UIC John Marshall Journal of Information Technology & Privacy Law

Volume 18
Issue 4 *Journal of Computer & Information Law - Summer 2000*

Article 6

Summer 2000

Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks, 18 J. Marshall J. Computer & Info. L. 1019 (2000)

Sarah Faulkner

INVASION OF THE INFORMATION SNATCHERS: CREATING LIABILITY FOR CORPORATIONS WITH VULNERABLE COMPUTER NETWORKS

I. INTRODUCTION

Computer hackers[1] are a serious threat to businesses and their customers.[2] Businesses that operate complex computer networks and online businesses are more susceptible to attacks by computer hackers.[3] However, these are not the only systems that are susceptible to attack. Multifaceted phone systems are often attacked by "phone phreaks"[4] and

[1] *See* Bruce Sterling, *The Hacker Crackdown* (visited Sept. 26, 1999) <http://www.graylab.ac.uk/help/hackers/part2.html>. The term "hacker" by most recent definition, means someone who intrudes into computer systems without authorization or permission. *Id.* Hackers have been described as "computer intruders," "computer trespassers," "crackers," and "wormers." *Id.* Originally, the term hacker described "free-wheeling intellectual exploration of the highest and deepest potential of computer systems." *Id.* Further, hacking can describe the process of making information and computers open to everyone. *Id.* Historically, the term hacker referred to a member of the Tech Model Railroad Club of Massachusetts Institute of Technology, and "to hack" meant to undertake a project of creating a product that had no constructive purpose, but rather was created or undertaken for the "wild pleasure" of involvement. *Id.* *See also* Briggs v. Maryland, 704 A.2d 904, 907 n.4 (Md. 1998). Members of the Tech Model Railroad club resent that their term is now used to describe one who commits illegal acts with a computer. *Id.* They maintain that more appropriate terms such as "thieves," "password crackers," or "computer vandals" are more accurate descriptions. *Id.*

[2] *See* Dorothy Denning, *Who's Stealing your Information?* (visited Sept. 26, 1999) <http://www.infosecuritymag.com/apr99/cover.htm>. In 1997, the American Society for Industrial Security conducted a survey of Fortune 1000 companies and the 300 fastest growing U.S. companies and found that they could be losing more than $250 billion annually to information thieves. *Id.* More than half of the 172 companies surveyed stated that they have been the victim of information misappropriation. *Id.*

[3] *See* David Icove, et. al., Computer Crime 129 (1995). Communications among computers vastly increases their power. *Id.* However, the more connections and communications a computer has with outside networks, such as systems in branch offices, across the country, and in foreign countries, the more susceptible the computer is to having those channels used for iniquitous means. *Id.* The F.B.I. reports that four of five computer crimes investigated over the past few years were aided by Internet access. *Id.*

[4] Sterling, *supra*, note 1. Before computer networks, degenerates who infiltrated phone systems were known as "phreaks." *Id.* Now, since the advent of computers the line

have caused large monetary losses as well.[5] The question of who is liable for these monetary losses due to illegal activity is the subject of this comment.

Notorious computer hacker Kevin Mitnick caused millions of dollars worth of damages by stealing software programs, e-mail, monitoring computer systems and impersonating employees of victim companies.[6] Some of the companies Mitnick violated included major information technology giants such as Motorola, Novell, Fujitisu, and Sun Microsystems.[7] He used many different methods to steal and infiltrate these companies including: social engineering, cloned cellular telephones, "sniffer" programs, and hacker software programs.[8] Many other means of unauthorized access exist including: password cracking, exploiting known security weaknesses, and network spoofing.[9] However, the methods that

between "phreaks" and hackers has blurred considerably. *Id.* However, a small behavioral distinction remains, hackers are more interested in the system as a whole where "phreaks" like to manipulate the system to get through to others fast and cheap. *Id.* For the purposes of this comment the term hacker will be used to denote either a computer hacker or a "phone phreak." *Id.*

[5] *See* JEAN GUISNEL, CYBERWARS ESPIONAGE ON THE INTERNET 111 (1997).The United States Secret Service determined that in 1994, $2.5 billion of phone fraud was perpetrated. *Id.* The telecommunications industry estimates between $1 billion and $9 billion. *Id.*

[6] *See* U.S. Department of Justice, *Kevin Mitnick Sentenced to Nearly Four Years in Prison* (visited Sept. 26, 1999) <http://www.usdoj.gov/criminal/cybercrime/mitnick.htm>. Mitnick pled guilty to a series of federal offenses including: four counts of wire fraud, two counts of computer fraud, and one count of illegally intercepting a wire communication. *Id.* *See generally*, TSUTOMU SHIMOMURA & JOHN MARKOFF, TAKEDOWN THE PURSUIT AND CAPTURE OF KEVIN MITNICK, AMERICA'S MOST WANTED COMPUTER OUTLAW- BY THE MAN WHO DID IT (1996) A first hand account of Kevin Mitnick's crimes by one of his victims. *Id.*

[7] *See* U. S. Department of Justice, *supra* note 6, at 3.

[8] *A Message to Phone Cloners: Wrong Number*, SAN DIEGO BUSINESS JOURNAL, April 12, 1999 *available in* NewsBank Record Number: 001030DCB77D601F783CA. Social Engineering is simply a bullying process whereby a person pretends to be an authority figure and demands a new password, or demands that he be allowed to access the system. *Id.* Phone cloning occurs when someone steals the embedded ID codes in a cell phones that identifies the user. *Id.* Those codes are then programmed into other cell phones and used illegally. *Id.* Criminals can use various technologies to clone phones including radio scanners that can intercept the codes while phones are in use by their legitimate owners. *Id.* Password sniffer programs monitor all traffic on certain parts of a network. *Id.* *See also* ICOVE, supra note 3, at 139. Sniffer programs collect all the data from the start of the network connection and look for encrypted account names and passwords being transmitted as part of this traffic. *Id.* Hacker software is often software that is used by legitimate computer programmers and network analysts used in a way to promote nefarious goals. *Id.*

[9] *See* Lawrence E. Bassham and W. Timothy Polk, *Threat Assessment of Malicious Code and Human Threats* (last modified Mar. 10, 1994) <http://www08.nist.gov/nistir/threats/ subsection3_4_2. html>. Some of the methods hackers use to gain access to computers are: password cracking, exploiting known security weaknesses, and network spoofing. *Id.* Password cracking is often simple to do because users often choose easily guessed passwords. *Id.* *See also* Am. Tel. and Tel. Co. v. Jiffy Lube International 813 F. Supp. 1164, 1165 (D. Md. 1993). For example, Jiffy Lube installed a telephone system with a remote

hackers use to infiltrate networks become as advanced as the newest technology and are always improving.

Another high profile computer crime occurred on September 13, 1998, when The New York Times was broken into by computer hackers who committed over $1 million worth of damages.[10] Fortunately, through the advent of modern technology, there are many methods which companies can utilize to make their networks more secure.[11] Unfortunately, many companies do not take appropriate measures to ensure the safety and security of their computer network.[12] Companies almost always hold information that is not only valuable to itself, but to others, such as payrolls or claims processing, handling shipping and deliveries for other companies, and credit card numbers.[13] It is also common for companies to sell this information to other companies.

On May 4, 2000,[14] a computer virus known as "the love bug"

access feature, by which an off-site caller could make long distance phone calls by using an unpublished 800 number and imputing a code. Jiffy Lube chose the code "Lube." *Id.* Hence, Jiffy Lube became liable for $55,727.39 of unauthorized calls that were made on their line. *Id.* Hackers can exploit known security weaknesses through configuration errors and security bugs. Bassham & Polk, *supra*. Configuration errors occur when the system allows unwanted exposure, i.e. makes the contents of a file system available to all other systems on the network. *Id.* Security bugs occur when unexpected actions are allowed on the system because of a loophole in an application program. *Id.* Network spoofing is accessing a network by an unauthorized system impersonating an authorized one. *Id.*

[10] *See* John Vranesevich, *Loan Gunman=HFG?* (last modified Sept. 15, 1999) <http://www.antionline.com/cgi-bin/News?type=antionline&date+09-13-1999&story+loan.news>. The attack on The New York Times falls one year almost to the day from the date the Nasdaq was broken into. *Id.*

[11] *See* Icove, *supra* note 3, at 134- 35.There are many different ways to protect communications; such as: access control, cryptographic methods, firewall technology, and various physical measures. *Id.* One of the most common methods of controlling access to networked computers is through the use of a password. *Id.* Knowledge of password is crucial, because whoever presents the correct password is granted access. *Id.* Easily guessed passwords provide little protection. *See generally*, Am. Tel. and Tel. Co. v. Jiffy Lube, 813 F. Supp. 1164. Another method of protection is cryptography. *Id.* Data is encrypted, or scrambled so as to be meaningless to anyone who does not have the key to decrypt it. *Id.* A Firewall is a buffer between any connected public networks and a private network. *See also* Kevin Downs et. al., Internetworking Technologies Handbook 752 (1998). It is hardware and software that provides a barrier between an internal network and an external network such as the Internet. *Id.* Firewalls control all incoming and outgoing communications. *Id.* Andrew R. Basile, Jr. et. al., Online Law 34 (Thomas J. Smedinghoff, ed., Software Publishers Ass'n 1996). Communications between computers are first relayed to the firewall before reaching the intended recipient. *Id.* Physical measures to protect communications include acts as simple as locking the server in a room. *Id.*

[12] *See* Basile, *supra* note 11.

[13] *See* Lance Rose, Netlaw Your Rights in the Online World 142 (1996). Because companies hold information for other companies they must be concerned for their safety as well as their own. *Id.*

[14] *'Love' Ain't Grand: New E-Mail Bug Wreaks Havoc*, Chi. Trib., May 5, 2000, *available in* 2000 WL 3662597.

wreaked havoc on computers all over the world to a tune of $15 billion in damages, infecting at least 14 United States Federal Agencies,[15] including the Pentagon, the Central Intelligence Agency, Congress and private companies such as Microsoft, and Dow Jones & Co.[16] The virus spread by way of an attachment that when opened, sent itself to all addresses in the user's Microsoft Outlook address book.[17] Essentially, the virus is transferred through the attachment, so if the attachment is deleted, the virus is deleted as well.

This comment will address the issue of liability for monetary losses in the event that a company's computer network or multifaceted phone system is violated. It will also explain what duty of care companies have to maintain a secure system. In addition, this comment will alert the reader to some of the newest technologies available to companies in order to protect their networks, including: encryption, firewalls and virtual private networking. Recognizing that oftentimes the real victim of an attack is someone other than the company itself, this comment will propose a model statute for states to adopt to protect these third-party victims. A proposed clause for use by company contracts providing a safeguard for the computer networks of all involved is also included. Lastly, this comment will suggest that the increased use of insurance to protect online and network environments is a desirable solution to the problem of liability.

II. BACKGROUND

A. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("The Act") was designed to protect government computers, and other computers whose use carries a high fiduciary duty, against any unauthorized access.[18] Computers that are not used by banks, credit unions, credit card insurers, consumer reporting agencies, or the United States government are still protected if the unauthorized conduct involves an additional element such as the obtaining of information and that it involved interstate or foreign commu-

[15] *Computer Virus Hits 14 Agencies*, Chi. Trib., May 10, 2000, *available in* 2000 WL 3664345.

[16] *'Love' Ain't Grand: New E-Mail Bug Wreaks Havoc, supra* note 14.

[17] *See Id.*

[18] 18 U.S.C. § 1030(a)(2) (1996).

> Whoever intentionally access a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution. . .or contained in a file of a consumer reporting agency on a consumer. . .information from any department or agency of the United States. . .

Id.

nication.[19] However, The Act is primarily aimed at protecting government computers.

The Act imposes a criminal penalty for up to twenty years, for repeat crimes or those involving government security, or a fine or five years imprisonment for offenses against non-government computers.[20] Interestingly, The Act has undergone several changes since it was enacted in 1984.[21] One of these changes included, a lowering of the *mens rea* requirement.[22] This bar establishing the required mental state for the crimes was lowered as a result of pressure on Congress to punish the new forms of crime occurring on the Internet.[23] Internet crime is a serious issue because its harm exceeds monetary damages.

In *United States v. Morris*,[24] a Cornell graduate student, in an effort to illustrate how quickly a computer virus can spread, created a program called a "worm" and released it on the Internet.[25] The worm spread faster than he had expected and it caused considerable damage at many locations all over the country.[26] While it was evident that Morris did not intend to cause any damage, he did intend to access computer systems without authorization.[27] The court held that Morris' actions, merely accessing the other computers, was sufficient to hold him liable for damages.[28]

Ironically, The Act punishes authorized users who *unintentionally*

[19] *See* 18 U.S.C. § 1030(a)(2) (1996) (protecting computers if the information obtained by the conduct results from involvement in interstate or foreign communication).

[20] *See* 18 U.S.C. (c) (1996).

[21] *See* Haeji Hong, Note, *Hacking Through the Computer Fraud and Abuse Act,* 31 U.C. DAVIS L. REV. 283, [repaginated by author (copy on file with author)] n.7 (1997). Since its enactment in 1984, Congress has attempted to increase its effectiveness by changing it several times. *Id.*

[22] *Id.* at 10. *See also* BLACK'S LAW DICTIONARY 985 (6th ed. 1990). Mens rea is an element of criminal responsibility, a guilty or wrongful purpose, guilty knowledge and willfulness. *Id.*

[23] *See* Hong, *supra* note 21 at n.7.

[24] 928 F.2d 504, 505 n.1 (2d Cir. 1991).

[25] *See Id.* "A 'worm' is a program that travels form one computer to another but does not attach itself to the operating system of the computer it 'infects.'" *Id.* "It differs from a "virus," which is also a migrating program, but one that attached itself to the operating system of any computer that uses files from the infected computer." *Id.*

[26] *See id.* at 506.

[27] *See id.* at 506-07. Morris had completed his undergraduate work at Harvard and had acquired significant computer experience and expertise. *Id.* The program he developed was designed to demonstrate the inadequacies of current security measures. *Id.* The worm Morris created was supposed to occupy little computer operation time and not interfere with normal use of computers. *Id.* Also, Morris' attempts to kill the worm after it was evident that it was causing damage indicate that he did not intend to do any harm. *Id.*

[28] *See id.* at 509. The court found that The Computer Fraud and Abuse Act that Morris was prosecuted under only required that he "knowingly" accessed a computer and not that he intended to damage the computer. *Id.*

do damage,[29] but does not punish authorized users who *intentionally* do damage.[30] In *Briggs v. Maryland*,[31] a disgruntled ex-employee allegedly placed passwords[32] on many of the computer files at his former office, and then placed those passwords in a directory entitled, "ha-ha-he-he."[33] The decision recognized that current and former employees, like the damage done by the ex-employee in this case, cause much economic loss resulting from computer abuse.[34] However, the court looked to the legislative history of The Act and determined that Congress did not intend to punish those who had authorization to access computers, only those who accessed the computers without authorization.[35]

There is a civil cause of action created under The Act.[36] The Act provides that any person who suffers damage or loss because of a violation may maintain a compensatory damages claim and may be awarded injunctive relief or another equitable relief, but The Act does not specify the other equitable remedies that are permitted.[37] Interestingly, The Act specifically states that "any person" may maintain an action for damages, but The Act does not mention whether Congress intended the term "person" to apply to corporations, businesses, or other injured organizations.[38]

B. State Law Punishing Unauthorized Access or Use

Every state, except Vermont, has a criminal statute prohibiting unauthorized access or use of a computer.[39] Some states, however, only prohibit the unauthorized use of a computer and not access. Those states that prohibit the unauthorized access to a computer usually have

[29] *See* U.S. v. Morris, 928 F.2d at 509.

[30] *See* Briggs v. Maryland, 704 A.2d 904, 910 (Md. 1998).

[31] *Id.* at 905.

[32] *Id.* "A password is the most common form of user authentication and it is used to prevent unauthorized access to a computer system." *Id.* at 905 n.2. "It is a sequence of characters that one must enter prior to obtaining access to a computer." *Id.*

[33] *Id.* at 906. The plaintiff was a securities investment company who entrusted the defendant to program and design software to maintain the company computer system. Id. He was in charge of maintaining the entire computer system. Id.

[34] *See id.* at 908 n. 5 citing National Institute of Justice Computer Crime: Criminal Justice Resource Manual xvi (2d ed. 1989) "Scholars have noted that serious economic loss linked to computer abuse is caused by current and former employees rather than by outsiders." *Id.*

[35] *See id.* at 910.

[36] *See* 18 U.S.C. § 1030 (g) (1996). "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. . ." *Id.*

[37] *Id.*

[38] *Id.*

[39] *See* Briggs v. Maryland, 704 A.2d at 908. The federal government, all of our sister states except for Vermont, have computer crime statutes. *Id.* 18 U.S.C. § 1030 (1994).

a requirement that the access be willful or intentional, thus protecting the employee who accidentally deletes or modifies a program while attempting to fix a problem, or deletes a program upon her employer's orders.[40] If willful intent were not required, it would be possible to hold employees criminally liable for their inadvertent acts.

In Illinois, the term access is defined as "to use, instruct, communicate with, store data in, receive or intercept data from or otherwise utilize any services of a computer."[41] Statutes that protect computer users from unauthorized use or access have been paralleled to those statutes that prohibit the breaking and entering of an intruder to an individual's home.[42] The severity of the damage done to your computer data, like an individual's home, indicates what punishment is due.[43] Mere access to a computer under most state law is a misdemeanor.[44]

C. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA") prohibits a third-party from intercepting or disclosing electronic communications, in the same way that federal wiretapping laws prohibit the interception of telephone calls.[45] The ECPA also prohibits unauthorized access to, and disclosure of, stored electronic communications such as voice mail and e-mail.[46] Under the ECPA, accessing another's e-mail without that indi-

[40] *See* Basile, *supra* note, 11 at 478.

[41] 720 Ill. Comp. Stat. 5 / 16D-2(e) (West 1999).

[42] *See* Basile, *supra* note 11 at n.34 (citing Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 Jurimetrics, J. 3 (Fall 1994)).

[43] *See id.*

[44] *See* Black's Law Dictionary 999 (6th ed. 1990). A misdemeanor is a lesser offense than a felony and is generally punishable by a fine, penalty, forfeiture or jail sentence for less than one year. *Id.*

[45] 18 U.S.C. § 2510 (1970). Some of the definitions used by the Electronic Communications Privacy Act are:

> (1) 'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception. . .
>
> (5) 'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral communication through the use of any electronic communication. . .

Id.

[46] 18 U.S.C. § 2701 (1996). E-mail enables an individual to send an electronic message, like a note of letter, to another individual or to a group of addresses. *Id.* Reno v. American Civil Liberties Union, 117 S. Ct. 2329 (1997). The message is generally stored electronically and waits for the recipient to check her "mailbox." *Id.* It also alerts the recipient of its arrival by some sort of prompt. *Id.* *See generally,* Thomas R. Greenberg, *E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute,* 44 Am. U. L. Rev. 219 (1994) (discussing employer monitoring of employees by e-mail and voice mail); *see also*

vidual's consent constitutes a criminal violation,[47] just like reading another's post office mail. The ECPA also provides that, if person intercepts an e-mail message that she knows, or has reason to know, was begot by unlawful means, it is a felony offense.[48] However, this is not an absolute truth. Merely looking at a computer screen with an e-mail message on it,[49] or pressing a button on a pager and observing the telephone numbers[50] does not offend the EPCA.

However, The EPCA does not extend to purely internal e-mail systems.[51] The EPCA (Section 2701)[52] prohibits intentionally gaining unauthorized access to an electronic communications facility, service facility, or merely exceeding authorized access to such a facility.[53] The ECPA also bars unauthorized persons from hacking another's directories, files, or other prohibited areas of the system.[54]

D. Attempts to Apply Contract Principals to Hacker Attacks

In its simplest terms, contract law is based on an agreement between two or more persons that creates an obligation to do, or not to do, a particular thing.[55] Contracts can be express, as in the above example,

Joel Cohen and Michele Pahlmer, *Criminality Beware: Computers Have Long Memories,* 215 N.Y.L.J. 1 (1996); Mary Frances Lapidus, *Using Modern Technology to Communicate with Clients: Proceed with Caution and Common Sense,* 34 Hous. Law 39 (1996).

[47] 18 U.S.C. § 2701(b)(1)(A) (1999). If one intentionally access another's e-mail or other electronic communication, for the purpose of commercial advantage, malicious destruction or damage, or private financial gain, the punishment could be a fine or imprisonment for not more than one year or both. *Id.*

[48] *See* Jonathan Rosenoer, CyberLaw 171 (1997) (citing 18 U.S.C. §2511(1)(d)).

[49] *See* Wesley College v. Pitts, 974 F.Supp. 375, 384 (D. Del. 1997). "The EPCA defines 'intercept' as the 'acquisition' of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* The court held that a computer screen was only the medium for the information, not an intermediary used to receive the information. *Id.*

[50] *See* United States v. McLeod, 493 F.2d 1186, 1188 (7th Cir. 1974).

[51] *See* 18 U.S.C. § 2701 (1999). The Electronic Communications Act does not specify which types of e-mail or other electronic communication it covers, however, it is a federal statute that is not attached to the spending power and so is dependant on the commerce clause for power. *Id. See also* U.S. Const. Art. I § 8. The commerce clause allows the federal government "to regulate commerce among the several states." *Id.* Hence, The Electronic Communications Act can only govern over communications within the stream of commerce as prescribed by the commerce clause. *Id.*

[52] 18 U.S.C. § 2701 (1999).

[53] *See id. See also* Rosenoer, *supra* note 48 at 172. Rosenoer believes that the ECPA would not bar a person from accessing a file placed on a public area such as a FTP, gopher, or World Wide Web directory. *Id.* Rosenoer warns that system administrators should not leave important files such as encrypted passwords in a pubic area. *Id.*

[54] *See id.*

[55] *See* Black's law dictionary 322 (6th ed. 1990). "A contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the

implied, or inferred by the conduct of the parties.[56] An implied contract is not created by the explicit agreement of the parties, and can only exist if there is no express contract.[57] It can be created through an inference of law, as a matter of reason and justice from the party's acts or conduct,[58] through the circumstances surrounding the transaction, if these circumstances make it reasonable, or based on the assumption that a contract existed between the parties by tacit understanding.[59]

Privity to the contract is an essential element that must be met to establish a binding, valid contract. Privity is a mutual or successive relationship to the same right of property, or an identification of the interests of both parties representing the same legal right.[60] Privity to a contract is a relationship between parties, out of which there arises some mutuality of interest.[61] Consumers are barred from making successful claims against businesses for losses due to hackers because there is a lack of privity between the businesses and the consumers.[62] For exam-

law in some way recognizes as a duty." *Id.* *See also* RESTATEMENT (SECOND) OF CONTRACTS § 3.

[56] *See* BLACK'S LAW DICTIONARY 323 (6th ed. 1990). It is an agreement which legitimately can be inferred from intention of parties as evidenced by circumstances and ordinary course of dealing and common understanding of men. *Id.*

[57] *See* Chem-Tronix Lab v. Solocast Co., 258 A.2d 110, 113 (Con. Cir. Ct. 1968). Implied contracts are not expressed in words. *Id.* They arise when a plaintiff, without being requested to do so, renders services under circumstances indicating that she expects to be paid, and the defendant, knowing such circumstances, avails herself of the benefit of those services. *Id.*

[58] *See* Carroll v. Lee, 712 P.2d 923, 926 (Ariz. 1986). In Carroll, a woman sued her excohabitant for some real and personal property they obtained during their fourteen years together. *Id.* at 925. The court found that an implied contract existed between the parties. *Id.* at 928. While the contract was not in writing, it "was assiduously and scrupulously adhered to by both parties." *Id.* at 925. Together they had acquired property and placed title of it in both of their names. *Id.* The court found that the parties had agreed to an arrangement where Judy would stay at home and take care of the household duties and Paul would work as a mechanic. *Id.* Even though the duties between them were different, the court held that was of no consequence. *Id.* at 926. "Any performance which is bargained for is consideration." *Id.*

[59] *See id.*

[60] *See* Petersen v. Fee Intern., Ltd., 435 F.Supp. 938, 942 (D. C. Okl 1974).

> [P]rivity is a word with many meanings and only some of the meanings express the relationship which must exist between a defendant and a third-party is to be held in contempt for doing the act which the defendant is prohibited to do. . . privity is not established merely because persons are interested in the same question or in proving the same set of facts or because the question litigated is one which might affect such other person's liability as a judicial precedent in a subsequent action.

Id.

[61] Howarth v. Pfeifer, 443 P.2d 39, 43 (Alaska 1968).

[62] *See* David L. Gripman, *The Doors are Locked But the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem,* 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 177-78 (1997).

ple, if a hacker violates Company A by means of Company B's lax security, A does not have a claim against B because no privity of contract exists.[63] The requirement of privity can be waived by statute if equity so dictates, as in sales law.[64] Crimes involving computers can be extremely costly to fix.[65] Most states provide for a civil remedy against the computer hacker for such losses.[66] However, most hackers do not have the resources to pay a judgment against them.[67]

There exists a strong need to create liability for companies who do not maintain adequate security on their computer networks.[68] While the imposition of a strict duty of care is unfair, state legislatures should add a civil liability provision providing for suit when companies or individuals have not maintained a reasonably safe computer network resulting in harm to those individuals or businesses harm.

III. ANALYSIS

A civil remedy addressing the needs of computer hacker victims is essential to compensate for the currently inadequate legal remedies. Contract and tort law are not amenable for use by victims of computer hackers, thus these victims remain injured. Generally, contract law requires that the parties to the suit be in privity of contract.[69] The injured party most often lacks privity of contract and has no recourse in tort for her financial damages. Under the economic loss doctrine, damages that

[63] *See id.* The author states that in this scenario, corporation A is harmed without the ability to sue corporation B for the damages it incurred because of the prohibition of using tort law in cases involving purely financial damages. *Id.* Further, the author argues that tort law concept of negligence is appropriate in this situation and that corporations should exercise due care in protecting their computer networks against attack by hackers. *Id.*

[64] *See, e.g.,* U.C.C. § 2-318. A seller's warranty whether express or implied extends to any natural person who is in the family or household of his buyer or who is a guest in his home it is reasonable. *Id.* A seller may not exclude or limit the operation of this section. *Id.*

[65] *See Internet Security Alert,* PC/COMPUTING, June 1999, available in Infotrac A54555964. Cybercrime is taking a bottom-line toll on the corporate workplace. *Id.* Last year, losses exceeded $100 million—and that figure continues to skyrocket as security as security breaches pose an increasing threat to U.S. corporations, banks and even the government. *Id.*

[66] *See* 18 U.S.C. § 1030 (g) (1996).

[67] *See* Bruce Sterling, *supra* note 1. Hackers are mostly young suburban American white males. *Id.* at 5.

[68] *See id.*; *see also* GUISNEL supra note 5, at 111.

[69] *See* Downriver Internists v. Harris Corp., 929 F.2d 1147, 1149 (6th Cir. 1991). In Downriver Internists, a medical partnership sued the purchaser of computer hardware and software for breach of warranty when it failed to operate to their satisfaction. *Id.* at 1149. The court decided that the suit was actually a breach of contract action for economic losses, and as such, the privity requirement must still be met. *Id.*

are purely financial are not recoverable in tort.[70] Therefore, tort law is also an unavailable remedy since the injured party has suffered only monetary losses.[71] It is essential to create a civil remedy for these injured parties by enacting a statute.

It is necessary, therefore, to examine the economic loss doctrine and its application to the loss suffered as a result of computer hackers.[72] A discussion of the requirement of privity of contract to establish a claim under contract law is also warranted.[73] A proposed contract clause businesses can include to protect themselves against computer hackers is provided.[74] A model statute for states to adopt promoting the protection of the interests of computer and telecommunications users is proposed.[75] Finally, this comment suggests steps corporations and businesses may take to protect themselves and their customers by insuring their networks.[76]

A. The Economic Loss Doctrine

The economic loss doctrine[77] is a rule that prohibits parties from recovering monetary losses, absent injury to person or property, under tort law.[78] Moreover, it bars recovery for a defective product when there

[70] See Seely v. White Motor Co., 403 P.2d 145, 151 (Cal. 1965). *See also* CSY Liquidating Corp. v. Harris Trust and Sav. Bank 162 F.3d 929 (7th Cir. 1998). In CSY, a bank sold a debtor-company's eight million dollar promissory note to debtor's competitor resulting in sale of that debtor's assets to his competitor. *Id.* at 932 The debtor then brought suit against the bank alleging breach of fiduciary duty and with the tort of negligent interference with a contract. *Id.* Justice Posner, writing for the court held that the "doctrine of economic loss rules out recovery for such indirect losses—losses for example when a store is burned down by the negligence of a third-party." *Id.* at 932. A tort may have indirect consequences that are beneficial—for example, to competitors of the store that was burned down, they may receive more benefits from it, which the other store owner can not sue for. *Id.*

[71] *See id.* at 932.

[72] See infra Part III.A.

[73] See infra Part III.B.

[74] See infra Part III.D.

[75] See infra Part III.F.

[76] *Id.*

[77] Moorman Mfg. Co. v. Nat'l Tank Co., 435 N.E.2d 443, 449 (Ill.1982). "Economic loss" has been defined as "damages for inadequate value, costs of repair and replacement of the defective product, or consequent loss of profits- without any claim of personal injury or damage to property. " *Id.* Economic loss has also been defined as the lesser value of the product because it does not function properly for the purpose it was designed and sold. *Id.*

[78] *See* Seely v. White Motor Co., 403 P.2d 145,151 (Cal 1965); *see also* Moorman Mfg. Co. v. Nat'l Tank Co., 435 at 449; *but see* Regents of the Univ. of Minn. v. Chief Indust., 106 F.3d 1409 (8th Cir. 1997) In Regents, the University decided to purchase a new grain dryer for one of its stations. *Id.* at 1410. Seven years later when it started a fire, the University sued the maker of the grain dryer. *Id.* The court held that the University was a merchant

is no personal injury involved.[79] The rationale behind this doctrine is that contract law is better suited than tort law to address the needs of the parties.[80] Essentially, parties enter into an agreement and create a document that reflects the most favorable terms for themselves.[81] Parties agree upon a contract that reflects their needs and anticipates losses or problems that may occur during the contract term.[82] For example, a buyer and seller are free to negotiate their own warranties to protect each party from harm by the other party.[83] If parties were permitted to sue in tort for monetary losses, they could bargain without regard to potential problems, and the resulting losses would be entirely placed on the manufacturer or the seller.

Contract law and tort law are distinguishable in that contract law rests on obligations imposed by bargain, and tort law rests on obligations imposed by law.[84] The economic loss doctrine is an effort to maintain this distinction thereby preventing "contract law from drowning in a sea of tort."[85]

under the Minnesota statute equivalent to the U.C.C. in order to manuever around the harsh effects of the economic loss doctrine. *Id.*

[79] *See* Seely v. White Motor Co., 403 at 151.

> The distinction that the law has drawn between tort recovery for physical injuries and warranty recovery for economic loss is not arbitrary and does not rest on the 'luck' of one plaintiff in having an accident causing physical injury. The distinction rests, rather, on an understanding of the nature of the responsibility a manufacturer must undertake in distributing his products. He can appropriately be held for physical injuries caused by defects by requiring his goods to match a standard of safety defined in terms of conditions that create unreasonable risks of harm. He cannot be held for the level of performance of his products in the consumer's business unless he agrees that the product was designed to meet the consumer's demands.

Id.

[80] *See* Moorman Mfg. Co. v. Nat'l Tank Co., 435 at 450. Tort law is best applicable to situations where personal injury arises "from a sudden or dangerous occurrence." *Id.* "The remedy for economic loss, loss relating to a purchaser's disappointed expectations due to deterioration, internal breakdown or non-accidental cause , on the other hand, lies in contract." *Id.*

[81] *See generally*, Budgetel Inns v. Micros Systems, 8 F.Supp.2d 1137, 1142 (E.D. Wis. 1998) (discussing that by creating their own terms in their agreement, the parties to a contract can encourage the party best suited to assess the risk of economic loss, to assume, allocate, or insure against the risk). *Id.*

[82] *See id.*

[83] *See id.*

[84] *See id.* "While contract law seeks to hold commercial parties to their promises, ensuring that each party receives the benefit of their bargain, tort law protects society's interest in human life, health, and safety." *Id.*

[85] East River S.S. Corp. v. Transamerica Delavai, 476 U.S. 858, 859 (1986). In East River, a shipbuilder contracted with a turbine manufacturer to design, build, construct and supervise the installation of turbines that would be used as the main propulsion units for four oil-transporting supertankers. *Id.* at 860. After construction, the ships were sent to the turbine manufacturers. *Id.* Due to a design defect, all ships malfunctioned, but only

Economic injuries are contractual in nature when they involve the sale of a product, and are best left to contract law principles.[86] The seminal case for the economic loss doctrine is *Seely v. White Motor Co.*[87] In *Seely*, a defective truck overturned but did not injure anyone or anything but itself.[88] The owner sued on grounds of strict liability and breach of

the products themselves were damaged. *Id.* Justice Blackmun held that in admiralty law, regardless if the plaintiff alleges negligence or strict liability, no products-liability claim lies when the product in question only injures itself, and results in purely economic damages. *Id.*

[86] *See e.g., Moorman*, 435 N.E.2d at 445. In *Moorman*, the plaintiff purchased a grain storage tank from the defendant. *Id.* When a crack developed in the tank, the plaintiff filed suit seeking to recover for the losses incurred in repairing the tank as well as for consequential losses related to the lost use of the tank. *Id.* The plaintiff sued under the theories of strict liability, negligence, and misrepresentation. *Id.* The court held that the losses claimed were economic and therefore the plaintiff was barred from recovery in tort. *Id. But see* In The Matter of the Complaint of Nautilus Motor Tanker Co., 900 F. Supp. 697, 699 (D. N.J. 1995). In *Nautilus*, the vessel owner Nautilus attempted to limit or exonerate his liability for an oil spill caused by his vessel. *Id.* The court found Nautilus to be 100% responsible for the grounding and oil spill. *Id.* The *Nautilus* court cited People Express Airlines v. Consolidated Rail Corp., 495 A.2d at 701, and opined that "abandoning the physical harm requirement for recovery of economic losses 'discourages others from similar tortious behavior. . .vindicates reasonable conduct that had regard for the safety of others, and ultimately shifts the risk of loss and associated costs of dangerous activities to those who should be and are best able to bear them.'" *Id. See also* North Am. Chem. Co. v. Superior Court of L.A. County, 69 Cal. Rptr. 2d 466, 467 (Ct. App. 1997). The North American Chemical Company sought a writ of mandate to compel the restoration of a cause of action in negligence against Harbor Pac a packaging company. *Id.* According to North American, Harbor Pac had negligently packaged its product in such a way as it became contaminated. *Id.* Even though North American claimed only economic loss, the court held that the "packaging and shipping contract with Harbor Pac imposed a duty on Harbor Pac which required it to reasonably and carefully perform its contractual obligations." *Id.* The court found that the economic loss rule did not apply because the loss was foreseeable. *Id. But c.f.* Squish La Fish v. Thomco Specialty Products 149 F.3d 1288 (11th Cir. 1998) In *Squish*, the plaintiffs had purchased adhesive to affix their product to cardboard for packaging. *Id.* The plaintiffs, Squish La Fish, used the adhesive on about 8,600 of their 10,000 units and the adhesive could not be removed. *Id.* The adhesive had to be removed by soaking in mineral oil. *Id.* Thirty percent of all products sold were returned due to the glue and oily residue from the mineral oil. *Id.* Plaintiff filed suit against Thomco alleging negligence in recommending the wrong adhesive. *Id.* They sought damages for lost profits from their other contracts for sales of their products. *Id.* The court held that the economic loss doctrine was not applicable, but still disallowed the plaintiffs to recover. *Id.*

[87] *See* Seely v. White Motor Co., 403 P.2d 145,151 (Cal 1965). In *Seely*, Judge Hand recognized the distinctions between the law of sales and the law of tort. *Id.* at 148. "The history the doctrine of strict liability in tort indicates that it was designed, not to undermine the warranty provisions of the sales act or of the Uniform Commercial Code, but, rather, to govern the distinct problem of physical injury." *Id.*

[88] *See id.* at 147. Apparently, the truck had been malfunctioning from the date the owner took possession. *Id.* It "bounced violently," in a process known as "galloping." For eleven months the owner made attempt to repair the truck with the help of the manufacturer, to no avail. *Id.* Judge Traynor noted that when the warrantor repeatedly fails to

express warranty.[89] However, Justice Traynor refused to allow recovery because the plaintiff had suffered only monetary loss and not physical injuries.[90] Likewise, in *Dakota Gasification Co. v. Pascoe Building Systems*,[91] the owner of an oxygen plant was denied monetary damages when part of the oxygen plant's roof caved in due to a faulty weld.[92] Even though property that was not connected to the plant itself was damaged, the court held that the damage was within the bargainer's contemplation at the time they negotiated the contract.[93]

The computer user and the telecommunications user are most likely not in a position to bargain for or create warranties with the companies who control the information industries.When an individual user suffers a loss due to a hacker, that individual will have to utilize contract law for a remedy against the company, often the individual becomes responsible for all unauthorized charges made on their account.[94] If the user has no

correct the defect as promised, it is liable for the breach of that promise as a breach of warranty. *Id.* at 148.

[89] *See id.*

[90] *See id.* at 151. Justice Traynor stated that:

> [a] consumer should not be charged at the will of the manufacturer with bearing the risk of physical injury when he buys a product on the market. He can, however, be fairly charged with the risk that the product will not match his economic expectations unless the manufacturer agrees that it will.

Id.

[91] 91 F.3d 1094, 1097 (8th Cir. 1996).

[92] *See id.* In *Dakota*, several pipeline companies formed the ANG Coal Gasificaiton Company and contracted with J. Kaiser Company for construction of a federally funded $2 billion synthetic natural gas production plant. *Id.* at 1096. It was to be one of the largest synthetic natural gas plants in the world and the only one in the United States. *Id.* Kaiser subcontracted to Lotepro for labor, material and equipment, Loetpro then subcontracted with Del Con to furnish the metal building that would enclose the oxygen plant. *Id.* During construction, one of the parties noticed that some of the welds were defective. *Id.* It was decided that Pascoe would mend the defective welds by welding hundreds of steel plates over them. *Id.* Eight years after the defective welds were mended, and after several inspections, a part of the roof collapsed. *Id.* at 1097. *See also,* Cloverhill Pastry-Vend Corp. v. Continental Carbonics Prods. 574 N.E.2d 80 (Ill App. Ct. 1991) (noting that metal chips were found in baked goods as a result of defendant's dry ice machine). Dixie- Portland Flour Mills v. Nation Enters. 613 F.Supp. 985 (N.D. Ill. 1985) (noting that sand was added to the flour that was used to prepare pizzas).

[93] *See Dakota*, 91 F.3d at 1099. *But see Seely*, 403 P.2d at 151. The economic loss doctrine generally applies to strictly monetary losses and to personal or property injury, excluding the item in question. *Id.* The court in Dakota reasoned that the economic loss doctrine, is better suited to contract law, utilizing the law of warranty, because it permits the parties to specify the terms of their bargain and protect themselves from commercial risk. *Id.*

[94] *See e.g.*, A.T. & T. v. Fleming and Berkley 131 F.3d 145 (9th Cir. 1997) (Unpublished decision) (noting $35,636.82 worth of unauthorized calls were attributed to a law partnership); *see also* American Message Ctr. v. FCC, 50 F.3d 35 (D.C. Cir. 1994). F.C.C. refused to force Sprint to forgive $160,000 worth of unauthorized long distance telephone calls charged to plaintiff. *Id.* A.T. & T. Corp. v. Community Health Group, 931 F.Supp. 719

agreement with the company or relation to the company (no privity), then the individual has no contractual recourse. Without privity, this user will be barred from bringing a tort claim against the company since the economic loss rule disallows the awarding of damages to a party that has only suffered monetary loss. A victim of a hacker attack, under the Computer Fraud and Abuse Act ("CFAA"), has recourse only against the hacker himself, not the company.[95] As a result, it is imperative that a law be enacted to hold companies responsible thereby protecting victims of computer hackers and providing them with a remedy.

B. Privity of Contract

Privity of contract was a prerequisite to establish legal responsibility at common law.[96] Courts required that a nexus exist between the buyer and seller of goods.[97] It was a way of limiting a storekeeper's liability to only those to whom he had a contractual duty.[98] There are several theories explaining how the privity doctrine was developed; however, it evolved to a theory raised in cases after 1670.[99] Dean Prosser suggests that the privity doctrine was developed to bolster the En-

(S.D.Cal. 1995) (noting over $80,000 worth of unauthorized calls charged to health care entities); A.T. & T. v. Jiffy Lube Int'l, 813 F.Supp 1164 (D. Md. 1993) (noting $55,727.39 charged to Jiffy Lube after its phone system was hacked); A.T. & T. v. New York City Human Resources Admin., 833 F.Supp. 962 (S.D.N.Y.) (noting that $537,506.64 of unauthorized phone calls were charged to the city of New York and A.T. & T. asked for $529,000 of that amount); Thrifty-Tel v. Bezenek 46 Cal.App.4th 1559 (Cal. Dist.Ct. App. 1996) (noting that $33,720 was awarded to a long-distance telephone service provider under a trespass to chattels theory, when teenagers did not manage to complete any long distance calls, but merely tied up the phone lines).

[95] *See* 18 U.S.C. § 1030(g).

[96] *See* Steven Bonnano, *Privity, Products Liability, and UCC Warranties: A Retrospect of and Prospects for Illinois Commercial Code §2-318*, 25 J. Marshall L. Rev. 177, 178 (1991).

[97] *See id.*

[98] *See id.*

[99] *See* Vernon V. Palmer, *The History of Privity—the Formative Period (1500- 1680)*, 33 Am. J. Legal Hist. 3 (1989). Between 1500- 1680, the number of suits won by the beneficiary was enormous because the modern doctrine of privity had not been established. *Id.* at 5Palmer, offers four theories explaining how the doctrine of privity developed: (1) the interest theory, 2) the benefit theory, (3) the agency cases and (4) the consideration theory. *Id.* at 5- 6. First, the interest theory's rationale is that if non-performance of the action caused an injury to his interest, he should receive compensation. *Id.* at 6. Second, the benefit theory, was associated with cases in which the party to whom the benefit of a promise accrues may bring the action. *Id.* at 22. Third, the agency cases, "reveal that potential privity objections were avoided by the notion that the legal persona of the agent merged into that of his principal." *Id.* at 6. Fourth, the consideration theory came about after the interest and benefit theories were replaced or absorbed and relief for the beneficiary was curtailed at common law. *Id.* at 7, 38. It was considerably strict, and dealt with a specific group of cases involving collections of debts. *Id.* at 38.

glish Industrial Revolution.[100]

Later, privity of contract would become essential for establishing legal responsibility for injury by a seller of goods.[101] When the United States adopted the common law, the doctrine of privity of contract was included.[102] While many courts still adhere to strict privity requirements, through the years, other courts and some statutes have attempted to lessen the harshness the requirement of privity can bring.[103] The privity doctrine is still widely used in computer related cases.

The privity doctrine is formally defined under the Uniform Commercial Code, the ("U.C.C.") which has developed three multiple choice options for states to pick when adopting a warranty provision expanding the privity doctrine for the sale of goods.[104] However, it has not yet been

[100] *See* Bonnano *supra* note 96, at 178 (citing W. PAGE KEETON, PROSSER AND KEETON ON THE LAW OF TORTS § 53, at 357 (5th ed. 1984)). Prosser argues that "courts sought, perhaps more or less unconsciously, to limit the responsibilities of growing industry within some reasonable bounds." *Id.*

[101] *See* Bonnano, supra note 96, at 179.

[102] *See id.*

[103] *See e.g.* U.C.C. § 2-318 (1992); *See also*, Petersen v. Fee Inter'l, 435 F.Supp. 938 (N.D. Okla 1975). In *Peterson*, the plaintiffs sued the defendants for patent infringement, false marking and unfair competition. *Id.* at 939. The court discussed the "privity" and reasoned that it is a word with many meanings and that only some meanings express the relationship which must exist between a defendant and a third-party if the third-party is to be held in contempt for doing the act which the defendant is prohibited to do. *Id.* In its broadest sense, privity is defined as mutual or successive relationships to the same right of property, or such an identification of interest of one person with another as to the same legal right. *Id.* The meaning attached to the word privity in its use as a synonym for the instant parties is an identification of interest of one person with another as to represent the same legal right. *Id.* See also Squish La Fish v. Thomco Specialty Products, 149 F.3d 1288, 1291 (11th Cir. 1998). Georgia recognizes two exceptions to the economic loss rule: one, negligent misrepresentation and two, the "accident exception" which allows recovery when a "sudden and calamitous event not only causes damage to a product but also poses an unreasonable risk of injury to persons and property." *Id.* at 1291 n. 1.

[104] The Three Alternatives listed as A, B, and, C are as follows:

> A seller's warranty whether express or implied extends to any natural person who is in the family or household of his buyer or who is a guest in his home if is reasonable to expect that person may use, consume, or be affected by the goods and who is injured in person by breach of the warranty.
>
> U.C.C. § 2-318 (1992). Alternative A
>
> A seller's warranty whether express or implied extends to any natural person who may reasonably be expected to use, consume or be affected by the goods and who is injured in person by breach of warranty.
>
> U.C.C. § 2-318 (1992). Alternative B
>
> A seller's warranty whether express or implied extends to any person who may reasonably be expected to use, consume or be affected by the goods and who is injured by breach of the warranty. A seller may not exclude or limit the operation of this section with respect to injury to the person of an individual to whom the warranty extends.
>
> U.C.C. § 2-318 (1992). Alternative C

Id.

formally decided whether the definition of a "good" under the U.C.C. would include an Internet connection, a computer network, a series of files, a telephone call or e-mail.[105] While a defective software program may be a "good;"[106] a telephone call, e-mail, Internet connection or computer file may not fall under the definition. Therefore, the expansion of the privity doctrine through the U.C.C. is not amenable for use by the victim of a computer or telecommunications crime unless the term "good" encompasses information or the other computer related items such as an Internet connection, or a computer network.

C. The Privity Doctrine as Applied to the Computer Fraud and Abuse Act

The CFAA contains a provision that provides a civil action for damages arising out of its violation.[107] There are two important aspects of this clause; first, it states that "any person who suffers damage" may bring a civil action.[108] This is important because it does not limit the action to a person in privity of contract, it allows anyone who has suffered damage to bring suit.[109] However, the term "person" is not specifically defined to include other entities such as organizations and corporations.[110] Second, it only allows for compensatory damages in an action against the violator.[111] Hence, the CFAA clearly creates liability when an individual is harmed, but does not definitively give this same right to companies and other organizations. The CFAA needs to define "person" broadly to give companies the right to bring suit.

D. A Need for Accountability for Corporations that Maintain Substandard Computer Networks

No country in the world relies more on its computers than the

[105] *See* Blacks Law Dictionary 694 (6th ed. 1990). "It may include every species of personal property or it may be given a very restrictive meaning." *Id.* Thus, "good" is a term of variable content and meaning. *See also* U.C.C. § 9-105(h) (stating that the term "goods" includes such intangibles as unborn animals and growing crops). *See also* Blacks Law Dictionary 694 (6th ed. 1990) (providing yet another definition). All things which are movable at the time of identification to the contract for sale other than the money in which the price is to be paid are goods. *Id.*

[106] *See e.g.* Advent Systems Ltd. v. Unisys Corp., 925 F.2d 670 (3rd Cir. 1991); *see also* RRX Indus., v. Lab-Con, 772 F.2d 543 (9th Cir. 1985); *but see* Honeywell v. Minolta Camera Co., No. 87-4847 *available in* 1991 WL 841033 (D.N.J. July 19, 1991). *See also* Andrew Rodau, *Computer Software: Does Article 2 of the Uniform Code Apply?*, 35 Emory L.J. 853, 864-74 (1986).

[107] 18 U.S.C. §1030(g). *See generally,* Hong *supra* note 21and accompanying text.

[108] *See generally,* Hong *supra* note 21.

[109] *See id.*

[110] *See id.*

[111] *See id.*

United States.[112] Sensitive documents and information are contained on the hard drives of computers across the country.[113] For example, most every hospital stores sensitive patient information in computer databases, while schools maintain their students names, addresses, telephone and social security numbers, grade point averages and other private information on computer hard drives.[114] Additionally, banks utilize computer systems to contain the account balances of countless Americans and businesses.[115] Businesses hold information about sales transactions, billing, customer information, and credit card numbers in their computer systems.[116] In fact, information about almost every conceivable topic is stored on computers.[117]

Even more important than personal information, including an individual's employee records, tax returns, social security numbers, and other private information, is the national security information which is contained in government computers such as the Department of Defense, NASA, the Center of Disease Control, and the Federal Bureau of Investi-

[112] *See* William Cohen, *Preserving America's Privacy and Security In the Next Century: A Strategy for America in Cyberspace* (visited Sept. 26, 1999) <http://www.epic.org/crypto/legislation/cesa/report_9_16_99.html>. In a report to the President of the United States from the Office of the Press Secretary, the author writes that "the computer has and will continue to revolutionize virtually all aspects of American society, just as electricity, the power grid, and the railroad changed our forefathers' society." *Id.* Further, the report notes that the computer and its application in business, commerce, education and recreation has transformed the American economy. *Id.* America is becoming a country of "knowledge workers," with the ubiquitous application of computer technology at its core. *Id.* America's productivity is grounded in computer applications and networks. *Id.*

[113] *See generally* GUISNEL, *supra* note 5. Anyone who has received a monthly statement from the phone company knows how much personal information is contained in computers. *Id.* The statement tells who was called, the amount of time spent on the phone and the hour which we called. *Id.* The Pentagon utilizes the Automatic Digital Network (Autodim) for its communications, which is supplemented by another device, the Automated Message Handling System designed to allow military information analysts to "have a real-time picture of military and political trends around the world." Id. at 177.

[114] *See* GUISNEL, *supra* note 5, at 18-19; *See also* FEDERATION OF AMERICAN SCIENTISTS, REDEFINING SECURITY: Ch. 8 (visited Sept. 25, 1999) <http://www.fas.org/spg/library/jsc/chap8.html>. *See e.g.* Hodge v. Jones 31 F.3d 157 (4th Cir. 1994). In *Hodge*, the Carroll County Department of Social Services maintained a computer database that contained a record on every Maryland citizen who had received any services, ranging from food stamps to child protective services. *Id.* at 161. The plaintiffs were investigated by the Social Services because of possible child abuse. *Id.* After the allegations were found to be unsubstantiated, the plaintiffs sued to have the records removed to no avail. *Id.*

[115] *See Letter from The White House, to The Congress of the United States*, <http://www.epic.org/crypto/legislation/cesa/transmittal.html>. The demand for more and better access to information and electronic commerce continues to grow among financial, medical, and educational institutions, manufacturers and merchants and state and local governments. *Id.*

[116] *See id.*

[117] *See id.*

gation.[118] While it is certain that government computers are utilizing security measures, some private businesses are not.[119] Major corporations may have an impressive computer security system, but its auxiliary companies that access it may not.[120] Hackers know how to exploit weaknesses of subsidiary companies in order to gain access to the bigger company's computer system.[121] It is because of this that companies must take preventative steps.

An unlikely case from 1932 that is analogous to this issue is *T. J. Hooper v. Northern Barge Corporation*.[122] In *T.J. Hooper*, two barges towed by two tug boats set off from Virginia to New York.[123] While traveling, the weather turned poor and the barges sank.[124] The cargo owners sued the barge owners and the barge owners sued the tug boat owners.[125] The court decided that the owners of the tug boats were liable for half the loss of the barges because they did not have weather radios aboard.[126] The court said that although the use of weather radios had not become standard industry practice, it is the job of the court to

[118] *See* FEDERATION OF AMERICAN SCIENTISTS *supra* note 114. The Federation of American Scientists believe the Defense and Intelligence Communities focus more attention on information systems security. *Id.* The United States is increasingly dependant of information systems and networks. *Id.* Information systems control the basic functions of the nation's infrastructure, including the air traffic control system, power distribution and utilities, phone system, stock exchanges, the Federal Reserve monetary transfer system, credit and medical records, and a host of other services and activities. *Id.* Over 95% of Defense and Intelligence Community voice and data traffic uses the public phone system. *Id.*

[119] *See* Gripman *supra* note 49, at 170. Computer network security is virtually nonexistent is many companies which subjects such companies to substantial risk. *Id.* A disabled computer network can cost a company millions of dollars. *Id.*

[120] *See* John Leming, *The Next Great War: Cyber-Warfare*, E. PA. BUS.J. CORRESPONDENT, June 7, 1999, *available in* NewsBank, record number 011580DDE294B782939CA. General Motors may be well equipped to withstand cyber-attacks, but the corporation itself has approximately 10,000 suppliers, which in turn may have 40,000 suppliers of their own. *Id.* By going after one link in the chain, hackers could conceivably halt all production at General Motors. *Id.*

[121] *See* GUISEL, *supra* note 96 (providing a detailed description on the methodology of hackers). *See generally* SHIMOMURA & MARKOFF *supra* note 6.

[122] *See* 60 F.2d 737 (2d Cir. 1932).

[123] *Id.* at 737.

[124] *Id.*

[125] *See id.* Judge Hand reasoned that if the tugs would have carried radio receiving sets which would have warned them of the inclement weather, they would have had the opportunity to seek shelter in the Delaware Breakwater en route. *Id.*

[126] *Id.* at 739-40. Hand held that an adequate receiving set (weather radio) suitable for a tug can be purchased at a small cost. *Id.* He reasoned further that these tugs were towing heavy coal laden barges and strung out for a mile have little power to maneuver and do not expose themselves to weather which would cause them great damage. *Id.* They could have had at hand the only protection against the dangers of which they can learn of in no other way. *Id.*

make the general practice of calling the standard of proper diligence.[127] Another unlikely analogous case is *DiMarco v. Lynch Homes—Chester County, Inc.*[128] In *DiMarco*, a man contracted hepatitis from his girlfriend and sued her physician for not warning her to refrain from sexual activity.[129] *DiMarco* argued that a physician owes a duty of care to a third-party when he fails to properly advise a patient with a communicable disease, and the patient then passes that disease onto a third-party.[130] The court in *DiMarco* held that the duty of a physician is "within the foreseeable orbit of risk of harm."[131] Therefore, if a person is within this "foreseeable orbit of risk of harm" and her health is threatened because of a misdiagnosis of a patient, she has a cause of action against the physician.[132]

There are many ways to encourage people and businesses to maintain secure computer networks. Companies could hold each other liable for attacks by hackers. This can be done contractually. A company that allows another to access its computer system should make sure to include a clause in the contract that holds it responsible for maintaining a reasonably secure computer network.[133] A sample of such a clause de-

[127] *Id.* at 739.

[128] 583 A.2d 422 (Pa.1990).

[129] *See id.* at 423. Janet Viscichini was a blood technician taking a sample from a resident of the Lynch Home, June 18, 1985. *Id.* The resident struck or kicked her and caused the needle to prick her skin. *Id.* Viscichini learned later that the patient was infected with hepatitis and she sought medical attention from the appellants. *Id.* The appellants told her that if she remained symptom free for six months, she would not have been affected for six weeks. *Id.* Viscichini waited eight weeks before resuming sexual relations. *Id.*In September, Viscichini was diagnosed with hepatitis, and in December, DiMarco was diagnosed with hepatitis as well. *Id.*

[130] *DiMarco*, 583 A.2d at 424. The Court noted that physicians are the "first line of defense against the spread of communicable diseases, because physicians know what measures must be taken to prevent the infection of others." *Id.*

[131] *Id.* (quoting Doyle v. S. Pittsburgh Water 199 A.2d 875, 878 (1964)). The court further borrowed a quote from Superior Court Judge Frank Montemuro, Jr. who originally heard the case and restated: "This case involves a communicable disease." It hardly needs to be said that the prevention and control of communicable diseases is a momentous task which is of the utmost importance to the health and welfare of our citizens." *Id.* at 425. The communicability of a disease was analogized to a hacker who unleashes a virus that spreads from computer to computer. *Id.* at 425 n.3.

[132] *Id.*

[133] *See c.f.* RESTATEMENT (SECOND) OF TORTS § 283(c) (1964) (providing the standard of the "reasonable man.").

> Negligence is a departure from a standard of conduct demanded by the community for the protection of others against unreasonable risk. The standard which the community demands must be an objective and external one, rather than that of the individual judgment, good or bad, of the particular individual.It must be the same for all persons, since the law can have no favorites; and yet allowance must be made for some of the differences between individuals, the risk apparent to the actor, his capacity to meet it, and the circumstances under which he must act.

signed to protect companies is offered below:

> Agreement to Maintain a Secure Computer Network.
>
> In exchange for the right to access Acme Co. computer's supply database, Company A agrees to use a computer network that is reasonably secure when accessing Acme's computer network. This includes but is not limited to, at Company A's expense, the use of encryption software, firewalls, and all other methods necessary to create a reasonably secure network environment.
>
> If Acme Co.'s computer supply database is infiltrated, damaged, tampered with altered, corrupted or any combination of these by way of Company A's or subsidiary of Company A's, remote access dial-up or any other method by which Company A could use to access Acme Co.'s computer supply service., Company A will be held responsible for all costs associated with returning Acme Co.'s computer supply database to its original configuration, arrangement and formation as it was before the access occurred.[134]

Because companies are reluctant to come forward when their systems are hacked, they can opt to include in their secure network clause an agreement to arbitrate rather than litigate their disputes.[135]

E. Examples of Security Devices

Included in this section are descriptions of some security devices network engineers can use to make their networks more secure.[136] These devices are used in conjunction with one another to create an environment with a higher level of security.[137] This is in no way an exhaus-

Id.

[134] *See* Restatement (Second) of Torts, § 324 (1965) (providing the basis from which this clause was adapted and extended):

> One who, being under no duty to do so, takes charge of another who is helpless adequately to aid or protect himself is subject to liability to the other for any bodily harm caused to him by
>
> (a) the failure of the actor to exercise reasonable care to secure the safety of the other while within the actor's charge, or
>
> (b) the actor's discontinuing his aid or protection, if by so doing he leaves the other in a worse position than when the actor took charge of him.

Id.

[135] David Lazarus, *Silicon Valley's Hired Guns: Hackers have created a need for security experts to ward off attacks* (visited October 2, 1999) <http://infoweb8.newsbank.com/bin/gate.exe?f=doc&state=r06pr8.3.14>. Fred Smith, a New Mexico attorney specializing in computer crimes, states that "[t]here's a perception that public displays of this kind of dirty laundry will lead people to devalue the company." *Id.* Further, " better just to deal with it internally." *Id.*

[136] See infra Parts E.1- 3.

[137] Interview with Jeremy A. Faulkner, Microsoft Certified Systems Engineer, in Lisle, IL (Oct. 17, 1999). The most important aspect of network security is to protect the data that is essential to conduct business. *Id.* There are four major areas concerning the protection of data. First, the data must always be protected through the network or on the Internet by using either encryption or a Virtual Private Network ("VPN"), if necessary. *Id.*

tive list, as new methods are being developed continuously.[138]

In addition to implementing these and other security devices, corporations should consider performing an audit of their current computer system.[139] Often companies that have a good reputation for security will find that areas of vulnerability still exist.[140]

1. *Firewalls*

A firewall is a hardware device with software that restricts the access to a network by forcing all to pass through it.[141] The firewall filters the traffic from the external world to the internal system and from the internal system to the external world.[142] In theory, only acceptable traffic is allowed to pass through the firewall.[143] The firewall can be configured in a variety of different ways according to the needs of the network.[144] For example, a firewall can be used to keep some, or all, users from accessing the Internet while not allowing the Internet access to the internal network.[145]

Second, physical access to all network devices must be controlled. *Id.* Third, internal networks must be protected from the Internet and other connected networks if necessary. *Id.* Fourth, and possibly the most important, is protecting the network from the data which is on it from damage caused by accident, misuse or even mischievous users. *Id.* The network's users can be a network administrator's worst enemy when it comes to network security. *Id.*

[138] *See* sources cited *supra* note 11 and accompanying text.

[139] *See* Lazarus, *supra* ncte 135. Nearly one third of U.S. companies, financial institutions, government agencies and universities say outsiders penetrated their computers last year. *Id.* Former hackers, now termed "white hats" use their skills to assess the vulnerability of computer networks. *Id.* Security audits can range from anywhere between $20,000 to $200,000, depending on the depth, hours allotted and extensive as the company desires. *Id.*

[140] *See id.* After 20 minutes of trying, a "white hat" found a glitch in the computer system of a well-known multimedia company in Northern California. *Id.*

[141] *See* Icove, *supra* note 3 at 140.

[142] *See* interview with Faulkner, *supra* note 137. Firewalls are primarily used to protect internal networks from the Internet. *Id.* They are also used to control what users can access on the Internet. *Id.* Firewalls are not usually placed on the computer, rather they are a separate network device, about the size of a V.C.R., some can be the size of a server. *Id.*

[143] *See* interview with Faulkner, *supra* note 137. Encryption software is built into many other software applications placed on the computer such as Microsoft Outlook, an E-mail program. *Id.* Encryption software is highly useful for businesses needing to send private information such as accounting and payroll documents over the Internet. *Id.*

[144] *See* Icove *supra* note 3 at 138- 39. Encryption transforms original information, called "plaintext" into scrambled information called "ciphertext." *Id.* The technique selected for encryption is known as the encryption algorithm and it determines how simple of complex the process will be. *See generally,* Garfinkel, Practical UNIX Security (1995); *see also* Russell Computer Security Basics (1991).

[145] *See* Icove, *supra* note 3 p.140. Firewalls offer new ways to protect a network form attacks, while allowing its users to have some access to the Internet. *Id.* A firewall must

2. *Encryption Software*

Encryption software uses algorithms to encode data.[146] Once data is encoded and decoded, it can be sent through the Internet, or network environment, and it will appear like claptrap to anyone who does not hold the "key" to decode it.[147] The main advantage of encryption is the privacy it affords.[148] Private information such as a document containing credit card numbers can be encrypted and distributed without the danger of disclosure to unwanted persons.[149]

3. *Virtual Private Networks*

Virtual Private Networks ("VPN") take encryption to a higher level, and provide companies with the added protection they need.[150] Instead

be installed, configured and maintained correctly in order to function properly. *Id.* It is possible to completely block all access to and from the Internet, or to simply block particular users from the Internet. *Id.* *See generally* FITES ET. AL. CONTROL AND SECURITY OF COMPUTER INFORMATION SYSTEMS (1989); *see also* DENNING COMPUTERS UNDER ATTACK: INTRUDERS, WORMS AND VIRUSES (1992).

[146] *See* ROBERT B. GELMAN ET. AL., PROTECTING YOURSELF ONLINE 47- 48 (1998).

[147] *Id. See also* ROSENOER, supra note 48 at 213- 14 (1996). Much debate surrounds the topic of encryption. *See also* Electronic Privacy Information Center, *CESA Bill Text,* (visited Sept. 26, 1999) <http://www.epic.org/crypto/legislation/cesa/bill_text.html>. In an effort " [t]o protect the privacy, security and safety of the people of the United States through the support for the widespread use of encryption, protection of the security of cryptographic keys, and facilitation of access to the plaintext of data for legitimate law enforcement purposes," the White House proposed the "Cyberspace Electronic Security Act of 1999" (CESA). *Id. See also,* Electronic Privacy Information Center ("EPIC"), *CESA Analysis* (visited Sept. 26, 1999) <http://www.epic.org/crypto/ legislation/cesa/analysis.html>. The purpose of the CESA is to update law enforcement and privacy rules for the widespread use of encryption. *Id.* CESA reflects a careful balance balancing between the interests of public safety and privacy. *Id. See also* EPIC Press Release, *Encryption Policy Electronic Privacy Information Center Questions Impact of New Clinton Cyrpto Policy; Says Effect on Average Users Remains Unclear* (visited Sept. 26, 1999) <http://www.epic.org/crypto/ legislation/cesa/analysis.html>.Under the current system, there is no statutory protections for the privacy of stored recovery information, the government may be able to obtain this information from a recovery agent with, a grand jury subpoena. *Id.* According to David Sobel, the general counsel for EPIC, more details of the new policy must be released before its impact on user privacy can be assessed. *Id.* He noted that it may not be in the best interest of the average computer user. *Id.*

[148] See *id.*

[149] *See id.*

[150] *See* C. Reid Turner, *Create a Private Network Across the Internet VPNs Keep Communications Confidential,* 10 SMART COMPUTING IN PLAIN ENGLISH 70, 70- 73 (1999). Companies use VPNs because they serve three major needs, the first of which is the need to support remote users. *Id.* Through a VPN, employees can securely access internal company resources from home or while traveling. *Id.* Second, is the need to tie remote offices together and connect them to company headquarters so that resources at one site are available to the other. *Id.* While this could be done on the Internet, the VPN ensures that the communication remains private. *Id.* Third, need to connect a company with its customers

of utilizing a manual encryption software package to encrypt a file or a document, all data is encrypted before it is placed on the public network, and decoded when they arrive at the other end of the public network.[151] Data, such as a message travels through a passage called a tunnel. All the encryption is done automatically.[152] The tunnels utilized by the VPN run through the Internet on the same network infrastructure.[153]

F. Creating a Civil Cause of Action for Victims of Hackers

Creating liability for corporations is best facilitated by contract. Corporations may use a clause like the one in section D, or may create their own through bargaining. Unlike a corporation, private citizens lack this bargaining power. If an individual, while shopping at a grocery store, slips on a banana peel, that individual may seek recourse against the grocery store and the dropper of the peel. If an individual's credit card is stolen off a web site, their current recourse for damages is only against the computer hacker.[154] In *Yanzick v. Tawney*,[155] a woman maintained a proper cause of action in negligence when she sued the grocery store after getting pinned between an ice machine and a car on the grocery store's sidewalk.[156] The court held that the her injuries were foreseeable because the ice machine was located on the sidewalk between the grocery store and the parking lot and the cars parked so as to jut onto the sidewalk.[157] Further, the court found that a defendant must ascertain the condition of her premises and use reasonable care to protect her

and suppliers. *Id.* Companies want to let authorized parties have restricted access to corporate information. *Id.*

[151] *See id.* at 71-72. A message is made up of two parts, a header and the data. *Id.* These parts function like an envelope and a letter. *Id.* The header contains information specified by the IP and is needed to deliver the message. *Id.* The data refers to the user data that is needed by whatever applications happen to be communicating. *Id.* A VPN will encrypt the entire IP message, both header and data and wrap the result with a new IP header. *Id.* This is done so that the information about which computers are communicating through the tunnel cannot be discerned by examining the original header. *Id.* The only visible header in the tunnel is the newly created header with the generic information. *Id.* Businesses can use VPNs to protect the privacy of all data that is sent through the encrypted tunnel. *Id.* Once the tunnel is created, and you have the VPN, a business can use E-mail, File Transfer Protocol (FTP), web browsers, or terminal emulation software without fear of "prying eyes." *Id.*

[152] *See id.* at 71. The hardware and software at the tunnels endpoints are responsible for the encryption that hides the information and the authentication that controls access to the tunnel.

[153] *See id.* at 70.

[154] *See* 18 U.S.C. § 1030.

[155] *See* Yanzick v. Tawney 605 P.2d 297, 298-99 (Or. App. 1979).

[156] *See id.* at 298.

[157] *See id.* at 300.

patrons from dangers by the arrangement and use of the premises.[158] Just as the court in *Yanzick* found that a negligence claim was valid because of the grocery store's placement of an ice machine, businesses should be held accountable for the security flaws in their networks.[159] A business has a duty to maintain a reasonably safe premises, it should have a duty to maintain a reasonably safe cyber-premises.[160]

The majority of states have computer crime statutes.[161] This comment proposes that to protect the interests of their customers, businesses need to be placed on notice that they must maintain their computer networks so as to create a minimal risk of infiltration by hackers.[162] Companies have a myriad of options in securing their networks and should be required to utilize the technology to protect themselves and the public.[163] Below is a sample statute intended to give private citizens and businesses a civil action to recover damages suffered from sub-standard computer security.

G. The Corporate Computer Network Responsibility Act

This Act applies to all businesses, corporations, partnerships and organizations which

(1) own or operate a computer network; and

(2) the computer network holds data for another person, business or organization;

and

(3) that have more than 25 employees or contractors.

(b) If any person, business or organization is;

through the authorized or unauthorized access of a computer network belonging to any person, corporation or organization that was au-

[158] *See id.*

[159] *See id.* at 298. "Defendant as the operator of a business to which the public is invited, has the duty to provide and maintain a reasonably safe place for its patrons in the reasonable pursuit of activities within the scope of the invitation." *Id.*

[160] Schnuphase v. Storehouse Markets 918 P.2d 476, 478 (Utah 1996). A store owner has a duty to exercise reasonable care in maintaining the premises. *Id.* There are two theories by which plaintiffs can allege negligence in maintaining their premises: the first theory involves an unsafe condition of a temporary nature, in this instance, a plaintiff must show one, that the business owner knew or should have known of the hazardous condition, and that the owner had enough time to remedy the situation, and that he failed to do so; the second theory involves an unsafe condition of a permanent nature. *Id.* Under the second theory, notice is presumed. *Id.*

[161] *See* 18 U.S.C. § 1030 (g) (1996).

[162] *See e.g.* Mullins v. Pine Manor College 449 N.E.2d 331 (Mass. 1983). In *Mullins*, a college was held liable when a student was raped on campus. *Id.* The Court utilized an established principle of law that states, a duty voluntarily assumed must be performed with due care. *Id.*

[163] *See* Denning, *supra* note 2.

thorized to hold the information, file(s) or other items capable of being held by a computer for that person, business or organization is destroyed, altered, transmitted, corrupted, or deleted in such a manner as to cause monetary or other substantive harm; and

the harm imposed upon the victim could have been prevented if the business would have maintained a reasonably safe computer network,

(c) then, the person who suffered damage or loss by reason of a violation of this act may maintain a civil action against the violator to obtain compensatory damages and/or injunctive relief damages in an amount not more than the amount of losses suffered.

Evidence of a reasonably safe computer network would be the use of encryption software, Virtual Private Network Structure, firewall technology, and/or servers under lock and key also, the use of any other technology in the area of computer security.

Effect on other laws

Nothing in this section shall be construed to limit the application of 47 U.S.C. 230.[164]

No effect on criminal law

Definitions

business, corporation, partnerships and organizations shall retain their common meanings and include all employment, occupation, profession, or commercial activity engaged in for gain or livelihood.[165]

computer network: a collection of computers, printers, routers, switches, and other devices that are able to communicate with each other over some transmission medium[166]

[164] 47 U.S.C. § 230.

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil Liability

No provider or user of an interactive computer service shall be held liable on account of –

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent , harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)

Id.

[165] *See* BLACKS LAW DICTIONARY 198 (6th ed. 1990)(defining "business.").

[166] *See* DOWNS, *supra* note 11 at 177. The definition of "computer network" was taken from the definition offered in this technical handbook. *Id.*

The adoption of this act, or a similar act, would provide accountability for the corporations in creating, maintaining and updating their computer networks.

H. Corporate Network Responsibility Act's Effect on Internet Service Providers

Internet Service Providers ("ISPs")[167] are protected by 47 U.S.C. § 230.[168] ISPs are in a unique position under the law in that they are shielded from civil liability.[169] This is because it is the policy of the United States to encourage the use and the development of the Internet.[170] It is also the policy of the United States to "preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services,[171] unfettered by Federal or State regulation."[172] An ISP's main purpose is to provide *access* to the Internet for other users not to provide content.[173] Unlike financial institutions, schools and medical facilities, the use of an ISP is optional for most people and contains only the information that a user specifically provides it. For this reason and the many other reasons enumerated by Congress, it would not be prudent to extend the Corporate Network Responsibility Act to ISPs.[174]

[167] *See* Zeran v. Am. Online, 958 F.Supp. 1124, 1126 n.1 (E.D. Va. 1997) An ISP offers access to its own computer network and organizational software allowing subscribers to interconnect easily with computer networks other than those proprietary to the "online service." *Id.*

[168] *See* infra text accompanying note 165.

[169] *See* infra text accompanying note 165.

[170] *See* 47 U.S.C. § 230 "(b) It is the policy of the United States – (1) to promote the continued development of the Internet and other interactive computer services and other interactive media. . ."

[171] 47 U.S.C. § 230

> (e) Definitions (2) Interactive Computer Service
>
> The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

Id.

[172] 47 U.S.C. § 230 (b)(2).

[173] *See supra* text accompanying note 165.

[174] 47 U.S.C. § 230 (b) Policy It is the policy of the United States—

> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
>
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material;

Id.

I. Limiting Liability Through the Use of Insurance

Just as business owners retain insurance to protect their premises from burglary, insurance specifically protecting their computer networks should also be purchased.[175] This additional coverage will protect business owners from loss due to hacker attacks and other computer problems.[176] Insurance for computer systems would provide an additional layer of protection for businesses, shielding them from the extraordinary costs of hacker attacks.[177] The use and availability of insurance policies of this type is increasing.[178]

A number of insurance companies specialize in coverage for telecommunications companies and tailor their services to these companies.[179] Some insurance companies offer "errors and omissions" insurance designed specifically to cover attacks by hackers.[180] "Errors and omissions" insurance protects companies from its negligent acts.[181] Further, insurance has developed into a critically important component of our civ-

[175] *See* Robert D. Chesler, *The Failure of the Comprehensive General Liability Policy and the Rise of Niche Insurance,* 192 N.Y. Law 13 (1998). Chesler notes that "Insurance is a unique blend of the private and public." *Id.* Each business person pays into a central fund so that financial support can by offered if anyone is struck with and unexpected tragedy. *Id.* Unfortunately, the Comprehensive General Liability policy no longer covers against the environmental, employment and intellectual property risks that menace most of the business world. *Id.* To cover the items and others above, business must find "niche" policies that will cover the minute facets of a business. *Id.* at 15.

[176] *See Insurance Solutions for the Telecommunications Industry* (visited Nov. 13, 1999) <http://www.tsbic.com/ telecom.htm>. E & O insurance also protects companies if they experience machinery breakdowns, loss of data or fail to maintain the company's software among other things. *Id.*

[177] See Chesler, *supra* note 175 at 16. Internet service providers and other technology professionals can purchase general liability and errors coverage that included computer-hacker theft. *Id.* Loss of a third-party's data that was in the policyholder's custody and copyright infringement. *Id.* Other policies may offer protection against computer viruses. *Id.* One problem for policy holders an insurers alike is that the world of the Internet and computer risk remains ill-defined and little known. *Id.*

[178] *See id.*

[179] *See Insurance Solutions for the Telecommunications Industry supra* note 176. This company called "Chubb" insures the electronics and broadcasting industries, including Internet service providers, web site designers, web hosts, Internet content providers and other companies concerned about the security of voice data and video traffic on their networks. *Id.*

[180] *See id.* Chubb claims its "errors and omissions" insurance coverage will provide "defense and indemnity for suits alleging damages because of the theft, distortion, manipulation or loss of customer data by a hacker." *Id.* Further, Chubb offers many "real-life" scenarios that they purport to cover, such as the following: "A company is sued for consequential damages alleging breach of security when a hacker broke through a firewall and distributed proprietary information." *Id.*

[181] *See* Society of Computer Professionals, *Errors and Omission Insurance* (visited Nov. 13, 1999) <http://www.comprof.com/p41.htm>. This organization urges professionals to retain Errors and Omissions (E & O) Insurance because, among other things, it protects

ilization, as complex machinery is known to fail and requires the protection of insurance.[182]

IV. CONCLUSION

The need for protection against attacks by computer hackers is real.[183] As security measures increase in proficiency, the hackers become more skilled as well. It is imperative that individuals have a remedy against the holder of their information if their information is stolen. Placing this burden on companies, who most often have more resources than the general public, will force them to implement better security for their computers and networks. Creating a statutory duty for businesses to maintain reasonably secure computer networks would promote responsible conduct and create an environment that individuals would be more apt to use. Encryption software, and the new developments in virtual private networking make security more efficient, superior, and altogether safer than previous methods.

Companies can make use of the clauses above to protect themselves and each other from damage done by an unauthorized entry into their computer network. While initially negotiating a contract, companies can be pro-active and bargain for a network protection clause. Such a clause will ensure that the companies have a remedy in contract if damage is done to their computer network, and their remains no statutory remedy. Hopefully, in the future, clauses protecting computer networks will become commonplace. Additionally, purchasing extra insurance for business computer networks protects everyone involved. Insurance specifically designed to protect computers and networks is increasingly becoming commonplace and can be purchased for large networks, small networks, or a single home computer. With the tremendous growth of e-commerce, increasingly sensitive information, *i.e.* credit card numbers, is contained on computer networks and passed through the Internet. It is vital that the legislature enact a statute to protect all users.

Sarah Faulkner

"an insured acting in his or her capacity as a professional from third-party claims arising from economic damage and damage and damage to public image or reputation." *Id.*

[182] *See* Paul Strassmann, *Computerworld For IT assurance, get some insurance* (visited Nov. 13, 1999) <http://www.computerworld.com/home/print.nst/idgnet/981102725E>. Strassmann argues that because of insurance, airplanes, cars, chemical factories and other facilities can operate even though they can stop functioning and at times can become dangerous. *Id.*

[183] *See* Denning *supra* note 2.