirement has been considered and was stalled in committee. A less intrusive approach is being considered by Representative Adam Putnam (R-Florida), chairman of the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, that may require public

[177] *See* Robert Lemos, *supra* note 69 (noting that it costs a credit card issuer between $2 and $5 to cancel and issue a new credit card).

[178] *See id.*

companies to report their cybersecurity efforts to the Securities Exchange Commission (SEC).[179] With several reporting proposals being considered by Congress, it is possible that a national reporting requirement may soon be adopted in some form. No matter what approach is taken, the law needs to make a statement that computer hacking is indeed a crime. This proposed reporting requirement is an effective way for the law to make that statement loud and clear.

APPENDIX

Computer hackers have a variety of tools for breaching the security of computer systems. Some of these tools such as social engineering are non-technical in nature. In addition, there are a wide array of technical tools available to hackers who want to break into computer systems. These technical tools include password cracking, war dialing, buffer overflow attacks, Trojan horses, and network packet sniffing.[180]

A. Social Engineering

The most commonly overlooked form of hacking is social engineering because of the lack of technical sophistication needed to employ this technique.[181] Social engineering has been defined to mean "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information [. . .] he needs to gain access to the system."[182]

For example, social engineering entails a hacker posing as an employee and utilizing a sense of urgency to coerce a corporate IT helpdesk into giving up a username or password. A hacker may pose as a company executive, out of town,

---

[179] *See* Grant Gross, *Cybersecurity legislation may go to Congress*, COMPUTERWORLD, Sept. 4, 2003, *at* http://www.computerworld.com/governmenttopics/government/legislation/story/0,10801,84586,00.html (The proposed legislation that would require public companies to file a cybersecurity checklist with the SEC, which would then be available for inspection by stockholders. The cybersecurity checklist would ask questions such as "Do you have an up-to-date IT assets list?").

[180] The author recognizes that the above list of technical tools available to hackers is not all-inclusive. As technology continuously changes, hackers will find new and innovative ways to breach computer systems. For example, when wireless systems were first introduced, hackers could access some wireless computer systems from their car, thus coining the term "war driving." For a good article about how war driving is accomplished, see Kevin Poulsen, *War driving by the Bay*, SECURITYFOCUS, Apr. 12, 2001, *at* http://www.securityfocus.com/news/192.

[181] For example, the Bush administration's September 18, 2002 draft of the "National Strategy to Secure Cyberspace" did not address social engineering. *See* Michelle Delio, *The Book on Mitnick is by Mitnick*, WIRED NEWS, Oct. 3, 2002, *at* http://www.wired.com/news/culture/0,1284,55516,00.html.

[182] Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, SECURITYFOCUS, *at* http://www.securityfocus.com/infocus/1527 (last updated Dec. 18, 2001) (quoting John Palumbo, *Social Engineering: What is it, why is so little said about it, and what can be done about it?*, SANS INSTITUTE, July 26, 2000, *at* http://www.giac.org/practical/GSEC/John_Palumbo_GSEC.pdf).

in a rush, and in desperate need of his network password.[183]

Yet another form of social engineering involves a hacker tricking a user into downloading an illicit program that allows the hacker back-door access to the computer system.[184] A good example of this type of social engineering occurred in September 2000 when unsuspecting AOL employees opened up a malicious email attachment that gave the hackers back-door access into the employees' computers.[185] Once the hackers were connected to AOL's computers, they had the ability to bump customers off of their AOL accounts, reset passwords, and access personal and billing information.[186]

B. Password Cracking

Most computer networks use some combination of usernames and passwords as a form of security to prevent unauthorized access into their computer systems. Hackers will oftentimes use password crackers to systematically guess these passwords for them.

There are three well-known types of password crackers. First, there are password crackers that use dictionary files, which contain an exhaustive list of all words listed in a dictionary.[187] Second, some password crackers are hybrids of dictionary password crackers, and use combinations of numbers or symbols with the dictionary files.[188] For example, these hybrids may try "cat," "cat1," "cat2," and so on.[189] Third, there are password crackers that utilize brute force, which iteratively try all combinations of numbers, alphabetic, and special characters

---

[183] In this true example, the hackers had actually studied the CFO's voice before impersonating the CFO. *See id.* In another example, the hackers determined the corporate director of IT's identity from a public domain name registry. By posing as the corporate director traveling on business and with a heavy deadline to obtain some PowerPoint slides, the hacker was able to pressure the help desk into revealing to the hacker the required software and appropriate credentials needed to obtain remote access to the corporate network. *See* JOEL SCAMBRAY ET. AL., HACKING EXPOSED: NETWORK SECURITY SECRETS & SOLUTIONS 561-62 (2d ed. 2001).

[184] *See* Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, SECURITYFOCUS, *at* http://www.securityfocus.com/infocus/1527 (last updated Dec. 18, 2001) (discussing how a hacker convinced an AOL employee to open by email what was supposed to be a picture of a car for sale but instead turned out to be a email exploit). See *infra* part E of the Appendix for a discussion regarding Trojan horses.

[185] *See* Jim Hu, *AOL boosts email security after attack*, CNET NEWS.COM, Sept. 21, 2000, *at* http://news.com.com/2102-1023_3-242092.html.

[186] *See id.* Although the hacker's attack could have been more malicious, the main effect of this attack was that some users found their AOL screen names were already being used when they tried to log in. *See id.*

[187] *See* Rob Shimonski, *Hacking techniques: Introduction to password cracking*, IBM DEVELOPERWORKS, July 2002, *at* http://www-106.ibm.com/developerworks/security/library/s-crack/.

[188] *See id.* (explaining that hybrid attacks are often successful because many people change their passwords by simply adding a number to the end of their current password)

[189] *See id.* Some hybrid password crackers add numbers or symbols to the end of the words in the dictionary list. Others will substitute symbols for letters—for example, "@" for the letter "a".

until a successful password is found-- no matter how long it takes.[190]

C. War Dialing

Most organizations protect their network computers from hackers through the use of an intrusion detection system or a firewall, which is something akin to having a big guard at the front door that stops intruders. These instruction detection systems or firewalls are installed on "gateway computers," which are the first point of contact (i.e. the front door) for outside computers attempting to gain access an organization's private network. While much time and money is spent on protecting the front door, many organizations fail to expend the same effort in protecting the back door—the modems that provide remote access for the organization's employees.

Because many organizations fail to adequately protect these modems, "war dialing" has developed as a way for hackers to exploit this vulnerability. A hacker would use a software program to dial a large block of the organization's telephone numbers (usually very late at night), and then examine the program logs[191] to determine which numbers were answered by modems that allow remote control access.[192] The hacker can then call back those modems and attempt to connect to them through remote control software.[193]

D. Buffer Overflow Attacks

Buffer overflow attacks are one of the most common methods used to remotely exploit target machines.[194] To understand buffer overflow attacks, one must understand how a software program allocates inputted data into memory.[195] When a software program receives an input by a user, it must store the user-inputted data somewhere. That somewhere is an allocated portion of the buffer (a

---

[190] See Harold W. Lockhart et. al., *How are brute force password cracking routines so successful*, ITSECURITY.COM SECURITY CLINIC, *at* http://www.itsecurity.com/asktecs/jul101.htm (last visited Mar. 26, 2004) (stating that given enough time, a brute force cracker will eventually discover the correct password).

[191] Software programs often keep track of data in files known as "computer logs." The computer logs are often utilized in modem communications to keep track of information that is sent and received during the initial authentication.

[192] See Michael Gunn, *War Dialing*, SANS INSTITUTE, Oct. 5, 2002, *at* http://www.sans.org/rr/papers/index.php?id=268. As an example, if a company's main telephone number were 555-1000, the hacker may dial the block of telephone numbers from 555-1000 to 555-1999, which would represent a block of one thousand telephone numbers. *See id.*

[193] *See id.*

[194] *See* Gary McGraw & John Viega, *Making your software behave: Learning the basics of buffer overflows*, IBM DEVELOPERWORKS, Mar. 1, 2000, *at* http://www-106.ibm.com/developerworks/library/s-overflows/ (stating that buffer overflows accounted for over 50% of CERT/CC advisories of major security bugs in 1999).

[195] The most common programs to have buffer overflow problems are those written in some version of C (C, C++, etc.). C/C++ is inherently unsafe because C/C++ does not automatically check the bounds of array and pointer references. *See id.*

memory region).[196] When a faulty program writes more information into the buffer than it has been allocated, a "buffer overflow" has occurred. The extra information that could not fit into the allocated portion of the buffer gets written into another unallocated portion of the buffer (the "spilled over" portion).[197] Hackers take advantage of this buffer overflow condition by realizing that they can intentionally overwrite the "spilled over" portion of the buffer with their own malicious code. The result is that the faulty program may execute the hacker's malicious code, thereby giving the hacker control over the computer running the faulty program.[198]

E. Trojan Horses

A Trojan horse is a program that masks itself as a legitimate program, but actually contains malicious code embedded within.[199] Sometimes the malicious code allows a hacker to gain control of the computer running the Trojan horse.[200] This type of Trojan horse operates by controlling free ports[201] on infected computers, thereby allowing the hacker access to the computer through the free port.

An innocent user may be tricked into opening an email attachment containing (or by otherwise downloading and installing) the Trojan horse, thinking that the program is legitimate.[202] Other times, hackers who have hacked into computer systems may not want to go through the trouble of hacking in again every time they want access to the infected computer. Instead, these hackers would install a Trojan horse that gives them at-will access to the infected computer.[203]

---

[196] Contiguous chunks of the same data types are allocated to a buffer. *See id.*

[197] *See id.* The example that the authors use for a buffer overflow is a cup. A cup can hold only so much water. If you overfill the cup, the spilled over water must go somewhere. In programming terms, the spilled-over water will find its way to another portion of the buffer and cause a buffer overflow. *See id.*

[198] *See id.* Buffer overflow attacks usually only result in the hacker obtaining the same level of access that the faulty program had. However, some buffer overflow attacks can result in the hacker obtaining the highest level of access possible (even though the faulty program previously didn't already have that access). *See id.*

[199] *See* Mathias Thurman, *On the Trail of an Elusive Trojan Horse*, COMPUTERWORLD, May 7, 2001, *available at* http://www.computerworld.com/printthis/2001/0,4814,60206,00.html (discussing that Trojan horses, "when launched, could destroy data, steal account information and allow a hacker to remotely control a system to launch attacks on other systems – all without the user's knowledge").

[200] *See id.* (explaining that a Trojan horse can let a hacker gain full control over an infected machine at a later date).

[201] A port is an external communication point on a computer operating system.

[202] Another example of social engineering in conjunction with Trojan horses is emails directing users to install false upgrades of Internet Explorer. *See* CERT, CERT ADVISORY CA-1999-02 TROJAN HORSES (1999), *available at* http://www.cert.org/advisories/CA-1999-02.html.

[203] *See id.* (explaining that once a hacker has compromised a system, the hacker may install Trojan horse versions of system utilities).

F. Network Packet Sniffers

Hackers often employ network packet sniffers ("sniffers") after they have successfully hacked into the target computer on a network. Once a hacker has hacked into the target computer, the hacker may need to gather passwords for other computer systems on the network, to obtain sensitive information, or to profile other computers on the same network. By installing a sniffer, the hacker can listen to (i.e. to capture) traffic transmitted between computers in the network on which the sniffer is installed.[204] By analyzing any unencrypted traffic captured by the sniffer, the hacker can reveal usernames, passwords, messages, and other personal or sensitive information that was transmitted along the network segment.

[204] *See* Matthew Tanase, *Sniffers: What They Are and How to Protect Yourself*, SECURITYFOCUS, *at* http://www.securityfocus.com/infocus/1549 (last updated Feb. 26, 2002) (discussing how a sniffer program switches a computer's network card to "promiscuous mode," and thus allowing a hacker to read all information being transmitted on the network that the network card is connected to).