# CYBER-EXTORTION: DUTIES AND LIABILITIES RELATED TO THE ELEPHANT IN THE SERVER ROOM

Adam J. Sulkowski
J.D., Boston College, M.B.A., Boston College

Assistant Professor of Business Law
Charlton College of Business
University of Massachusetts Dartmouth
285 Old Westport Road
North Dartmouth, MA 02747
Office: 508-999-8037
Mobile: 978-394-2834
Website: www.umassd.edu/charlton
E-mail: asulkowski@umassd.edu

# CYBER-EXTORTION: DUTIES AND LIABILITIES RELATED TO THE ELEPHANT IN THE SERVER ROOM[1]

## CONTENTS




[1] The author wishes to acknowledge those who lent their expert opinions, editorial input or other assistance, including Dr. Christopher T. Pierson, attorney with Lewis and Roca LLP's cybersecurity and intellectual property practice groups and President of the Phoenix, Arizona Infragard chapter, Special Agent Shelagh Sayers of the Federal Bureau of Investigation, Robert Richardson, Editorial Director of the Computer Security Institute, William A. Brandt, Jr., litigation and information management consultant and Blake A. Bell, senior knowledge management counsel with Simpson Thacher & Bartlett LLP. Thanks are also due Dr. Timothy Shea, Associate Professor of Management Information Systems at the Charlton College of Business at University of Massachusetts Dartmouth for inviting me to collaborate in researching the phenomenon of cyber-extortion and to graduate students Adam Silva (MBA, Charlton College of Business, University of Massachusetts Dartmouth) and Eddy Robert (MBA, Charlton College of Business, University of Massachusetts Dartmouth, JD, Southern New England School of Law) for their preliminary research on the phenomenon of cyber-extortion.

8. USA PATRIOT Act
9. State Consumer Protection Statutes
10. Contract Law
11. Torts
    a. Torts of Fraudulent and Negligent Misrepresentation
    b. Tort of Breach of Confidentiality

B. Downstream Liability to Other Businesses
1. Negligence
    a. Existence and Violation of a Duty of Care
    b. Causation
    c. Harm
    d. Analogous Cases
2. Agency
3. Trespass
4. Statutory Civil Suit Provisions
5. Product Liability Unavailable
6. Damages and Defenses
7. Why the Dearth of Tort Suits?

**IV. Conclusions**

## I. Introduction

Cyber-extortion – demanding money or something else of value in exchange for not carrying out threats to commit harm that would involve the victim's information systems – is an evolving and costly form of criminal activity. The title of this article reflects the fact that cyber-extortion, like the proverbial elephant in the room, is a large problem which has not been thoroughly discussed. This article fills a conspicuous void in existing scholarly and practitioners' literature by comprehensively analyzing the legal frameworks that apply to cyber-extortion and by discussing relevant public policy concerns.

The only publicly-available survey that has addressed cyber-extortion to date, a 2004 Carnegie Mellon University (CMU) survey of 100 companies, found that 17% of small and midsized businesses had been the target of some form of cyber-extortion.[2] A further 13% of respondents were unsure if their company had been targeted.[3] A common tactic in cyber-extortion scenarios is to threaten to incapacitate a victim's transactional website or other components of their information system. This is known as a denial-of-service (or DoS) attack. One way to succeed with a DoS attack – and a means for the cyber-extortionist to conceal their identity – is to hijack the information systems of unsuspecting businesses or other enterprises and use these hijacked information systems as the tools for incapacitating the targeted victim's website or systems. When a network of hijacked computers is used to overwhelm a victim's system, the attack is called a Distributed Denial of Service (DDoS) attack. Available evidence suggests that cybercriminals are employing increasingly sophisticated techniques and are increasingly motivated by the pursuit of financial gain.[4]

---

[2] Gregory M. Bednarski, *Enumerating and Reducing the Threat of Transnational Cyber Extortion against Small and Medium Size Organizations,* 2004 InformationWeek Research Fellowship, THE HEINZ SCHOOL, CARNEGIE MELLON UNIVERSITY, *available at* http://www.infinitel00p.com/library/InformationWeek-CMU_Cyber_Extortion_Study.pdf (last visited January 2, 2007) at 13.

[3] *Id.* The 2005 annual CSI/FBI Computer Crime and Security Survey did not separately measure cyber-extortion incidents, but listed as the second through eighth most-frequently occurring computer crimes, in sequence: DoS attacks, telecommunications fraud, unauthorized access to information, virus deployment, financial fraud, insider abuse of Internet access and system penetration – all of which can be elements of cyber-extortion – while the most common form of computer crime was laptop or mobile device theft. Lawrence A. Gordon, et al., *2005 CSI/FBI Computer Crime and Security Survey*, COMPUTER SECURITY INSTITUTE PUBLICATIONS, *available at* http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf (last visited January 2, 2007), at 12-13. For a discussion of why separate statistics need to be tracked for cybercrime, and a review of available data sources, *see* Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?* 9 VA. J.L. & TECH. 13, Fall 2004.

[4] For a discussion of technical details and data indicating that cyber-extortionists are becoming more professional, *see* Adam J. Sulkowski and Timothy Shea, *Cyber-Extortion: the Elephant in the Server Room*, (under review as of

It bears pointing out at the onset that the scarcity of case law on the topic of cyber-extortion to date means that legal questions related to cyber-extortion are not fully resolved. Specifically, U.S. courts have not grappled with the liability of professionals whose duties include protecting information systems and who fail in those duties when a cyber-extortionist follows-through on a threat to disrupt businesses and cause harm. The state-of-the-art in computer security and crime is advancing and awareness of risks has spread. Even minimum acceptable standards of care are arguably becoming established. Therefore, to both legal scholars and practitioners, cyber-extortion scenarios present an evolving web of responsibilities and possible liabilities that will demand scrutiny in the coming years – this article hopefully will serve as a catalyst to that much-needed debate.

The legal and business ramifications of a typical cyber-extortion scenario can be significant, ranging from liability for the abuse of private customer data to unwittingly allowing one's information system to be hijacked and used as a tool to commit an attack on another company in the context of a DDoS attack. Given the costs associated with cyber-extortion and the huge potential pool of malfeasors, targets and third party plaintiffs, it is vital to raise awareness of this form of crime, enhance knowledge of legal remedies and responsibilities and consider the policy implications of holding businesses responsible for the security of their information systems.

However, companies and their employees do not seem to be taking the threat very seriously. The 2004 CMU survey respondents believed that they were not likely to become victims of cyber-extortion attempts: 68% responded that they were at no or low risk of such an attack. Only 21% of the companies had formal training programs to teach employees how to respond to security breaches and only 37% had performed security assessments within the 6 months prior to being surveyed. These pieces of information are all the more troubling because 45% of survey respondents expressed a lack of confidence in the ability of their technical department to respond to security incidents.[5] While the annual CSI/FBI Computer Crime and Security Survey indicates that the adoption of information security precautions is slowly increasing, respondents on average do not believe that their companies adequately invest in

---

January, 2007) *available at* www.ssrn.com. The article also investigates why attorneys are generally the last to be informed of a cyber-security breach and suggests action steps that attorneys can take to prevent and mitigate the harm of cybercrimes.

[5] Bednarski, *supra* note 2, at 13.

information security awareness training.[6] According to the 2004 CSI/FBI Computer Crime and Security Survey, DoS attacks accounted for over $26 million in losses – accounting for the largest share of the total of $141,496,560 in losses reported by 269 respondents.[7] Therefore, while extensive statistical data is not publicly available, and while existing information is not completely consistent, it is clear that cyber-extortion is a significant problem for the business community.

The legal community needs to be aware of both the legal framework for prosecuting cyber-extortionists and the vast potential web of liabilities that may arise in the context of a cyber-extortion. Part II. Investigates the legal framework for prosecuting and recovering damages from the perpetrators of cyber-extortions. Part III. will examine the duties and potential liabilities of businesses that fail to protect themselves from being the victims or unwitting accomplices of cyber-extortionists. Part IV. will discuss the policy implications of holding businesses accountable for the security of their information systems.

## II. Legal Framework for Prosecution and Civil Liability of Cyber-Extortionists

### A. Defining Cyber-Extortion

As defined by the Hobbs Act, extortion is "the obtaining of property from another, with his consent, induced by wrongful use of actual or threatened force, violence, or fear, or under color of official right."[8] As elaborated upon below, extortion is a criminal act under federal and state laws. Cyber-extortion involves the added element of a threat of committing a wrongful act involving computers or information systems.

Courts interpret the definition of extortion – specifically, what constitutes a threatened wrongful act – broadly.[9] Blackmail threats – even those that are intended to enforce a legal right

---

[6] Gordon *et al., supra* note 3 at 17-18; Lawrence A. Gordon et al., *2006 CSI/FBI Computer Crime and Security Survey*, COMPUTER SECURITY INSTITUTE PUBLICATIONS, *available at* http://www.gocsi.com/press/20060712.jhtml, (last visited January 2, 2007) at 13.

[7] Lawrence A. Gordon, et al., *2004 CSI/FBI Computer Crime and Security Survey*, COMPUTER SECURITY INSTITUTE PUBLICATIONS, *available at* CSI/FBI 2004 Computer Crime and Security Survey, *available at* http://www.reddshell.com/docs/csi_fbi_2004.pdf (last visited January 2, 2007), at 10.

[8] 18 U.S.C. § 1951(b)(2) (2000).

[9] *See U.S. v. Jackson*, 180 F.3d 55, 65-71 (C.A.2 N.Y. 1999), (definition of extortion and precedent cases and legislative history and intent of the Hobbs Act Congress discussed at length).

– may constitute extortion.[10] Thus, attempting to embarrass a victim into paying an overdue bill may constitute extortion,[11] as may the attempt to humiliate someone into paying a valid court judgment.[12]

Cyber-extortions often are comprised of three distinct illegal acts: the threat, the act (if committed), and often a preliminary criminal act to make the threatened act credible. For example, as described below: the threat to disrupt information systems with the goal of extorting money is a crime; if the threat is fulfilled, the act of disrupting information systems is itself a crime, and a credible threat to disrupt information systems typically involves showing that the information system's security has already been breached, which is also a crime.

B. What Has Worked: the Case of *U.S. v. Ivanov*[13]

Out of a handful of colorful, headline-grabbing arrests, only one court opinion was available in Westlaw as of early 2007 that substantively explored the bases for establishing jurisdiction and liability in the context of a cyber-extortion: *U.S. v. Ivanov*.[14] Furthermore, as of

[10] At least one scholar has maintained a restricted definition of extortion which requires that the threatened act be criminal; such a definition places some blackmail scenarios into a separate category. *See* Bednarski, *supra* note 2 at 3. Besides being consistent with court precedents, the author has decided to maintain a broad definition because (1) cyber-extortion is under-reported (2) not widely discussed and (3) is relatively unexplored territory for scholars, attorneys, managers and courts. Therefore, there is reason to believe that whatever data has been collected has at times been reported by individuals without knowledge or concern for precise differences in the definitions of cyber-extortion versus cyber-blackmail. Thus, it is not only consistent with court precedent, but more consistent with common understanding and usage of those reporting the cited data to maintain the broad definition of extortion.

[11] The only exception may be instances of blackmail where the disclosed facts have a reasonable nexus to the pursuit of a legal right, such as threatening disclosure of non-payment of dues or a consumer complaint. *See Jackson*, *supra* note 9 at 70-71. Otherwise, as pointed out by the Second Circuit, the truth of the damaging allegations underlying the threat is not a defense to a charge of extortion. *Id.* at 66, citing to *United States v. Von der Linden,* 561 F.2d 1340, 1341 (9th Cir. 1977) (per curiam), *cert. denied,* 435 U.S. 974 (1978); *Keys v. United States,* 126 F.2d 181, 185 (8th Cir.), *cert. denied,* 316 U.S. 694 (1942); *cf. United States v. Pascucci,* 943 F.2d 1032, 1033-34, 1036-37 (9th Cir. 1991).

[12] In Washington, the state Supreme Court recently ruled that attempting to embarrass a former girlfriend into paying a valid court judgment of $5,000 by posting nude photographs online and mailing them to third parties constituted extortion under Washington's extortion statute. *State v. Pauling*, 149 Wash. 2d 381, 69 P.3d 331 (2003) (citing to *U.S. v. Jackson*, *supra*, note 9).

[13] 175 F. Supp. 2d 367 (D. Conn. 2001).

[14] Since then, one case has cited to *U.S. v. Ivanov*. *See Robert Diaz Assoc. Enterprises, Inc. v. Elete, Inc.*, 2004 WL 1087468, (S.D.N.Y. May 14, 2004) (finding, as in *Ivanov,* that for jurisdictional purposes, the Computer Fraud and Abuse Act should be interpreted to apply to where a defendant intended harm to occur, even if the technology that facilitated or allowed the harm to be perpetrated is physically located elsewhere). One similar case yielded a court opinion that specifically addressed the discrete issue of evidence gathering. *See U.S. v. Gorshkov*, 2001 WL 1024026 (W.D.Wash.). Otherwise, as mentioned above, only one other opinion discusses extortion and computers, in the context of a man using both conventional mail and the internet to publicize nude photos of his ex-girlfriend in an effort to embarrass her into paying a valid court judgment in his favor. *Pauling,* 149 Wash. 2d 381. The only

2007, there was no scholarly article available that was dedicated to the topic of cyber-extortion. The following Parts discuss *U.S. v. Ivanov* and the statutes that comprise the legal framework applicable to cyber-extortionists.

The fact pattern of *U.S. v. Ivanov* was paradigmatic of headline-grabbing cyber-extortion cases: from Russia, Aleksey Ivanov accessed the information system of a Connecticut-based website-hosting and credit card processing company. The government claimed that defendant Ivanov's e-mailed offer to help protect the company from having its data destroyed in exchange for $10,000 amounted to extortion.[15] The published court opinion deals with a motion to dismiss indictments for extortion, computer fraud, conspiracy and possession of unauthorized access devices (credit card information) for lack of subject matter jurisdiction. The court opinion explains why subject matter jurisdiction under the Hobbs Act, Computer Fraud and Abuse Act and Access Device Statute were all appropriate, despite the fact that the defendant was not in the U.S. at the time of his alleged criminal acts.

The next five Parts describe *Ivanov*'s lessons for establishing jurisdiction and applying relevant federal statutes to the context of cyber-extortion.[16] The subsequent five Parts will consider additional grounds for prosecuting cyber-extortionists and for civil lawsuits against cyber-extortionists.

1. Acquiring Jurisdiction

In *Ivanov*, Judge Thompson relied on two rationales for concluding that he had jurisdiction over the case. First, the intended and actual harm of the defendant's actions in Russia occurred in the United States.[17] This on its own would allow for jurisdiction to be exercised by a U.S. court over a foreign defendant under any of the laws relevant to the case. Second, Judge Thompson reasoned that Congress intended that all three statutes under which the defendant was charged were intended by Congress to apply extraterritorially.[18] The opinion

---

somewhat novel holding of this case is that under Washington State's extortion statute, the use of blackmail to pressure a victim into paying a legal debt or judgment constitutes second degree extortion. *Id.*

[15] *Ivanov*, 175 F. Supp. 2d at 369.

[16] For a detailed analysis of various alternative cybercrime scenarios and how federal statutes would be applied in other contexts, *see* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177 (2000), *available at* http://www.sinrodlaw.com/cybercrime.doc (last visited January 2, 2007).

[17] *Ivanov*, 175 F. Supp. 2d at 370-373.

[18] *Id.* at 373.

describes how the statutes were interpreted or amended to explicitly cover foreign in addition to interstate contexts.[19]

2. The Hobbs Act

The Hobbs Act of 1941, in relevant part, states:

> Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both.[20]

The Hobbs Act was the main piece of federal legislation criminalizing extortion in the pre-Internet era. As demonstrated by *Ivanov*, even before the passage of any modern computer crime legislation (since amended to cover extraterritorial contexts) the Hobbs Act would have allowed for the prosecution of cyber-extortionists, and was interpreted to apply to threats originating from abroad.[21]

3. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act of 1986 (CFAA) contains several sections that are related to cyber-extortion.[22] CFAA has also been referred to as the leading federal legislation applicable to a DDoS attack.[23]

It is helpful to begin this analysis of the relevant sections of the CFAA with a step-by-step dissection of the elements of a typical cyber-extortion attempt. First, unauthorized access to

---

[19] *Id.* at 373-375.
[20] 18 U.S.C. § 1951(a) (2000).
[21] Judge Thompson noted that the U.S. Supreme Court characterized the Hobbs Act as speaking "in broad language" *Ivanov,* 175 F. Supp. 2d at 373 (citing to *Stirone v. United States,* 361 U.S. 212, 215, 1960). Judge Thompson then explained how the Third Circuit, relying in part on *Stirone,* concluded that: "[E]ven if none of the [defendants'] overt acts had occurred in this country ... Congress could give the district court jurisdiction under the commerce clause so long as [the defendants'] activities affected [the victim's] commercial ventures in interstate commerce within the United States." *Ivanov* at 373, citing to *United States v. Inigo,* 925 F.2d 641, 648 (3d Cir. 1991).
[22] 18 U.S.C. § 1030 (2000).
[23] Jerry Wegman & Alexander D. Korzyk, *Internet Denial of Service Attacks: Legal, Technical and Regulatory Issues*, J. OF LEGAL, ETHICAL AND REG. ISSUES, Vol. 7, No. 1 (2004), *available at* http://www.cbe.uidaho.edu/wegman/blaw265/DOS%20paper%20AA%202003%20web.htm (last visited January 2, 2007). *See also* Aaron Burstein, *A Survey of Cybercrime in the United States*, 18 BERKELEY TECH. L.J. 313 (2003).

an information system with intent to defraud is often one element of a typical cyber-extortion attempt. Second, by accessing the information of a business or any other enterprise, the extortionist effectively obtains something of value from another. Third, intentionally accessing protected computers via interstate or foreign communications for the purposes of financial gain or committing a criminal act are typical components of cyber-extortion. Finally, cyber-extortion is often completed by communicating a threat to damage some component of the accessed information system.

All four of the components above were criminalized by CFAA, and constituted four of the counts against defendant Ivanov.[24] Knowingly accessing protected computers with intent to defraud was criminalized by Section 1030(a)(4). Obtaining something of value violates Section 1030(c)(3)(A). Intentionally accessing protected computers and obtaining information via interstate and foreign communications for purposes of financial gain and in furtherance of a criminal act violates Sections 1030(a)(2)(C) and 1030(c)(2)(B).

Finally, transmitting a threat to cause damage via interstate or foreign communications violates Section 1030(c)(3)(A). Section 1030(a)(7) explicitly clarifies that extortion attempts fall under the ambit of Section 1030(c):

> [Whoever] with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce a communication containing any threat to cause damage to a protected computer shall be punished as provided in subsection (c) of this section.

Section 1030(e)(8) defines "damage" as any "impairment to the integrity or availability of data, a program, a system, or information" that either causes at least a $5,000 loss within a one year period, interferes with medical diagnosis or treatment, causes physical injury to a person or threatens public health or safety. The meaning of damage under the CFAA has been interpreted broadly, such that DDoS attacks that use a large volume of e-mails to disable a website has constituted damage under the CFAA.[25] Individuals may be convicted of unauthorized access to a computer under the CFAA without intending to do harm.[26]

---

[24] *Ivanov,* 175 F. Supp. 2d at 370, 374-375.
[25] In *America Online, Inc. v. National Health Care Discount, Inc.* (121 F. Supp. 2d 1255, N.D. Iowa 2000), the court decided that unsolicited bulk e-mail advertising created the sort of damages defined by the CFAA in § 1030(e)(8)(A).
[26] *U.S. v. Morris*, 928 F.2d 504 (2d Cir. 1991).

Significantly, Section (g) of the CFAA allows for civil actions for the recovery of compensatory damages or injunctive or other equitable relief by private plaintiffs. Such an action must be brought within two years of the date of the act complained of or the date of discovery of the harm. The minimum amount of harm required to bring such an action is $5,000 of losses within a one year period.

4. Access Device Statute

The Access Device Statute criminalizes the possession of counterfeit access devices knowingly and with intent to defraud that affects interstate or foreign commerce.[27] In the case of *Ivanov* and future potential cyber-extortion cases, the acquisition of customer credit card numbers and merchant account numbers constitutes a violation of this law.[28]

5. Conspiracy

Even if a cyber-extortion attempt does not result in the victim transferring something of value to a would-be extortionist, the fact that steps are taken to commit the crime constitute in themselves the crime of conspiracy.[29] One of the counts against Ivanov was based on the federal conspiracy statute.[30]

C. What Could Also Work

In addition to the preceding statutes that have been proven to be applicable to cyber-extortion by the case of *U.S. v. Ivanov*, the following statutes and common law doctrines may allow for prosecuting and recovering damages from cyber-extortionists.

1. Racketeer-Influenced and Corrupt Organizations Act

[27] 18 U.S.C. § 1029 (2000).
[28] *Ivanov*, 175 F. Supp. 2d at 370, 375.
[29] In 1909 Congress enacted the first general aiding and abetting statute applicable to all federal criminal offenses, providing that "those who provide knowing aid to persons committing federal crimes, with the intent to facilitate the crime, are themselves committing the crime." *Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 181 (1994) (citing to *Nye & Nissen v. U.S.*, 336 U.S. 613, 619, 1949).
[30] Specifically, *Ivanov* was charged with conspiracy to commit offense or to defraud under 18 U.S.C. § 371.

Because cyber-extortionists are becoming better organized, more coordinated and may be shown to demonstrate patterns of criminal conduct, the Racketeer-Influenced and Corrupt Organizations Act (RICO), the federal organized crime statute, is relevant.[31] According to Daniel B. Kelly, RICO has recently become "the preferred legal weapon for establishing criminal and civil liability in a panoply of situations involving allegedly extortionate conduct. Prosecutions for extortion under RICO originally targeted so-called 'organized crime enterprises' that intimidate legitimate business owners for money."[32] RICO allows for both government prosecutions and private lawsuits of organized extortion groups and for the recovery of treble damages.

2. Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 (ECPA)[33] updated the legal framework governing the surveillance of oral and wire communications established in the Omnibus Crime Control and Safe Streets Act of 1968.[34] The ECPA provides criminal and civil penalties for accessing, obtaining or altering electronic communication without permission.[35] Therefore, while not relied upon in *Ivanov*, ECPA could be another basis for prosecuting a cyber-extortionist.

---

[31] 18 U.S.C. §§ 1961-68 (2000). RICO was passed as Title IX of the Organized Crime Control Act of 1970. According to Gerald E. Lynch, RICO is controversial because of its harsh penalties and broad language, which has resulted in prosecutions that Congress may not have foreseen. Gerald E. Lynch, *RICO: The Crime of Being a Criminal. Parts I & II*, 87 COLUM. L. REV. 661, 661 (1987).

[32] Daniel B. Kelly, *Defining Extortion: RICO, Hobbs, and Statutory Interpretation in Scheidler v. National Organization for Women, Inc.*, 123 S. CT. 1057 (2003), HARV. J.L. & PUB. POL'Y 953 (Summer, 2003). Kelly cites to the following recent examples: *United States v. Corrado*, 304 F.3d 593 (6th Cir. 2002) (upholding convictions of Detroit Mafia for conspiracy and extortion under the Hobbs Act and RICO); *United States v. DiDomenico*, 78 F.3d 294 (7th Cir. 1996) (upholding convictions of Chicago Mafia for extortion, bribery, and murder under RICO); *United States v. Eufrasio*, 935 F.2d 553 (3d Cir. 1991) (upholding convictions of organized criminals for racketeering, RICO conspiracy and attempted extortion).

[33] 18 U.S.C. §§ 2701-2712 (2000).

[34] COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD (CSTB) & NATIONAL ACADEMY OF ENGINEERING (NAE), *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues*, Stewart D. Personick and Cynthia A. Patterson, *eds.,* (National Academy of Sciences, 2003).

[35] While the USA PATRIOT Act (discussed in Part III.A.8.) removed certain restrictions upon government surveillance of electronic communications, those changes are not relevant to the restrictions against non-governmental interference with electronic communication. *See* William F. Zieske, *Demystifying the USA Patriot Act*, 92 ILL. B.J. 82 (February, 2004).

3. The Travel Act and Interstate Transmission of Threats to Injure Another's Reputation

Interstate travel in order to promote extortion violates the Travel Act.[36] Transmitting threats to injure another person's reputation across state lines with the intent to extort money is also a crime.[37] While it is possible to threaten or complete a cyber-extortion without violating either of these statutes, they conceivably could constitute additional grounds for prosecution.

4. Other Criminal Statutes at the Federal and State Level

There are other federal statutes that could constitute grounds for prosecuting a cyber-extortionist that were not originally intended for online environments.[38] It also bears mentioning that cyber-extortionists may be prosecuted using state cybercrime statutes.[39] There are also a variety of other statutes at the federal and state level that specifically criminalize the unauthorized disclosure of private information, as discussed below in the context of the businesses' and executives' duties to consumers and employees in Part III.A. Where a cyber-extortionist accesses or misuses private information, there may be grounds for prosecution in federal and state privacy laws.

5. Civil Liability of Cyber-Extortionists

The civil suit provisions of the CFAA present the strongest foundation for a lawsuit to recover damages.[40] This Part reviews other possible bases for civil liability. However, as a practical matter, it is often difficult to identify or bring a civil suit against cyber-extortionists, especially those who operate outside of the United States.[41] Further, cyber-extortionists may lack adequate financial resources to compensate their victims. Therefore, although the following

[36] 18 U.S.C. § 1952 (2000).
[37] 18 U.S.C. § 875 (2000).
[38] For example, the Espionage Act, 18 U.S.C. §§ 793, 794 and 798 (2000), the Wire Fraud Act, 18 U.S.C. § 1343 (2000), and the Economic Espionage Act, 18 U.S.C. § 1831 (2000) could all possibly be violated by a cyber-extortion scenario, as suggested in *Critical Information Infrastructure Protection and the Law: An Overview of Key Issue, supra* note 34 at 36.
[39] An exhaustive state-by-state review of computer crime statutes is outside of the practical scope of this article, and there are a number of online compilations of state computer crime laws. *See, e.g.,* Computer Crime Statutes State by State, *available at* http://www.onlinesecurity.com/forum/article46.php (last visited January 2, 2007); Computer Crime Laws by State *available at* http://nsi.org/Library/Compsec/computerlaw/statelaws.html (last visited January 2, 2007).
[40] *See supra*, Part II.B.3.
[41] When an extortionist is not in the U.S. and cannot be lured into the U.S., the extradition process is available for a criminal prosecutor to forcibly bring an extortionist into the U.S., assuming that the extortionist can be located and apprehended abroad. However, nothing similar to the extradition process exists for forcing a foreign extortionist to appear before a U.S. court in a civil suit.

tort theories may be viable bases for lawsuits, they may not be practical means for victims to seek redress for the harms that arise in the context of a cyber-extortion.

a. Trespass to Personal Property

Common law actions for trespass to personal property have been successful in the context of electronic communications.[42] Because DDoS attacks often involve a website or information system becoming incapacitated by barrages of unwelcomed e-mails to an e-mail account, decisions such as *CompuServe, Inc. v. Cyber Productions, Inc.*[43] are particularly relevant. In this decision, a federal district court found that unwanted e-mails constituted a trespass to personal property, or chattel.[44] Similarly relevant is the decision in *eBay, Inc. v. Bidder's Edge, Inc.*, which found trespass to personal property when a website's speed was degraded by a program scouring a victim website and collecting information.[45]

The tort of trespass to chattel requires that there be intent and a showing that there was actual harm.[46] As elaborated upon below in Part III.B.3., the requirement that there be proof of harm has recently been reasserted. Therefore, while some courts have appeared not to strictly enforce this requirement, a plaintiff would be most likely to succeed in a recovery for trespass to personal property where the plaintiff could prove substantial damages.[47] The initial, willful hacking of a computer system for the purposes of presenting a credible threat would probably not be grounds for a suit against a would-be cyber-extortionist based on trespass to personal property

[42] For a compilation of cases from six states and four federal circuit courts of appeal finding that common law trespass claims are viable in the context of electronic communications. *See* Marjorie A. Shields, *Applicability of Common-Law Trespass Actions to Electronic Communications*, 107 A.L.R.5th 549 (2003).

[43] 962 F. Supp. 2d 1015 (S.D. Ohio 1997). Some have pointed out that the case of *Thrifty-Tel, Inc. v. Bezenek,* 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996), was the first case to find that a cause of action exists for trespass to chattels in the context of hacking into a computer, and that parents could be held liable for the hacking of their child.

[44] For a discussion of the reasoning and implications of the *CompuServe* decision, *see* Steven E. Bennett, *Canning Spam: CompuServe, Inc. v. Cyber Promotions, Inc.*, 32 U. RICH. L. REV. 545 (1998).

[45] 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

[46] *See* Shields, *supra* note 43 at 549. *See infra* Part III.B.3. for an elaboration upon the precise differences among courts in terms of their practical approaches to finding whether a trespass to personal property has occurred.

[47] In *School of Visual Arts v. Kuprewicz,* 771 N.Y.S.2d 804 (N.Y. Sup. 2003), the trespass to chattels was the unwelcomed receipt of job applications and pornography that breached no security systems, but did place a burden on the computer systems. The trial and appellate courts in *Intel Corp. v. Hamidi* also illustrated the trend of courts to not require a showing of damages to find a trespass to chattels by even ordering an injunction after a plaintiff ceased pursuing a lawsuit, but the California Supreme Court reversed those decisions. *See* 30 Cal.4th 1342, 1 Cal.Rptr.3d 32 (Cal. 2003). The *Hamidi* decision has been interpreted by practitioners nationwide as reasserting the requirement that damages be proven when attempting to recover for a trespass to personal property, according to Dr. Christopher T. Pierson. Correspondence with Dr. Christopher T. Pierson, March 20, 2006). For a discussion of how the damage requirement in trespass cases in the online context was being abrogated prior to the *Hamidi* decision, *see* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439 (2003).

because the lack of significant measurable harm would amount to the failure to demonstrate one of the essential elements of the tort.

b. Interference with Contractual Relations

Jerry Wegman and Alexander Korzyk raise the possibility that the tort of interfering with contractual relations may be viable as a claim in the context of DDoS attacks.[48] As they explain, the tort requires proof of a legally enforceable contract existing between two parties, and that a third party unjustifiably interfered with the execution of that contract. They offer the case of *Pennzoil Co. v. Texaco, Inc.*[49] as an illustration, wherein Texaco was held liable for inducing Getty Oil Co. to breach its contract agreeing to merge with Pennzoil, resulting in damages of $11 billion. Wegman and Korzyk point out that the perpetrators of DoS attacks are interfering with contracts between websites and their customers and between customers and their Internet Service Providers.

The likelihood of success of a lawsuit based exclusively on this theory would be low compared to using the civil suit provisions of the CFAA. First, this variety of tort requires that an extortionist intentionally made someone break a contract.[50] Second, this variety of tort typically involves someone interfering with a contractual relationship with the intent to replace one of the contracting parties.[51] In these two respects, an extortion scenario differs significantly from the paradigm illustrated by *Pennzoil v. Texaco*.

c. Invasion of Privacy

Daniel J. Solove suggests that there may be grounds for a lawsuit based on the tort of public disclosure of private facts because some cyber-crime scenarios may involve the fulfillment of a threat to divulge or sell or use confidential customer data that is of a highly personal or sensitive nature.[52] In a majority of states, a person has a cause of action for public

---

[48] Jerry Wegman & Alexander D. Korzyk, *Internet Denial of Service Attacks: Legal, Technical and Regulatory Issues*, JOURNAL OF LEGAL, ETHICAL AND REGULATORY ISSUES, Vol. 7, No. 1 (2004), *available at* http://www.cbe.uidaho.edu/wegman/blaw265/DOS%20paper%20AA%202003%20web.htm (last visited January 2, 2007).
[49] 481 U.S. 1 (1987).
[50] 18 AM. JUR. TRIALS 57 *Actions For Interference With Contract Rights* §9 (2006).
[51] *Id.* at §10.7.
[52] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967 (2003) (*see* pages 972-973 for a discussion of the public policy concerns related to disclosure of personal information and free speech rights).

disclosure of personal information when another widely discloses a private matter that is "highly offensive to a reasonable person" and "is not of legitimate concern to the public."[53] This tort allows lawsuits for disclosing true information even if the information was obtained through lawful means.[54] Arguably, the broad category of tort known as invasion of privacy[55] has an easier-to-prove sub-category called intrusion upon seclusion.[56] This may be more desirable grounds upon which to base a lawsuit against a cyber-extortionist because the unauthorized acquisition of private information is the key element; proof of publicity of the information is not required to win damages.[57]

In the context of cyber-extortion, these torts would provide for the recovery of damages against the extortionist, but not the company that fails to adequately protect confidential customer data. This is because an actionable disclosure does not take place when the disclosure is the result of an unlawful act of someone other than the defendant.[58] The case of *Corcoran v Southwestern Bell Tel. Co.* is instructive: the plaintiffs failed to establish publication by the telephone company where the company mailed their bill to the plaintiff's daughter-in-law's address (at the plaintiffs' daughter-in-law's request) and where the daughter opened the bill.[59] The court came to this conclusion because the opening of the misdirected bill was an intervening illegal act over which the telephone company had no control.[60] A court could find that, in the context of cyber-extortion, the extortionist's actions are a supervening illegality that eliminates the possibility of suing a corporation with negligently inadequate information systems security. However, the torts dealing with invasion of privacy could be viable bases for attempting to recover from cyber-extortionists that access or publicize private information.

Because cyber-extortionists are difficult to identify and apprehend and because they may lack sufficient resources to compensate for the damage that they cause, it is likely that the victims of cyber-extortion will seek redress for their harms from other sources. Both consumers and employees whose data may be compromised and businesses who suffer financial losses will

---

[53] RESTATEMENT (SECOND) OF TORTS § 652D (1977).
[54] Solove, *supra* note 52, at 971.
[55] RESTATEMENT (SECOND) OF TORTS § 652A (1977).
[56] RESTATEMENT (SECOND) OF TORTS § 652B (1977).
[57] *Id.*
[58] Sheila D'Ambrosio, *Invasion of Privacy By Public Disclosure of Private Facts,* 43 AM. JUR. PROOF OF FACTS 2D 449 (September 2005).
[59] 572 SW2d 212 (Mo. App. 1978).
[60] *Id.* at 215.

likely look to the institutions whose information systems became the tools for committing the harms. Namely, individuals whose data is accessed and misused will likely attempt to seek compensation from the businesses who failed to adequately secure the compromised information, and businesses who suffer losses will likely attempt to seek compensation from other businesses whose information systems were hijacked and used to cause harm. The focus of the following Parts is therefore upon the duties of executives to guard the privacy of information and to prevent their businesses' information systems from being used to cause harm.

## III. Duties and Liabilities of CEOs and CIOs

Executives' potential liability to third parties for failures in their duties to protect against cyber-attackers has been examined from a negligence perspective in one article in the Westlaw database.[61] Less than half a dozen other analyses of liabilities for allowing one's computers to be used as attack zombies in DDoS attacks are available online. The severe consequences of DDoS attacks are discussed slightly more in the IT arena, often in trade periodicals, and perhaps out of the motivation, in some instances, to sell information security services.

### A. Customers and Employees

The duties and possible liabilities of Chief Executive Officers (CEOs) and Chief Information Officers (CIOs) to consumers and employees are defined by statutes, regulations and common law doctrines. Since cyber-extortion may involve holding sensitive and private data hostage or threatening its misuse, destruction, publication or the disclosure of its being compromised, the issue of data privacy is significant in evaluating potential executive liability to third parties.

#### 1. No Federal Statute Controls When Individuals Must Be Notified of Data Privacy Breaches

As of early 2006, no federal law defines when customers or employees must be informed of an information security breach that compromises the privacy of their personal or otherwise

[61] Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, (Winter, 2002).

sensitive data.[62] Thus, even the FDIC delayed an announcement to its employees about the theft of personal information, partly to further its efforts in identifying the culprits.[63]

At least 30 pieces of relevant federal legislation have been proposed and were circulating in the U.S. Congress as of 2005, but none as of 2006 were close to being passed by the House or Senate.[64] However, there is a patchwork of differing reporting obligations to employees and customers created by 22 – soon to be as many as 39 – state statutes.[65] California's Security Breach Information Act [66] has been the object of commentary by both scholars and practitioners.[67] Companies doing business internationally should be cognizant of higher standards applicable to data privacy and the disclosure of data privacy breaches that exist in Europe.[68]

However, despite the lack of a consistent federal legal framework governing when disclosures must be made to customers about breaches to the confidentiality of sensitive data, as discussed in the following Parts, federal statutes and recently promulgated regulations impose duties on executives to maintain controls on the privacy of certain forms of information.[69] An up-to-date inventory of state privacy statutes is available online.[70]

---

[62] Glen Fest, *Data Breach Notification: States Differ On When To Sound The Alarm,* BANK TECHNOLOGY NEWS, January, 2006, *available at* http://www.banktechnews.com/article.html?id=20060103PM82XNSG (last visited January 2, 2007).

[63] *Id.* The discovery that the Department of Justice had made social security numbers available on the Internet was another event that prompted questions about how quickly enterprises must inform individuals about compromised private data. Larry Greenemeier, *InformationWeek Exclusive: Justice Department Reveals Social Security Numbers*, INFORMATIONWEEK, December 23, 2005, *available at* http://www.informationweek.com/news/showArticle.jhtml?articleID=175400150 (last visited January 2, 2007); Larry Greenemeier, *Social Security Numbers On The Justice Department's Web Site Could Lead To Identity Theft*, INFORMATIONWEEK, *available at* http://www.informationweek.com/blog/main/archives/2005/12/social_security.html (last visited January 2, 2007).

[64] Tony Kontzer & Larry Greenemeier, *Sad State of Data Security*, INFORMATIONWEEK, January 5, 2006, *available at* http://www.wstonline.com/showArticle.jhtml?articleID=175801687 (last visited January 2, 2007).

[65] *Id.*

[66] Cal. Civ. Code § 1798.82 (2003).

[67] *See* Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches,* 22 J. MARSHALL J. COMPUTER & INFO. L. 457 (Winter, 2004); Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1 (Fall 2003).

[68] *See* Preston & Turner, *supra* note 67, at 468.

[69] For a more extensive discussion of the justification for myriad federal and state statutes related to data privacy that are applicable to specific types of information, *see* Daniel J. Solove, *supra* note 52, at 972 (2003). Solove points to federal statutes that "restrict disclosure of information from school records, cable company records, video rental records, motor vehicle records, and health records. ... Various states have also restricted the disclosure of particular forms of information, such as data about health, alcohol and drug abuse, sexual offense victims, HIV status, abortion patients, and mental illness." *Id.* at 972 (footnotes omitted).

[70] ELECTRONIC PRIVACY INFORMATION CENTER, *Privacy Laws by State*, *available at* http://www.epic.org/privacy/consumer/states.html (last visited January 2, 2007).

2. Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002 (commonly referred to as SOX)[71] has generated extensive scholarly commentary,[72] but its relevancy to information security is relatively under-appreciated. Section 404 of SOX requires that internal controls on information systems be put in place and that they be documented and tested at least once a year.[73] Section 302 of SOX requires the company's principal officers to certify each annual and quarterly report with respect to their review of the report and the internal controls now mandated by the Act. Section 906(a) of SOX requires CEO and CFO certification of the veracity of each periodic report that contains financial statements, with criminal penalties for failure to comply. "Knowing" violations of a CEO's or CFO's certification duties are punishable by up to $1 million in fines or up to 10 years' imprisonment.[74] "Willful" violations of a CEO's or CFO's certification duties are punishable by up to $5 million in fines or 20 years' imprisonment. SOX provides for both civil and criminal penalties. Corporate executives – and even directors – may be not only exposed to criminal liability, but also to suits by private citizens in court.[75]

The requirements that executives either confirm that adequate "internal controls" are in place has led to a burgeoning market in information technology (IT) systems claiming to be "Sarbanes compliant," inasmuch as the systems are secured from both internal and external

---

[71] Pub. Law No. 107-204, 116 Stat. 745 (codified as amended at 15 U.S.C. §§ 7201-7266 (2005) and in scattered sections of 18 U.S.C., 28 U.S.C. & 29 U.S.C.). Elsewhere SOX has been referred to as the Corporate and Criminal Fraud Accountability Act of 2002. *See,* e.g. Robert P. Riordan and Lisa Durham Taylor, *Sarbanes-Oxley Whistleblower Claims: Fast Start or Fizzle*, *available at* http://www.lawmemo.com/articles/sox.htm (last visited January 2, 2007).

[72] *See, e.g.*, Andrew A. Lundgren, *Sarbanes-Oxley, Then Disney: the Post-Scandal Corporate-Governance Plot Thickens*, 8 DEL. L. REV. 195, (2006); Roberta Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance,* 114 YALE L.J. 1521 (May, 2005); Byron F. Egan, *The Sarbanes-Oxley Act and Its Expanding Reach,* 40 TEX. J. BUS. L. 305 (Winter, 2005); Larry Catá Backer, *Surveillance and Control: Privatizing and Nationalizing Corporate Monitoring After Sarbanes-Oxley*, 2004 MICH. ST. L. REV 327; Niels Schaumann, *The Sarbanes-Oxley Act: A Bird's Eye View*, 30 WM. MITCHELL L. REV. 1315 (2004).

[73] For a more in-depth discussion of duties created by the Sarbanes-Oxley Act, *see* Larry Catá Backer, *The Duty to Monitor: Emerging Obligations of Outside Lawyers and Auditors to Detect and Report Corporate Wrongdoing Beyond the Federal Securities Laws*, 77 ST. JOHN'S L. REV. 919 (Fall 2003).

[74] For a discussion of the legislative history of the Sarbanes-Oxley Act and, to a certain extent, the relatively greater significance of corresponding federal sentencing commission guidelines *see* Frank O. Bowman, III, *Pour Encourager les Autres? The Curious History and Distressing Implications of the Criminal Provisions of the Sarbanes-Oxley Act and the Sentencing Guidelines Amendments that Followed*, 1 OHIO ST. J. CRIM. L. 373, 405 (2004).

[75] It is important to note, however, that the SEC's ability to impose civil liability on directors is subject to the same standard as under any other statute. *See* Nicolas Morgan, *Court Rejects SEC's Imposition of Civil Penalties against Directors in Early Test of Sarbanes-Oxley*, *available at* http://www.dlapiper.com/files/upload/CorpGov_051123.htm (last visited January 2, 2007).

tampering.[76] The obligation to confirm the status of internal control systems coupled with the threat of both criminal and civil sanctions has raised the possibility that SOX lawsuits, like RICO civil suits, will successfully be initiated in contexts that were not contemplated by legislative drafters.[77]

A single vulnerability of an internal control of a corporation that is exploited to cause harm to third parties may now conceivably result in (1) the CEO, CFO and company being sued by a defrauded third party, such as a customer; (2) the CEO, CFO, company and its accounting firm being sued in a class action lawsuit brought by public shareholders; (3) an accounting firm suing the CEO and CFO for failing to disclose the vulnerability and (4) the Securities and Exchange Commission bringing civil and criminal proceedings against the company and its CEO and CFO.[78]

Interestingly, a recent survey of fraud examiners revealed widespread perceptions that (1) SOX has been effective in revealing frauds, yet (2) fraud in the corporate world is still a major and worsening problem and (3) bribery and extortion still rank among the most prevalent forms of financial fraud.[79] While the context of SOX's passage and its content indicate that the act was intended to combat corporate fraud, the mandated maintaining of internal controls guards corporations against external bad actors as well – including those bent on extortion. The discovery of an executive's false assurance of adequate internal controls and monitoring is grounds for liability, regardless of how that false assurance comes to light.

One indication of how seriously executives have taken the prospect of being sued or prosecuted for maintaining inadequate internal controls is their expenditures on SOX-compliant IT systems. A recent survey by the Gartner Group has found that IT budgets grew by 10 to 15 percent in 2006, up from an increase of 5 percent in 2004.[80] "Projects that were not aligned with compliance and corporate governance were delayed or cancelled, and SOX efforts inhibited the

---

[76] Mark Rasch, *Sarbanes Oxley for IT Security?* THE REGISTER, May 3, 2005, *available at* http://www.theregister.co.uk/2005/05/03/sarbanes_oxley_for_it_security/ (last visited January 2, 2007).
[77] J. Brent Wilkins, *The Sarbanes-Oxley Act of 2002: The Ripple Effects of Restoring Shareholder Confidence*, 29 S. ILL. U. L.J. 339, 346 (2004/2005).
[78] John S. Vishneski, III, *New Liabilities Created By Sarbanes-Oxley; Are Your Directors, Officers Covered? available at* http://www.mayerbrownrowe.com/publications/article.asp?id=1179&nid=6: (December 1, 2003) (last visited January 2, 2007).
[79] Gene J. Koprowski, *Study: Sarbanes-Oxley Law Not Changing Technology Business Culture*, TECHNEWSWORLD, http://www.technewsworld.com/story/47467.html (last visited January 2, 2007).
[80] Dinesh C. Sharma, *Compliance laws boosting IT budgets*, MSN TECH & GADGETS, *available at* http://msn.com.com/2100-9595_22-5996670.html (last visited January 2, 2007).

purchase of large amounts of software related to building new technologies and deploying new projects," stated French Caldwell, a Vice President of Research at Gartner.[81]

3. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act of 1999 (GLBA)[82], facilitated affiliations between banks, securities firms, and insurance companies by repealing provisions of the Glass-Steagall Act.[83]

GLBA controls the ways that financial institutions deal with the nonpublic personal information of individuals. The Act consists of three sections: The Financial Privacy Rule regulates the collection and disclosure of private financial information; the Safeguards Rule stipulates that financial institutions must implement security programs to protect such information; and the pretexting provisions prohibit the practice of accessing private information using false pretenses. The Act also requires financial institutions to give customers privacy notices that explain their information-sharing practices.[84]

The Federal Trade Commission was empowered to enforce GLBA by 15 U.S.C. § 6805(a)(7) and promulgated regulations in 2000.[85] The FTC rules implemented GLBA and also provided sample compliance privacy notes.[86]

As noted by the Federal District Court for the District of Maryland in *F.T.C. v. AmeriDebt, Inc.*, GLBA and related regulations define financial institutions "very broadly."[87] Universities and other enterprises that deal with a variety of financial records also fall under the ambit of GLBA and therefore have a responsibility to secure personal records. GLBA directs that all institutions implement an Information Security Program and designate a program coordinator.

The greatest limitation of GLBA from the view of privacy advocates is that it does not provide any remedies for individuals should a firm fail to comply with the Act's disclosure

[81] *Id.*
[82] 15 U.S.C. § 6801 *et seq.* GLBA is also known as the Financial Industries Modernization Act.
[83] The FTC tried to use GLBA as a basis for regulating lawyers, but this was rejected by U.S. Court of Appeals for the District of Columbia. *N.Y. State Bar Ass'n v. FTC*, 2004 WL 964173, at 3 (D.D.C. Apr. 30, 2004).
[84] 15 U.S.C. § 6803(a).
[85] For a succinct analysis of the regulations implementing the GLBA, *see* L. Richard Fischer, *The Gramm-Leach-Bliley Act and Its Implementation*, SG066 ALI-ABA 65 (2002).
[86] 16 C.F.R. § 313.18 (2002).
[87] 343 F.Supp.2d 451 (2004) at 457.

provisions.[88] According to GLBA, executives may be subject to enforcement actions of state insurance authorities, federal regulators and the Federal Trade Commission.[89] However, according to Section 505(b)(1), enforcement equates to implementation of standards.[90] As one commentator pointed out, "the law establishes ... overlapping regulatory supervisory enforcement mechanisms to identify and correct abusive policies and practices rather than to remedy or resolve individual rights affected by specific infractions. The structure is thus somewhat illusory, lacking in any recourse for an individual to remedy the infringement of his or her privacy."[91] In the words of Jolina C. Cuaresma, "Without the threat of monetary remuneration, adherence to these privacy provisions may not be a high priority for firms faced with a barrage of economic pressures. This lack of remedies further compromises the individual's right to privacy."[92]

4. Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[93] originally had three main goals: (1) to guard patients' protected health information from unauthorized disclosures; (2) to improve the quality of healthcare by restoring trust in the system; and (3) to protect and improve the rights of consumers to access their own healthcare information.[94]

HIPAA required the Secretary of the Department of Health and Human Services (HHS) to recommend privacy measures to Congress.[95] HIPAA's Administrative Simplification provisions required the establishment of standards for electronic health care transactions and the security and privacy of health data. Requirements for administrative, physical and technical safeguards for ensuring the privacy of health data took effect April 20, 2005.[96]

---

[88] Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 514 (2002), citing to 15 U.S.C. § 502(e)(3)(C).
[89] 15 U.S.C. § 505.
[90] *Id.* § 505(b)(1).
[91] David W. Roderer, *Tentative Steps Toward Financial Privacy*, 4 N.C. BANKING INST. 209, 213 (2000).
[92] Cuaresma, *supra* note 88 (footnotes omitted).
[93] Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C.; 26 U.S.C.; 29 U.S.C.; 42 U.S.C.) (2003).
[94] David R. Morantz, *HIPAA's Headaches: A Call for a First Amendment Exception to the Newly Enacted Health Care Privacy Rules*, 53 U. KAN. L. REV. 479 (January, 2005).
[95] For a description of the long history of the promulgation of the HIPAA privacy standards, *see Id.*
[96] 45 C.F.R. §160, §164 (2002). *See* Pietrina Scaraglino, *Complying With HIPAA: A Guide for the University and Its Counsel*, 29 J.C. & U.L. 525 (2003).

"Protected Health Care Information," includes any "individually identifiable information concerning the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for that provision of health care to an individual."[97] The law states that "covered entities" include health care providers, health plans (which include group plans), insurance companies, parts of Medicare, Medicaid, long-term care providers, and health care clearinghouses, which process health data and provide billing services. However, employee welfare benefit plans and entities such as universities are covered.[98] The law requires covered entities that transmit, process, or disclose protected health information to limit such disclosures to the minimum amount necessary, known as the "minimum necessary" information.

A single unintentional violation of the law is punishable by a $100 fine,[99] but multiple violations in one calendar year can result in a $25,000 fine;[100] therefore, these provisions could affect businesses if confidential health care data is compromised in the course of a cyber-extortion. However, HIPAA regulations do not create a private right of action to recover damages from keepers of medical records who unintentionally disclose a record.[101] Instead, private parties have the right to file a formal complaint with a covered provider or health plan or with HHS about violations of the provisions of this rule or the policies and procedures of the covered entity.[102]

5. Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act of 1998 (COPPA)[103] requires companies that use websites to collect data about children under 13 years of age to (1) give clear notice of the type and use and disclosure of information collected, (2) allow ways for parents to easily review collected information and (3) limit collected information to what is reasonably

[97] Diane Kutzko et al., *HIPAA in Real Time: Practical Implications of the Federal Privacy Rule*, 51 DRAKE L. REV. 403, 411 (2003) (citations omitted). This article provides a thorough analysis of the statute's provisions.
[98] *See* Scaraglino, *supra* note 96.
[99] 42 U.S.C. § 1320d-5(a)(1) (2000).
[100] *Id.*
[101] 45 C.F.R. §160, §164 (2002).
[102] U.S. Department of Health and Human Services, *Protecting the Privacy of Patients' Health Information*, *available at* http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm (last visited January 2, 2007).
[103] 15 U.S.C. §§ 6501-6505 (2004).

necessary.[104] Companies must also obtain verifiable parental consent before collecting personal information of children under 13 years old.[105]

Of greatest significance to the present analysis, companies must maintain the confidentiality of the personal data that they collect on children under 13 years of age.[106] COPPA empowers the Federal Trade Commission (FTC) to oversee implementation and enforcement of the regulations[107] but, like GLBA and HIPAA, does not create a right for private parties to file a civil suit.[108] The final implementing rule went into effect on April 21, 2000.[109] FTC enforcement actions have led to companies paying up to $400,000 for violating COPPA.[110] Given that cyber-extortionists may disclose or threaten disclosure of companies' personal data about children, COPPA's penalty provisions could apply to a company that failed to protect the confidentiality of its data.

6. Unfair Trade Practices and the Fair and Accurate Credit Reporting Act

It is important to note the role of the Federal Trade Commission (FTC) in enforcing previously discussed legislative and regulatory security requirements. Another part of the FTC's mission is protecting consumers from false and deceptive trade practices.[111]

The Federal Trade Commission has prosecuted and settled with several companies – Eli Lilly, Microsoft, Guess, and Tower Records – for misrepresentations to consumers that security and privacy measures were more robust than they really were.[112] New York's Attorney General has also prosecuted and settled with several businesses, including Ziff Davis, Barnes & Noble,

---

[104] 15 U.S.C. § 6502(b)(1)(B)(i)-(iii). For a concise summary of COPPA, *see* Rachael Malkin, How the Children's Online Privacy Protection Act Affects Online Businesses and Consumers of Today and Tomorrow, 14 LOY. CONSUMER L. REV. 153 at 156-159 (2002) or Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751 (Fall 2001). For a description of how businesses were collecting and selling personal data on children under the age of 13, *see* Michelle Z. Hall, *Internet Privacy or Information Piracy: Spinning Lies on the World Wide Web*, 18 N.Y.L. SCH. J. HUM. RTS. 609 (2002).

[105] 15 U.S.C. § 6502(b)(A)(ii), (B)(iii).

[106] 15 U.S.C. § 6502(b)(1)(D).

[107] 15 U,S.C. § 6505(a).

[108] COPPA is not cited to as frequently in analyses of the possible liability of businesses for maintaining lax security standards or in reviews of statutes that are having an impact upon industry practices. One authority that discusses COPPA is Preston & Turner, *supra* note 67, at 478 (Winter, 2004). As reflected by the number of authorities cited in the corresponding Parts of this article, GLBA and HIPAA are more commonly cited as having affected both perceptions of what constitutes a reasonable standard of care and the actual functioning of businesses.

[109] FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (1999).

[110] Steven A. Wells, Mark Courtney, Peter Vogel, *[Un]Safe Harbor: No Common Denominator in Privacy Compliance*, 9 COMPUTER L. REV. & TECH. J. 257, 270 (Fall, 2004).

[111] Federal Trade Commission Act, 15 U.S.C. § 45(a) (2003).

[112] *See* Preston & Turner, *supra* note 67, at 478.

Victoria's Secret and the ACLU for making misrepresentations about or compromising the privacy of customer data.[113]

It is important to note that the FTC settlements have clarified how GLBA and HIPAA's information security requirements may be satisfied in practice. As summarized in the Computer Science and Telecommunications Board's (CSTB) and National Academy of Engineering's (NAE) *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues*:

> Recent FTC settlements have established "reasonable security" as a written, comprehensive information security program that (1) designates appropriate personnel accountable for information security, (2) assesses security risks, taking into account, among other things, employee training, (3) implements reasonable security safeguards to control risks, and (4) adjusts the information security program in response to regular testing and monitoring. The GLB implementing regulations and recent FTC actions go a long way to setting the stage for best practices and may give rise to a de facto industry standard for negligence liability. However, a number of questions remain about the FTC's *de facto* security standard. It is not clear whether ISO 17799 meets these requirements. Nor is it known what types of documentation, training, and supervision are necessary to meet the standard. The Microsoft settlement appears to indicate that damage is not necessary to trigger an FTC inquiry and the imposition of its security standard. Clearly, though, the recent FTC actions, combined with the GLB and HIPAA regulations, confirm that companies can no longer continue to address security issues informally. GLB and HIPAA regulations have caused a seismic shift in the financial and health care industries (similar to the effect of Y2K on the computer industry) as institutions scramble to comply with the detailed requirements.[114]

More recently, the settlements of the FTC's actions against ChoicePoint, BJ's Wholesale and DSW indicated that the very lack of information security safeguards – regardless of whether promises about data privacy were made – are grounds for prosecution as unfair trade practices

[113] *See Id.*
[114] CSTB & NAE, *supra* note 34 at 58.

when data is stolen.[115] In its case against ChoicePoint, the FTC charged that the database company violated the Fair Credit Reporting Act (FCRA) by furnishing consumer reports to subscribers who did not have a permissible purpose to obtain them and by failing to maintain reasonable procedures to verify the identities of the requesting entities and how they intended to use the information.[116] The settlement involved Choicepoint paying $15 million in penalties and agreeing to external security audits every two years.

In its settlements with BJ's Wholesale[117] and DSW[118], the FTC similarly showed that failure to take appropriate security measures to protect sensitive information may constitute an unfair practice that violates federal law. The settlements with both companies require them to implement a comprehensive information security program and obtain audits by an independent third party security professional every other year for 20 years.[119]

The prosecutions of BJ's Wholesale and DSW suggest that a viable *de facto* standard of care for securing information exists, and is violated by the following acts and omissions: storing sensitive information longer than a legitimate business need would so require, failing to use readily available technology to limit access to computer networks through wireless access points, failing to encrypt files and failure to employ sufficient measures to detect unauthorized access.[120] Failing to limit the connectivity between computers in different stores was also a basis for prosecuting these cases.[121]

---

[115] The FTC's enforcement actions against Choicepoint, BJ's Wholesale and DSW were all based on the Federal Trade Commission Act, 15 U.S.C. § 45(a) (2003).

[116] 163,000 consumers' personal financial records were compromised. *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress,* FTC Press Release No. 052-3069 (January 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm (last visited January 2, 2007).

[117] *BJ'S Wholesale Club Settles FTC Charges,* FTC Release, File No. 0423160 (June 16, 2005), *available at* www.ftc.gov/opa/2005/06/bjswholesale.htm (last visited January 2, 2007); decision and order and consent order and analysis are available at www.ftc.gov/os/caselist/0423160/0423160.htm (last visited January 2, 2007).

[118] *DSW Inc. Settles FTC Charges*, FTC Release, File No. 052-3096 (December 1, 2005), *available at* www.ftc.gov/opa/2005/12/dsw.htm, (last visited January 2, 2007); decision and order and consent order and analysis are available at http://www.ftc.gov/os/caselist/0523096/0523096.htm (last visited January 2, 2007).

[119] *In re BJ's Wholesale Club*, FTC Order No. 0423160, *available at* www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf (last visited January 2, 2007); *In re DSW, Inc.,* FTC Order No. 0523096, *available at* http://www.ftc.gov/os/caselist/0523096/051201agree0523096.pdf (last visited January 2, 2007).

[120] As with standards of care other contexts, this standard should not automatically be deemed to have been violated anytime there is a data security breach; rather, the FTC appears to be pursuing cases where there was a failure to take reasonable precautions. *See* Anne P. Fortney, Lisa C. DeLessio, *Federal Laws Applicable to Consumer Data Security Breaches*, 59 CONSUMER FIN. L.Q. REP. 229, 237 (Fall 2005).

[121] FTC Release, *supra* note 117; FTC Release, *supra* note 118.

7. Fair and Accurate Credit Transactions Act and the FTC's Disposal Rule

The Fair and Accurate Credit Transaction Act (FACTA) of 2003[122] amended the federal Fair Credit Reporting Act (FCRA)[123] and included provisions intended to enhance the accuracy and privacy of data, limit information sharing, and expand consumer rights to disclosure.[124] The Disposal Rule, passed by the FTC in July, 2005 as required by FACTA, calls for the disposal of information by, among other means, the destruction or erasure of electronic files containing consumer records to protect against unauthorized access or use of the information.[125] Significantly, the rule applies not just to businesses that acquire data through consumer transactions, but to landlords, employers, insurers, attorneys and private investigators, among others.[126] The Disposal Rule effectively defines another element of the duty of care that a business must fulfill if it wishes to meet the FTC's standard of taking reasonable care to prevent data theft or misuse.

8. USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001[127] reformed the Banking Secrecy Act (BSA).[128] Section 3, Title III of the USA PATRIOT Act and new regulations implementing the act require key financial sector industries to implement programs and employee training designed to prevent the services they offer from being used to facilitate money

---

[122] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003) (amending 15 U.S.C. §§ 1681-1681x; 20 U.S.C. §§ 9701-9708; and 31 U.S.C. § 5318 (2004)).

[123] Fair Credit Reporting Act, Pub. L. No. 104-208, 110 Stat. 3009 (1996) (current version at 15 U.S.C. § 1681 (2004)).

[124] It has been pointed out that while FACTA includes protections advantageous to consumers, it also preempts state laws that could go further in protecting consumers. *See* National Consumer Law Center, *Analysis of the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (2003)*, *available at* www.nclc.org/initiatives/facta/nclc_analysis.shtml (last visited January 2, 2007). There are some ways that states may still go beyond minimum federal protections. *See* Gail Hillebrand, *After the FACT Act: What States Can Still Do to Prevent Identity Theft* CONSUMERS UNION, *available at* www.consumersunion.org/pub/core_financial_services/000756.html (last visited January 2, 2007).

[125] FTC Disposal Rule, 16 C.F.R. § 682 (2005), *available at* http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf (last visited January 2, 2007); *further explanation available at* http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.htm (last visited January 2, 2007).

[126] *Id.*

[127] Pub. L. No. 107-56, 115 Stat. 272-402 (codified at 18 U.S.C. § 1960 and in other amended sections of the U.S. Code).

[128] Pub. L. No. 91-508, 84 Stat. 1114- 36 (codified as amended at 12 U.S.C. §§ 1730d, 1829b, 1951-1959; 18 U.S.C. §§ 6002; and 31 U.S.C. §§ 321, 5311-5314, 5316-5322).

laundering or the financing of terrorism.[129] A management-level compliance officer must be responsible for the institution's anti-money-laundering activities and must have independent board-level reporting authority.[130] Enterprises must actively monitor individual accounts to detect suspicious activity and must submit Suspicious Activity Reports and Currency Transaction Reports.[131] These reforms also require that enterprises providing financial services[132] retain data for five years and stipulate that reported-on individuals do not need to be informed.[133]

In examinations of banks for compliance, even five errors out of 1,500 transactions justified a bank being failed and in one federal reserve district, all 15 banks failed.[134] This indicates that the heightened regulatory requirements requiring greater scrutiny of accounts and longer periods of data retention have not yielded complete compliance. Most importantly, these statutory and regulatory requirements constitute an important piece of the legal obligations of executives with regard to the data systems of their enterprises.

9. State Consumer Protection Statutes

State consumer protection statutes may also be applicable to false promises of data privacy protection. Just as the FTC actions described above were based on federal laws prohibiting unfair trade practices, even when there was no reliance upon a false promise,[135] reliance upon false promises may not be necessary to prove an unfair trade practice under a state consumer protection statute. Rather, inadequate data security provisions alone may be adequate to demonstrate an unfair trade practice. While an attorney general could bring a prosecution,

[129] For up-to-date links to relevant regulations and compliance guidelines, *see* Office of the Comptroller of the Currency, Combating Money Laundering and Terrorist Financing: Bank Secrecy Act (BSA) and USA PATRIOT Act Regulations, *available at* http://www.occ.treas.gov/BSA/BSARegs.htm (last visited January 2, 2007).
[130] Ken Proctor, *Managing Compliance Risk: Bank Secrecy Act and the USA PATRIOT Act*, September 2, 2003, *available at* http://www.bankersonline.com/risk/brintech_cmprisk.html (last visited January 2, 2007).
[131] *Id.*
[132] Financial institutions are defined in the Bank Secrecy Act, 31 U.S.C. 5312(a)(2)(A) thru (X), as amended by the USA PATRIOT Act, and include not only banks but, for example, mutual fund companies, operators of credit card systems, money transfer companies and check cashers, securities brokers and dealers registered with the Securities and Exchange Commission, and futures commission merchants and accompanying introducing brokers registered with the Commodity Futures Trading Commission.
[133] 31 C.F.R. § 103 (2002).
[134] Proctor, *supra* note 130.
[135] *See supra*, Part III.A.6.

customers may bring actions to implement these statutory protections.[136] Harmed citizens may be entitled to treble damages or attorney's fees, incentivizing the use of these statutes to seek recovery, and exacerbating the exposure of business to liability when the confidentiality of customer data is breached.

10. Contract Law

Contract law is relevant where it can be demonstrated that a promise to keep information private was so essential to a purchase decision as to be a part of the basis of the bargain. If the data is made public – a breach of the promise to keep private information confidential – three possible remedies are conceivable. First, a court may allow the customer to rescind the contract[137] – that is, for example, to be absolved of any further obligations to make payments and receive benefits under a two-year cell phone contract. This could result in significant damages for cell phone service companies and similar services that rely on long-term contracts as a source of revenue. The second remedy under contract law is to award monetary damages to the plaintiff equal to the difference between the contracted goods or service as promised and the value of the goods and services as delivered – however, it may be difficult to assign such a value when the breach involves data being compromised.[138] Finally, in the event that foreseeable damages result from the violation of a promise, consequential damages are possible; these may present the most likely means of recovery in the context of someone suing to recover damages from the breach of a promise to keep data confidential.[139]

11. Torts

a. Torts of Fraudulent and Negligent Misrepresentation

If a business communicated that customer data would be kept private, then several types of tort liability may exist. Claims of tortious misrepresentation are based on the communication of false facts upon which a plaintiff relies to his or her detriment.[140] A concise differentiation of the three varieties of misrepresentation is as follows:

---

[136] Victor E. Schwartz & Cary Silverman, *Common-Sense Construction of Consumer Protection Acts,* 54 U. Kan. L. Rev. 1 (October, 2005).
[137] Andrew Kull, *Restitution As a Remedy For Breach of Contract,* 67 S. CAL. L. REV. 1465, 1514 (July, 1994).
[138] RESTATEMENT (SECOND) OF CONTRACTS, §344(a); UCC 1-106(1).
[139] RESTATEMENT (SECOND) OF CONTRACTS, §351.
[140] Richard H. Acker, *Choice-of-Law Questions in Cyberfraud,* 1996 U. CHI. LEGAL F. 437, n.12 (1996).

> Intentional misrepresentation, often called fraud or fraudulent misrepresentation or deceit, is an intentional tort requiring a showing that the defendant knowingly misrepresented the truth. Reckless misrepresentation – confusingly, also sometimes called intentional misrepresentation – occurs when the defendant is conscious that she doesn't know whether her assertions are true or false. And third, negligent misrepresentation may arise when a seller carelessly communicates information that she should know is false.[141]

All of these forms of misrepresentation would allow for the rescission of the agreement that was entered into based on the misrepresentations. Further, tort damages – more than conventional contractual remedies – typically allow for whatever damage award would place the plaintiff in the position he or she was in prior to the defendant's tortious conduct. In egregious cases where a court is convinced that future instances of such conduct ought to be deterred, punitive damages are possible.

Ethan Preston and Paul Turner argue convincingly that the privacy policies of businesses make them vulnerable for liability for both negligent misrepresentation and fraud because "businesses disclose their privacy policies in part to induce data subjects into transactions with the business and into providing them with information."[142]

b. Tort of Breach of Confidentiality

As pointed out by Daniel Solove, there is also the relatively new tort of breach of confidentiality which remedies disclosures of medical information by physicians and financial data by banks; liability under this tort has been extended to third parties who induce the disclosure.[143]

B. Downstream Liability to Other Businesses

---

[141] *See* J. David Prince, *Defective Products and Fraud and Misrepresentation Claims in Minnesota*, WILLIAM MITCHELL LEGAL STUDIES RESEARCH PAPER NO. 26 (September 2005) (abstract available on www.ssrn.com).
[142] Preston & Turner, *supra* note 67, at 478.
[143] Solove, *supra* note 52, at 971-972. Solove cites to *Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961) (disclosure by bank found to be tort of breach of confidentiality); *McCormick v. England*, 494 S.E.2d 431, 439 (S.C. Ct. App. 1997) (disclosure by physician found to be breach of confidentiality tort); *Hammonds v. AETNA Cas. & Sur. Co.*, 243 F. Supp. 793, 803 (N.D. Ohio 1965) (third party inducing disclosure found to be liable for tort of breach of confidentiality) and Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426 (1982).

Given that unsecured computer networks are hijacked and used to execute DDoS attacks as part of cyber-extortion schemes, that extortionists can be difficult to catch and may lack the resources to compensate their victims and that the owners of the unsecured networks may be identifiable and have the resources to compensate the victims, it is foreseeable that a victim of a cyber-extortion scheme involving a DDoS attack will sue the owners of the networks used to perpetrate the attack.

There is no statute that criminalizes allowing one's computer or network to be hijacked and used as a zombie to attack other computers or networks. However, there are doctrines and precedents that are applicable to this seemingly novel fact pattern. In the following Parts of this article, several avenues for establishing liability will be examined.

Some of the following applications of legal theories may seem like earnest speculation. Indeed, they are almost by definition speculative applications until a lawsuit is commenced that relies on these theories. To lend credibility to the following Parts and give credit where it is deserved, the following individuals must be recognized for their pioneering work on the issue of downstream liability for negligence in the context of DDoS attacks: Stephen E. Henderson and Matthew E. Yarbrough,[144] Robert Bourque and Blake Bell,[145] Ronald B. Standler,[146] and William J. Cook.[147] The authors are also indebted to Dr. Christopher Pierson for his practitioner's insights and expert opinions.

To date, there has been one lawsuit initiated against a company for allowing its website to be hacked and for the resulting damages to a third party. In this case, FirstNET, a Scottish Internet Service Provider, was flooded with traffic that was directed to it from the compromised website of Nike. FirstNET sued Nike in a Scottish court for the cost of redirecting traffic back to

---

[144] Henderson & Yarbrough, *supra* note 61.

[145] Robert Bourque and Blake Bell, C*omputer Owners Face Liability for On-Line Attacks*, N.Y.L.J., Aug. 11, 2000, at 1, *also available in essay form online as: Dealing with Liability Risks to Owners of Computers Used in Denial of Service Attacks at* http://www.stblaw.com/content/publications/pub289.pdf (last visited January 2, 2007).

[146] Ronald B. Standler, *Possible Vicarious Liability for Computer Users in the USA?* (2004) *available at* http://www.rbs2.com/cvicarious.pdf (last visited January 2, 2007).

[147] William J. Cook, Partner at Foley & Lardner LLP, Former Head of U.S. Department of Justice Computer Crime Task Force, *Liability Developments and Best Practices 2005*, presented at August 10, 2005 InfraGard National Conference, *available at* http://www.infragard.net/library/congress_05/regulatory_compliance/liability_developments.ppt#673,21 (last visited January 2, 2007); *The Legal Aspects of Cyberspace*, presentation at the Infragard Super Conference, May 15, 2003, *available at* http://www.wi-infragard.com/superconference.html (last visited January 2, 2007).

Nike.[148] At the time, in 2000, FirstNET also contemplated suing Nike in U.S. court on a tort theory for the damage suffered as a result of the disruption from the flood of traffic.[149] FirstNET reportedly withdrew its lawsuit and compensated Nike for an unspecified amount of "judicial costs."[150] This example demonstrates that, while the theories below have not been thoroughly tested, the concept of suing businesses for failure to secure information systems is within the realm of possibility.

1. Negligence

The common law provides for the tort of negligence. To establish liability for negligence, the following elements must be proven: (a) the existence of a duty of care, (b) the violation of that duty, and (c) proximate causation of a (d) harm.[151]

In the case of business D allowing its network to be used as a tool to threaten or commit a DDoS attack on business P, a court could conceivably find that (a) business D owed business P a duty of care to prevent its network from being vulnerable to hacking, that (b) business D's failure to meet certain security standards is a violation of that duty of care, and that (c) the violation of that duty of care is the proximate cause of (d) the harm caused by business P.

a. Existence and breach of a duty of care

In the context of a hypothetical lawsuit against a company for having inadequate information security, the plaintiff would argue that a defendant had a duty to secure its information system. The failure to secure an information system – not the hijacking or the DDoS attack – would be argued to constitute the breach of the duty of care. To evaluate the success of arguing these two elements, a review of what defines a duty of care is in order. The standard of care does not need to be perfection, but rather the amount of care that a reasonable person would

[148] Nike sued by Scottish-based ISP over web site attack, *available at* http://www.out-law.com/page-1325 (last visited January 2, 2007).

[149] Greg Lloyd Smith, Managing Director of FirstNET, indicated that his company planned to sue Nike in the U.S. for damages, based on the theory that Nike's unsecured website was an "attractive nuisance," explaining that:

> Much the same as a swimming pool in your back garden, such a potential danger must be protected at all costs in order to prevent damage or loss to others. The fact that Nike failed to ensure adequate security measures for their web address caused considerable damage to our company and denial of services to our on-line clients. Nike should be held responsible for all resulting losses. *Id.*

[150] http://web.archive.org/web/20011129000437/www.nikesucks.org/ (last visited January 2, 2007).

[151] 57A AM. JUR. 2D NEGLIGENCE § 6 (1989).

exercise.[152] In cases involving trained professionals, courts evaluate a defendant's conduct in light of the amount of care that a reasonable professional in that field would exercise.[153] In cases involving businesses, courts evaluate a defendant's conduct in light of industry standards.[154] Finally, legislation and regulations may be referred to in determining an appropriate standard of care.

Some have pointed out that federal statutes such as GLBA and HIPAA and the regulations that they authorized and the FTC consent agreements described above articulate standards of care that could be used in such a case.[155] Even if a court was convinced that it would not be appropriate to refer to those statutes or regulations as indications of an appropriate standard of care, expert witnesses in the field of information security or CIOs/CSOs could testify about accepted industry practices.

There is even precedent for a court to go beyond available evidence about standard industry practices and impose a higher, court-determined duty of care retroactively.[156] In such a case, a court may decide upon the reasonable standard of care by weighing the cost of a preventative, precautionary step against the likelihood and cost of foreseeable harms that were not protected against.[157]

Therefore, the criticism that a court could never determine an acceptable standard that defines a business' or an executive's appropriate duty of care is not a well-founded objection. It is a basic virtue of the Anglo-American tradition of the common law that judges have always applied established doctrines and principles to new-yet-analogous fact patterns.

However, as a practical matter, for the present time, practitioners doubt that a plaintiff could actually win at trial in a negligence suit against a company for failing to maintain adequate cyber-security standards such that its information systems become hijacked and used to commit

---

[152] 57A AM. JUR. 2D NEGLIGENCE § 135 (2005).
[153] 65 C.J.S. NEGLIGENCE § 164 (2005).
[154] 57A AM. JUR. 2D NEGLIGENCE § 164 (2005).
[155] It is worth clarifying that GLBA and HIPAA data security regulations, while useful in helping a court decide upon a reasonable duty of care, were not drafted with the specific intent to protect against DDoS attacks, and therefore their standards do not rise to the level of defining negligence *per se*. Henderson & Yarbrough, *supra* note 61, at 20-21. Violating a statutorily-specified standard of care, such as a building code requirement, constitutes negligence *per se*; in such a context, just the proof of the violation of specified standard is enough to establish liability for negligence.
[156] *The T.J. Hooper* , 60 F.2d 737, 740 (2d Cir. 1932). In his famous opinion finding tugboat owners negligent for not having weather radios aboard, even though that was not yet industry practice, Judge Learned Hand wrote that "there are precautions so imperative that even their universal disregard will not excuse their omission." Id. at 740.
[157] *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947). *See* Henderson & Yarbrough, *supra* note 61, at 20-21. This logic was also discussed in CSTB & NAE*, supra* note 34, at 49.

harm.[158] According to Dr. Christopher Pierson, attorney with Lewis and Roca LLP and President of the Phoenix Infragard Chapter, there are two reasons for this belief. First, many of these cases will settle before trial.[159] Second, at trial, a defendant's lawyer would have the advantage of being able to show that security practices still vary extremely widely in the business world.[160] However, according to Dr. Pierson, as security practices become more harmonized and routinized over time, the likelihood of a plaintiff winning a negligence lawsuit in the context of downstream liability will improve.[161]

Recent prosecutions initiated by the FTC are not dispositive, but their resolutions also suggest that there is a minimum reasonable standard of care with regard to cyber-security that is gradually evolving. As discussed above in Part III.A.6., settled lawsuits against several companies alleged that, for example, failure to encrypt data or properly control access to information systems were unfair trade practices. Since such allegations served as the basis for viable lawsuits, one of which resulted in a $15 million settlement, this suggests that in the near future, similar allegations could serve as grounds for arguing that a reasonable standard of care existed and was violated in a tort suit.

Given the facts and the trends above, it is reasonable to conclude that, in the near future, a court may conclude that there is a duty to secure information systems and that failure to secure an information system is a breach of that legally cognizable duty.

b. Causation

In addition to proving the existence of a duty of care and a violation of a duty, causation must be demonstrated. Beyond proving that the carelessness of the defendant caused the harm, it

[158] Correspondence with Dr. Christopher T. Pierson, March 20, 2006.
[159] *Id.*
[160] *Id.* Two cases serve to illustrate why practitioners are skeptical that a court would find that minimum standard of care for information security exists. In *Stollenwerk v. Tri-West Healthcare* (2005 WL 2465906, D. Arizona), there was no negligence found in a case where thieves twice broke into a facility, and on their second time, stole computers with personal data. One would imagine that the failure to heighten security after the first break-in would serve as the violation of a reasonable duty of care, but it did not. In *Guin v. Brazos* (2006 WL 288483, D. Minn.), allowing an employee to keep unencrypted data on a laptop computer which was taken home and stolen from the employee's residence was not held to constitute a violation of a duty of reasonable care. In both of these cases, however, the plaintiffs alleged that the harm was a higher risk of identity theft rather than actual harm – conceivably, the courts may have ruled otherwise, had there been actual identity theft committed as a consequence of the defendants' failure to take more aggressive steps to protect data security.
[161] Correspondence with Dr. Christopher T. Pierson, March 20, 2006.

is necessary that the harm be reasonably foreseeable.[162] Available survey data indicates that a growing majority of managers responsible for IT are aware of the risks of online crime and the risks of having inadequate information system security. As executives become familiar with phenomena such as DDoS attacks, it will be increasingly difficult to pretend to be ignorant that their unsecured networks pose a serious risk to others.[163]

c. Harm

The last possible objection to the argument that business executives may be found liable for negligence in allowing their networks to be hijacked and used to commit DDoS attacks is that non-monetary harm – in addition to purely economic harm – has traditionally been required for a court to find a defendant liable for negligence, but that requirement has been eroded.[164] Also, alternatively, some argue that the inability to serve customers and the possible loss of data qualify as physical damage.[165] Therefore, it is entirely reasonable to believe that a court may find a company liable for the economic losses to another company stemming from a DDoS attack.

d. Analogous Cases

The case of company D's inadequately secured network being hijacked to launch a DDoS attack on company P is very similar to other cases where courts have found liability for negligence. Practitioners and scholars have pointed out parallels that could be employed to convince a court that liability is appropriate.

---

[162] The causation element can be bifurcated into causation-in-fact and proximate causation. First-year tort classes in law school typically clarify the concept of proximate causation by meditating upon the case of *Palsgraf v. Long Island Railroad Co.* 248 N.Y. 339, 162 N.E. 99 (1928). The case involved employees of the Long Island Railroad sloppily assisting a passenger in his effort to board an already-moving train, during which a nondescript package fell onto the tracks. The package contained fireworks which ignited. The explosion dislodged distant scales on the station platform, which hit and injured Ms. Palsgraf. Ms. Palsgraf sued the Long Island Railroad Railway for negligence. The jury originally found the railroad company liable. On appeal, this decision was reversed. Writing for the majority, Judge Benjamin Cardozo opined that such cases must be evaluated not on the basis of a defendant's duty to the world-at-large, but on the basis of a duty to the plaintiff in the specific case. Therefore, while the sloppy efforts of Long Island Railroad's employees illustrated causation-in-fact (Ms. Palsgraf's injuries would not have occurred but-for the negligence of the railway employees), their conduct was not the proximate cause of her injuries. Another, simpler way of understanding proximate causation is to see it as a question of foreseeability. William L. Prosser, Handbook of the Law of Torts at 170-71 (4th Ed. West Pub. Co. 1971).

[163] Bourque & Bell, *supra* note 145, at 5.

[164] RESTATEMENT (THIRD) OF TORTS: *General Principles* § 3 (Discussion Draft 1999).

[165] Henderson & Yarbrough, *supra* note 61, at 11.

The most analogous case has been pointed out by Robert Bourque and Blake A. Bell[166] in consultation for this article, as well as Ronald Standler.[167] *AT&T v. Jiffy Lube International, Inc.*[168] is the latest in a sequence of cases finding that a telephone company client will be held liable for the cost of calls placed by unauthorized third parties.[169] This case is relevant to the paradigmatic DDoS attack inasmuch as the unauthorized third party hacked into Jiffy Lube's inadequately secured computerized exchange and used this as a conduit for the theft of over $55,000 worth of phone calls from AT&T.[170] In other words, this case demonstrates that negligently providing the means by which a third party can inflict harm can be the basis for liability.

In their 2000 article,[171] Bourque and Bell pointed to the case of *Computer Tool & Engineering, Inc. v. Northern States Power Co.*,[172] where a company sued both a local power and a local telephone company for negligence. Specifically, the telephone company, in laying cable, severed power lines, causing a power surge to damage a computer system owned by the plaintiff.[173] The lawsuit also attempted to recover damages from the power company on the theory that the power company could have protected the plaintiff company from the power surge.[174] In this case, the power company was shielded from liability only by virtue of being a public utility.[175] The remaining question of determining the relative fault of the plaintiff and the telephone company was properly deemed to be a question for the jury.[176] Once again, this case illustrates that, where a company, through its negligence, provides a conduit for another to inflict harm, there is viable basis for a negligence lawsuit.

Stephen Henderson and Matthew Yarbrough suggest that downstream liability in the context of a DDoS attack would be easier to establish than liability to handgun manufacturers or distributors because of the closer nexus between the defendant and plaintiff.[177] By implication, if

---

[166] Correspondence with Robert Bourque and Blake A. Bell, February 27, 2006.
[167] Standler, *supra* note 146, at 11.
[168] 141 P.U.R.4th 118, 813 F.Supp. 1164 (D.Md., 1993).
[169] *Id.* at 1167-69.
[170] *Id.* at 1165.
[171] Bourque and Bell, *supra* note 145, at 5.
[172] 453 N.W. 2d 569 (Minn. Ct. App. 1990).
[173] *Id.* at 571.
[174] *Id.* at 571.
[175] *Id.* at 573.
[176] *Id.* at 574.
[177] Henderson & Yarbrough, *supra* note 61, at 16-17.

suits against gun makers were viable, certainly a suit to establish downstream liability should be viable.[178]

Ronald Standler suggests that several further analogies may be used to convince a court that downstream liability should be found in a DDoS scenario.[179] Two in particular appear to be apt metaphors. First, Standler points out that, in some states, courts have found car owners liable when they leave the ignition keys in an unlocked and unattended car, and when those cars are subsequently stolen and used to cause harm.[180] Courts have found that such cases are examples of oversights that proximately caused harm to the plaintiffs because the intervening criminal act of the car theft was foreseeable.[181] The case of a car owner leaving their keys in an unlocked car is analogous to an executive or IT professional not taking reasonable steps to secure their network. In some states, this could be an analogy that might help to convince a court.[182]

Standler suggests that another analogous fact pattern is that of failing to secure domestic animals or agricultural livestock who subsequently cause harm to others.[183] In such cases, courts find animal owners to be strictly liable for the harm caused to other people by unsecured animals or livestock.[184] Any of these may prove to be useful metaphors in convincing a court that liability should arise for failing to take reasonable steps to secure something which may become a means of inflicting harm.

Based on the reasoning and examples presented in this Part, a court may conclude that a negligence suit is appropriate where a business failed to take reasonable steps – as defined by statutes, regulations, industry practices or even retroactively-applied standards determined by a judge – to secure its network, and where this failure allows for the hijacking and use of the network in a DDoS attack that results in harm to another company.

2. Vicarious liability – a prospect in the future?

---

[178] *Id.*
[179] Standler, *supra* note 146, at 4-6.
[180] *See, e.g. Abdallah v. Caribbean Sec. Agency*, 557 F.2d 61 (3d Cir. 1977); *Vining v. Avis Rent-A-Car Systems*, Inc., 354 So. 2d 54 (Fla. 1977).
[181] 57A AM. JUR. 2D *Negligence* § 638 (2005).
[182] However, Standler points out, in some states, the theft of the car is considered an intervening act, such that proximate causation does not exist between the car owner's negligence and the plaintiff's harm. Standler, *supra* note 146, at 6. *See, e.g. Poskus v. Lombardo's of Randolph, Inc.* 670 N.E.2d 383 (Mass. 1996).
[183] Standler, *supra* note 146, at 8.
[184] *See, e.g., Byram v. Main*, 523 A.2d 1387, 1389 (1987).

Agency law has been applied to software in the context of programs that automatically bid on – and commit to – transactions.[185] Automated interfaces that take sales orders are commonly referred to as e-agents. Per Section 15 of the Uniform Computer Transactions Act (UETA), drafted by the National Conference of Commissioners on Uniform State Laws in 1999, e-agents may enter into binding agreements on behalf of their principals. UETA has been adopted, with minor adjustments, by a majority of states. Section 107(d) of the Uniform Computer Information Transactions Act (UCITA) also states that a company or individual using an e-agent "is bound by the operations of the electronic agent, even if no individual was aware of or reviewed the agent's operations."

While it would represent a greater extension of existing legal principles than applying straightforward negligence theory, it is conceivable that a court would eventually accept the argument that a business' computers are agents in the context of tort liability as well. In such a scenario, the victim of a DDoS attack could argue that a zombie computer network is analogous to an employee. Under the common law tradition of agency relationships, an employer (one type of principal) is a responsible in many situations for the harms caused by an employee (one type of agent). While only one other author, Ronald Standler, has argued that vicarious liability could be applied to the context of a DDoS attack,[186] the possible application of agency law is worth considering.

Vicarious liability may be found in the context of employers failing to exercise reasonable care when hiring or retaining an employee.[187] To analogize to the context of a DDoS attack, one could argue that the defendant enterprise has failed to exercise reasonable care and has placed an agent – its information systems – in a position where it can cause harm to others. Vicarious liability may also be found for an agent's negligent acts so long as they are committed within the scope of the agent's work for the principal under the doctrine of *respondeat superior*.[188] Therefore, the employer will be found liable for an agent's negligent torts even

---

[185] Frank B. Cross and Roger LeRoy Miller, WEST'S LEGAL ENVIRONMENT OF BUSINESS, 462-63 (5th ed. 2004); *see* Todd V. Mackey, *Limiting Exposure for Internet Vendors: Separating the Wheat from the Chaff*, 21 J. MARSHALL J. COMPUTER & INFO. L. 207 (2003).

[186] Standler, *supra* note 146, at 10-11.

[187] Louis Buddy Yosha & Lance D. Cline, *Negligent Hiring and Retention of An Employee*, 29 AM. JUR. TRIALS 267 (database updated January 2006).

[188] The underlying theory of vicarious liability for harm caused by an agent is the doctrine of *respondeat superior* or "let the master respond." The logic of this doctrine is that the master ought to be accountable for the foreseeable risks created by requiring a servant to complete a given task and that the master is in a better position to compensate third parties for harms that may result. Similarly, it is foreseeable that a business' computers would be treated

while on a detour that is unbeknownst to the employer. To analogize to the context of a DDoS attack, one could argue that a hijacked computer system is like an employee on a detour – the computer system or the software is knowingly set loose in an environment where it may stray in the course of its employment, causing harm to others. In the case that came closest to considering the applicability of *respondeat superior* to this context, a company was held responsible for an online trespass by a computer program, albeit when the trespass was directed by one of the defendant company's employees.[189]

Admittedly, attempting to base a lawsuit solely on agency theory to recover damages from a company that has maintained inadequate security of its information systems would, for the moment, be an ill-advised strategy. By comparison, negligence theory appears more applicable. However, twenty years ago, it may have seemed equally far-fetched to argue that agency law would be applied to a computer program connected to a phone line, yet referring to software as an e-agent is now an uncontroversial matter of course. Therefore, agency law is a theoretical basis for finding liability for insecure information systems that should not be utterly dismissed. Over the coming decades, judges finding liability for unsecured information systems may well mention *respondeat superior* as part of the theoretical justification for their conclusions.

3. Trespass

This Part will describe why establishing downstream liability for failure to secure an information system would most likely fail under the current application of trespass theory to the online context. This Part will consider, however, how the application of trespass doctrines could foreseeably evolve such as to provide grounds for recovery.

As alluded to above, unsolicited electronic communications and violations of computer systems can constitute the intentional tort of trespass to private property, or chattels. Maintaining inadequate security, such that one's network to be hijacked and used to violate

---

analogously to agents, regardless of whether one prefers to think of a computer or information system as a servant or employee.

[189] *See Oyster Software, Inc. v. Forms Processing, Inc.*, WL 1736382 (N.D. Cal. 2001) (applying California law, the court ruled that even if the defendant company did not know about the initial act of sending a program to the plaintiff's website and copying its metatags, it could be liable for trespass to personal property if the plaintiff could prove that the defendant company was the employer of the individual who caused the harm).

another information system, is distinguishable because it is not an intentional act, but rather negligent conduct.

The level of the protection of ownership interests in real property is higher than the protection of ownership interests in personal property in that proving trespass onto land requires no proof of harm and inasmuch as, for example, an animal owner can be strictly liable for his animals trespassing onto another's land. Trespass to land may be found when minute particles or intangible electronic signals are sent over another's land.

Perhaps the most debated requirement in proving trespass to personal property in the online context is the element of proof of the deprivation or damage to the personal property. This requirement was recently reasserted by the California Supreme Court in the case of *Intel v. Hamidi*.[190] In this case, the California Supreme Court overturned the rulings of a trial court and appellate court that had found an ex-employee's repeated and unsolicited e-mails to current employees of Intel to constitute trespass to personal property.[191] The Court overruled the lower court decisions because of an insufficient showing of either injury to property or injury to the possessor's interest.[192] Practitioners across the country cite to *Hamidi* as having persuasive authority.[193] Arguably, when the California Supreme Court clarified the damage requirement in *Intel v. Hamidi*, the limitations of the trespass to chattels doctrine were highlighted; namely, that the doctrine is too rigid and fails to adequately balance rights.[194]

In contrast, state and federal courts in other jurisdictions have sometimes applied a looser standard when they decide cases involving a trespass to information systems. Other courts have accepted, for example, the loss of prospective business or a small decrease in processing speed or loss of server capacity as sufficient damage to personal property to support a finding of trespass

[190] 71 P.3d 296 (Cal. 2003). The Hamidi decision was foreshadowed by the decision in *Ticketmaster Corp. v. Tickets.Com, Inc.,* finding that some damage must be evidenced in a claim for trespass to personal property in the context of either (1) programs aggregating data from another website without authorization or (2) one website linking to another without authorization. WL 21406289 (C.D. Cal., 2003).
[191] *Hamidi*, 71 P.3d at 300-301.
[192] *Id.* at 303-311.
[193] Authors' correspondence with Dr. Christopher T. Pierson, April 3, 2006.
[194] *See* Steven Kam, *Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance,* 19 BERKELEY TECH. L.J. 427 (2004), Steven Kam proposes a theory of cyber-nuisance that would balance the relative utility of, for example, unsolicited e-mails, such that the harms caused by this conduct could be discouraged and redressed. *Id.* at 442-445.

to personal property. This trend was recently continued by an Illinois federal court in *Sotello v. Directrevenue.*[195]

Some scholars have pointed out that several court opinions have focused on whether the information system access was explicitly not allowed in justifying their finding of trespass and granting of injunctions. Patricia L. Bellia has pointed out that this was the case in *CompuServe Inc. v. Cyber Promotions, Inc.*,[196] *America Online, Inc. v. IMS*,[197] the lower courts in *Intel Corp. v. Hamidi*,[198] and *eBay, Inc. v. Bidder's Edge, Inc.*[199] – the harm in these cases was certainly not dispossession of property, and the economic harm that the courts perceived was more potential than actual in all of these cases.[200] This is perhaps best illustrated by the decision in *eBay*, where programs that scoured a website and collected publicly available information were violating the website's terms of use and were found to be interfering with property rights adequately to justify a court injunction on the grounds that such activity was a trespass to chattel.[201]

Several prominent scholars have lamented that courts have been sloppy in mixing metaphors and standards, arguing that it would be bad public policy for courts to drift toward treating electronic communications more like physical trespass to land.[202] The negative public policy impact of such a drift has been characterized as a tragedy of the anticommons, in that online commerce and freedom of expression depend on being able to access information on others' servers and that moving toward a *de facto* standard of trespass to real property would limit the potential of the Internet for business and expressive purposes.[203]

Although they represent a minority view, several other scholars have advocated that unauthorized computer network trespasses be explicitly treated the same as trespass to real

---

[195] 384 F. Supp.2d 1219 (N.D. Ill. 2005).
[196] 962 F. Supp. 2d 1015.
[197] 24 F. Supp. 2d 548 (E.D. Va., 1998).
[198] 71 P.3d 296.
[199] 100 F. Supp. 2d 1058.
[200] Patricia L. Bellia, Defending Cyberproperty, 79 N.Y.U. L. Rev. 2164, 2227 (2004).
[201] *eBay,* F.Supp.2d at 1069-1072.
[202] Hunter, *supra* note 47, at 439; Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561 (2001). Such a confusion on the part of courts is understandable, due to terminology such as "website," "logging onto," "hosting," or "visitors to a website," all of which imply physicality, even though, in the characterization of some authors, it is more accurate to say that a server transmits a website to a viewer. For an analysis of whether metaphors to the physical world have truly been a contributing factor to judges articulating standards more reflective of the physical world, *see* David McGowan, *The Trespass Trouble and the Metaphor Muddle,* 1 J.L. ECON. & POL'Y 109 (2005).
[203] *See, e.g.,* Hunter, *supra* note 47, at 443-444.

property.[204] The public policy in favor of such an explicit standard is compelling, in that it would discourage only access to information systems that is explicitly unauthorized. Much as the elevation of an exclusive right to real property was considered an essential step in furthering economic development and avoiding problems such as the tragedy of the commons in medieval England, one could argue that a "zero tolerance" approach to explicitly unwelcomed trespassing onto each other's servers is essential to the smooth conduct of commerce in the present era. Further, it can be argued that unauthorized access into an information system does bear adequate similarity to trespassing onto land so as to justify applying a standard similar to that of trespass to real property. A visit to a website is actually like stopping by someone's office and gesturing toward and requesting to borrow a book. In other words, even a permissible website visit does necessarily involve electronic signals entering the physical server associated with a "visited" site. Thus, metaphors comparing cyberspace to real space are not entirely unfounded.

A move toward the explicit adoption of the standards of trespass to real property would raise the prospect that one could be liable for damages caused by failure to secure one's network under a theory of strict liability.[205] The likelihood of winning a downstream liability suit would increase, inasmuch as additional or clearer analogies could be drawn between existing caselaw and the context of a cyber-trespass. Specifically, it would be possible to argue that failing to secure one's network resulting in its hijacking and use in a DDoS attack is analogous to failing to secure one's cattle, resulting in their stampede onto another's land. The enterprise that failed to secure its chattel, resulting in a trespass, could be found strictly liable for damages that resulted. While it currently may seem fanciful to argue that a hijacked information system sending slews of e-mails is analogous to stampeding cattle, this analogy would be irresistible in a jurisdiction that explicitly accepted that unwelcomed violations of one's server are equivalent to violating one's real property.

Much like applying agency law to online tort scenarios, this theoretical approach is not likely to succeed or even to be attempted in the immediate future. However, given that courts in

---

[204] Susan M. Ballantine, *Computer Network Trespasses: Solving New Problems with Old Solutions*, 57 WASH. & LEE L. REV. 209, 255 (2000). For a discussion of how analogizing to physical space could yield to a new, Internet-specific standard for online conduct, *see* Ronnie Cohen and Janine S. Hiller, *Towards a Theory of Cyberplace: A Proposal for a New Legal Framework*, 10 RICH. J.L. & TECH. 2 (2003). For a discussion of the range of possible alternative standards for governing online trespass, *see* Bellia, *supra* note 200, at 2164. Finally, as already mentioned, Steven Kam suggests that adopting nuisance standards from the context of real property would allow for the better balancing of rights and interests in the online context. *See* Kam, *supra* note 194, at 442-445.

[205] Standler, *supra* note 146, at 8.

some jurisdictions have already loosened the requirement of proof of damages in trespass to personal property cases in the online context, it is not impossible to imagine that some courts will eventually – either explicitly or in practice – apply a standard of trespass to information systems that resembles the standard of trespass to real property. This development could then serve as a basis for recovering damages against another enterprise that failed to secure its information system, resulting in a DDoS attack.

4. Statutory Civil Suit Provisions

It may be tempting to consider using CFAA in the context of downstream liability. However, it is inapplicable, because the unauthorized access must be intentional, even if no harm was intended. In the context of a downstream liability case, the defendant does not intend their information system to trespass or cause harm, but instead is responsible for the lack of security that results in a harm unintended by the defendant. Given this scenario, the civil suit provisions of the CFAA do not provide a means of recovering damages from an entity that fails to secure its information system.

As mentioned above in Part III.A.2., Section 404 of SOX requires that internal controls on information systems be in place, documented and tested at least once a year, Section 302 requires that executives certify reports and Section 409 requires that material financial changes be communicated with supporting data quickly to the public. These provisions have been interpreted by the IT community to necessitate enhanced access controls, encrypting data and protection against DDoS attacks, among other security measures.[206] Available data indicates that managers perceive that SOX's penalties and requirements have had a significant impact on information systems security.[207] While the civil suit provisions in SOX were not intended to create downstream liabilities, the text of SOX does not eliminate the possibility of companies using SOX provisions to sue executives, just like defrauded customers, for executives' failure to maintain adequate internal controls that resulted in harm.[208] Therefore, it is foreseeable that a

[206] Keith Pasley, *Sarbanes-Oxley (SOX) – Impact on Security In Software*, developer.com, *available at* http://www.developer.com/security/article.php/3320861 (last visited January 2, 2006).
[207] Gordon et al., *supra* note 3 at p. 21-22.
[208] For a brief summary of the legislative history of SOX § 404 and the high costs associated with complying with that section, *see* Joseph A. Castelluccio III, *Sarbanes-Oxley and Small Business: Section 404 and the Case for a Small Business Exemption,* 71 BROOK. L. REV. 429 (Fall, 2005).

DDoS victim may eventually attempt to sue a company pursuant to SOX, in addition to suing on other grounds, for failing to maintain the security of its information systems.

5. Product Liability Unavailable

Relatively unpublicized provisions of the USA PATRIOT Act amended the CFAA so that no civil actions may be brought against producers for "the negligent design or manufacture of computer hardware, software or firmware."[209] Further, Section 230 of the Communications Decency Act of 1996 (CDA) has been used to shield Internet Service Providers (ISPs) from liability.[210] The section reads: "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."[211] This language has been interpreted broadly to protect ISPs when their service is the mechanism for delivery of damaging computer programs.[212]

Therefore, despite the apparent analogy that hardware and software companies and ISPs may be providing the equivalent of negligently designed bridges and Ford Pintos for the information superhighway, and may therefore be vulnerable to product liability lawsuits, federal statutes afford these companies and their executives an unusual degree of protection. However, executives in other industries should not rely upon a hope that CDA will be extended further to shield all businesses from immunity when their unsecured computers become zombie attackers.[213]

6. Damages and defenses

As mentioned above, a key advantage of pursuing a tort claim in addition to or instead of pressing criminal charges is the recovery of damages. Assuming that a defendant's conduct is

---

[209] USA PATRIOT Act, § 814(d) (amending 18 U.S.C. § 1030(g) (2006)). *See* Beryl A. Howell, *Cybersecurity Liability: Is it Time to Get Off the Soapbox?*, 22 COMPUTER & INTERNET LAW., 5 (May 2005) at 3.
[210] *See, e.g., Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).
[211] 47 U.S.C. § 230(c) (1996).
[212] *Green v. America Online, Inc.* 318 F.3d 465 (3d Cir. 2003), *see* Laurin H. Mills, *ISP Immunity Provision Is Broadly Interpreted*, NAT'L L.J., April 13, 2002 at C19. It has been argued that U.S. statutory provisions should be harmonized with European standards, such that ISPs would be responsible for harmful activities that they knew about but chose not to remedy. *See* Michael L. Rustad, Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335 (2005).
[213] While CDA has even been used to protect eBay from liability when its forum was used to sell pirated sound recordings in *Stoner v. eBay, Inc.,* 2000 WL 1705637, 56 U.S.P.Q.2d 1852 (Cal. Superior, 2000) the CDA did not shield an ISP for knowingly allowing a hosted website to violate a trademark. *Gucci America, Inc. v. Hall & Associates*, 135 F.Supp.2d 409, 60 U.S.P.Q.2d 1714 (S.D. N.Y. Mar 14, 2001).

proven to be the exclusive cause of the damages, then the measurable harm caused by the conduct may be awarded. In egregious cases, a court may be convinced that future instances of such conduct ought to be deterred, and punitive damages may be awarded, further boosting one's economic incentive for pursuing such a lawsuit.

It is important to highlight, however, that there is the possible defense of comparative negligence that could be presented in a typical DDoS scenario. This defense could either reduce or entirely eliminate the award of damages, even if liability for negligence or vicarious liability or trespass to personal property can be readily established. To review: in our hypothetical scenario where company D was negligent and its network was compromised and used to launch a DDoS attack on company P resulting in harm, company P would be the plaintiff suing defendant company D to recover for damages. So far, so good. Defendant company D, however, could argue that company P bears part of the responsibility for its own losses because company P was itself negligent. In the vast majority of states, this is referred to as comparative negligence. In situations where the court decides that company P's own negligence is 0-50% responsible for its own harms, the final award is reduced by the appropriate percentage. In comparative negligence states, once a court finds that company P is more than 50% at fault for its own damages, company P will recover nothing. A minority of states allows for pure comparative negligence, which would allow for proportionate recovery even if plaintiff company P's own negligence is judged to be more than 50% of the reason for its damages.[214] There has been at least one instance where, once a hacking was discovered, the failure to mitigate damages was the basis for a court declining to award damages.[215]

The other possible defense would be to argue that an intervening criminal act is the true cause of the damages. This is not an unprecedented defense in tort cases. However, as mentioned above, a DDoS attack utilizing an unsecured network is most analogous to leaving the ignition keys in an unlocked and unattended car. In these cases, liability has been attached to the

[214] Prior to comparative negligence being adopted by the vast majority of states, any finding of a plaintiff being responsible for his or her own damages would serve as an absolute bar to recovery. Christopher J. Robinette and Paul G. Sherland, *Contributory or Comparative: Which Is the Optimal Negligence Rule?* 24 N. Ill. U. L. Rev. 41 (Fall 2003). This doctrine, known as contributory negligence, survives in a small minority of states. Jennifer J. Karangelen, *The Road to Judicial Abolishment of Contributory Negligence Has Been Paved by Bozman v. Bozman*, 34 U. BALT. L. REV. 265 (Winter 2004). Ultimately, the chances of the success of mounting a defense that involves proving the plaintiff's own negligence will be determined by the specific facts of a case.

[215] NTS AM. JUR. 2D *Computers and the Internet* § 73 (2005).

negligent conduct of the car owner.[216] The defense of an intervening act being the true cause of the plaintiff's harm fails because the intervening act is entirely foreseeable, and reasonable steps could have been taken to ensure that one's property does not become a tool for inflicting harm.

7. Why the dearth of tort claims?

Given the high profile of a few cyber-extortion attempts and, more broadly, the tens of thousands of complaints to the FTC about various other online misdeeds, the relative dearth of resulting tort claims is puzzling. Michael L. Rustad and Thomas H. Koenig provide some theories as to why there is a lack of case law applying tort liability to online contexts.[217] First, they point out that a lag time is typical whenever a new technology emerges. For example, applying "horse and buggy" legal principles to the automotive age took decades, and – of particular significance to the analysis in this article – eventually resulted in some creative stretching of old doctrines to fit the new paradigm.[218] Second, Rustad and Koenig point to the fact that tort law has been significantly retrenched in the majority of states through state statutes limiting damages and liability; they suggest that this hostile environment to tort suits may have contributed to the dearth of case law.[219] When asked by the author for his opinion, Blake A. Bell suggested that perhaps there are not more cases because larger companies – the most lucrative targets for a tort lawsuit – have taken the best security precautions.[220]

## V. Conclusions

Cyber-extortion is a large problem that has received inadequate coverage and attention. In instances where one can establish the identity of the extortionist, there are tools for prosecuting and recovering damages from the extortionist. However, one is typically unlikely to ascertain the identity or location of a cyber-extortionist and the cyber-extortionist is very

---

[216] See *Abdallah*, 557 F.2d at 61; *Vining,* 354 So. 2d at 54.
[217] Michael L. Rustad, Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77 (2003).
[218] *Id.* at 77-79. The authors borrow the words of former President Richard Nixon to illustrate the concept of legal lag. *Id.* at 77, As a law student at Duke University, Nixon observed that "in 1905 all of American automobile case law could be contained within a four-page law review article, but three decades later, a 'comprehensive, detailed treatment [of automobile law] would call for an encyclopedia.'" *Id. citing to* Richard M. Nixon, *Changing Rules of Liability in Automobile Accident Litigation,* 3 LAW & CONTEMP. PROBS. 476 (1936).
[219] Rustad & Koenig, *supra* note 217, at 139-140.
[220] Correspondence with Blake A. Bell, February 27, 2006.

possibly beyond U.S. borders. Because extortionists typically lack extensive financial resources, one is also unlikely to recover the full amount of desired damages. Therefore, government prosecution of cyber-extortionists may be a more appropriate means of deterrence and punishment of extortionists when they can be located.

Given the comparative ease of learning which businesses' information systems were hijacked to commit a cyber-extortion, and those companies' relatively deeper pockets, businesses with compromised information systems will soon be targets for civil lawsuits. This will obviously be a desirable development from the perspective of victimized businesses seeking the recovery of damages. Negligence is clearly the most applicable potential framework in seeking redress from a business that fails to take reasonable steps in protecting its information system, such as to allow it to become an attack zombie.

Some will lament that finding tort liability in such contexts will be a windfall to trial attorneys and will make businesses operating in the U.S. less competitive. Some may visualize a nightmare scenario of thousands of negligence lawsuits that could incapacitate businesses to an unreasonable degree. The alternative solution would be to propose a statutory or regulatory scheme as the appropriate approach to combat inadequate information system security. Further, some may argue that immunity from, or limitations to, tort liability should be created by statute.

The author suggests that allowing tort liability to serve as a means of deterrence and redress of harms is the more desirable option for businesses and society. Most importantly, tort law allows for the most flexible and adaptable standard to be applied to a rapidly changing technological environment. It bears pointing out that, far from requiring a standard of perfection, an action based on negligence theory will, practically by definition, seek out and enforce a reasonable standard. It will also reduce or prohibit damages to reflect the comparative negligence of plaintiffs who failed in their own responsibilities to meet a reasonable security standard. As this article has reviewed, the reasonable standard of care may be determined by reference to existing statutory and regulatory schemes that articulate minimum data security requirements. Second, in industries where statutory and regulatory minimum standards do not exist, the standard of care will be defined in reference to reasonable industry practices, to which expert witnesses can testify. These security experts presumably should have been consulted in the first place by reasonable executives. Finally, as we have seen, if a new paradigm suddenly evolves such that a court cannot defer to any other approach, a calculation may be used whereby

a court would consider the cost of prevention compared to the likelihood and cost of an undesirable outcome to determine what the reasonable applicable standard of care ought to be.

Contrast these bases for deciding upon a standard of care with the consequences of attempting to impose statutory or regulatory standards. Statutory and regulatory standards for information systems security would be plagued by the inherent difficulty of responding to the exigencies of the fast-evolving realities of technology and information security. Almost inherently, statutes and promulgated regulations would always be at least slightly out-of-date. Second, a higher and more costly standard may be imposed by statutes or regulations than is either desirable or would have been deemed necessary retrospectively in a negligence analysis. It bears repeating that IT spending in 2006 rose over 10% as a result of businesses purchasing data systems to satisfy the perceived requirements of SOX – a statute that did not even seek to regulate data systems security *per se*. Third, statutes and regulations may impose a perversely inappropriate standard by mistake. The CAN-SPAM Act[221] is a perfect example of a statute that imposed a counterproductive remedy. The statute mandated the inclusion of e-mail addresses in unsolicited messages to which a recipient could reply in order to "opt-out" of receiving further messages. This appeared to be a reasonable way to curb the perceived problem. However, it encouraged precisely what "phishers" (people who phish – that is, people who acquire and trade in personal information nefariously acquired online) desire: namely, verification that an e-mail account is active.[222] Fourth, to regulate and then adequately monitor, investigate and enforce IT security issues, a massive, expensive and unwieldy new government body would be necessary. Finally, the compounding of out-of-date standards over time can – and historically has – accumulated and spiraled into an unmanageable tangle. In the 1980s, it was realized that the penalties of federal criminal laws numbered in the thousands, were at times inconsistent, and were often generated by spasmodic responses to the crises of a particular moment. SOX is but the latest example of this phenomenon in U.S. legislation. The ability to prosecute for multiple counts of the same criminal charges means that the mandatory statutory minimum or maximum penalties are of exaggerated and mostly symbolic importance. Indeed, the purpose of the Federal Minimum Sentencing Commission was to efficiently bring consistency and predictability to criminal sentencing. Unfortunately, the Sentencing Commission is a small group of appointees

[221] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 18 U.S.C. §1037 (2006).
[222] Ravi Puri, *Gone Fishing*, 65 OR. ST. B. BULL. 37 (October, 2004).

who are unaccountable to an electorate during their term, yet they are allowed to make binding decisions in secret. This provides an object lesson for those who see tort liability as the enemy and statutory or regulatory standards as the obvious best choice: namely, the sediments of statutory and regulatory requirements may over time create a confusing mess of inconsistencies that may eventually get sorted out in a process that is less open and accountable than some may imagine.

Also, to address another important policy perspective: allowing tort liability to operate results is an incentivization of common-sense responsibility, or, in other words, a standard that both can be lived with and which one would want everyone else to live by. Responsible executives should – and should want to encourage others to – consult experts on cyber-security. Incentivizing a secure information infrastructure, especially in the early 21st century, serves the interests of everyone. Further, statutory and regulatory solutions are limited in their geographic scope. Given the size of the cyber-extortion problem, the geographic dispersion of the world's IT industry to countries such as India and the fact that an information system is only as strong as its weakest link, pursuing a comprehensive solution through the national legislatures of the world and treaty commitments between governments hardly appears practical. If tort liability was statutorily limited in the U.S. in the context of downstream liability, U.S. enterprises with weak links anywhere in the world may tolerate weaknesses that no reasonable person would wish to have allowed.

Thus, not only will downstream liability based on negligence become a reality in the absence of statutes that declare otherwise, but the business community should embrace tort liability in this context. Of course, large businesses could lobby and likely secure immunity from lawsuits, much as the USA PATRIOT Act immunized hardware and software manufacturers[223] and the Communications Decency Act immunized Internet Service Providers from tort liabilities.[224] This is actually undesirable, inasmuch as businesses would not only immunize themselves, but also everyone else, including negligent actors that one may later want to hold accountable for their unsecured networks. Embracing tort liability should also be seen as consistent with best practice-sharing and prevention efforts that have been voluntarily undertaken by industry – one should want to retain the ability to punish those who betray

[223] *See infra*, Part III.B.5.
[224] *Id.*

agreements to share best practices and who violate community standards. Ultimately, the policy debate framed in this conclusion will not be fruitful so long as cyber-extortion remains the elephant in the server room. An open dialogue – specifically about the duties and liabilities of businesses who become cyber-crime victims or who unwittingly provide the tools to perpetrate a cyber-crime – is overdue and should ideally involve scholars, practicing attorneys, business leaders, public interest group representatives and IT professionals.