

COMPUTER HACKING AND LIABILITY ISSUES:

WHEN DOES LIABILITY ATTACH?

W. Reid Wittliff
GRAVES, DOUGHERTY, HEARON & MOODY
A Professional Corporation
515 Congress Avenue, Suite 2300
P. O. Box 98
Austin, TX 78767-0098
www.gdhm.com
rwittliff@gdhm.com
(512) 480-5656 Telephone
(512) 480-5856 Telecopier

TABLE OF CONTENTS

	<u>Page(s)</u>
I. INTRODUCTION	1
II. STATUTORY LIABILITY	1
1. The Computer Fraud and Abuse Act - 18 U.S.C. § 1030(g)	1
a. 18 U.S.C. § 1030 (a)(2) - Unlawful Access to Obtain Information	2
b. 18 U.S. C. § 1030(a)(4) - Unlawful Access to Obtain Something of Value	3
c. 18 U.S.C. § 1030(a)(5)(A) - Unlawful Access Causing Damage	3
d. Civil Litigation Under the CFAA	3
2. The Texas Breach of Computer Security Statute	5
3. Claims Under the Federal Wiretap and Stored Communications Acts	7
III. TORT LIABILITY	11
1. Negligence	11
2. Negligent Hiring/Supervision	13
3. Trespass to Chattels	13
IV. OTHER AVENUES OF RECOVERY FOR COMPUTER HACKING	15
1. Contractual Liability	15
2. Theft of Trade Secrets	15
3. Copyright Claims	17
V. CONCLUSION	18

“To err is human, to really foul things up requires a computer.”
– Farmer’s Almanac, 1978

I. Introduction

Both federal and state statutes impose criminal liability on hackers for computer crimes, as well as provide civil liability for violations of the statute. But often hackers are difficult to find, are judgment-proof, or both. As victims of hackers look for deep pockets from which to recover damages, they will increasingly turn to the companies that operate on-line businesses and computer networks. This article reviews the legal theories under which a computer hacker could be found liable, and discusses theories by which a company which was the victim of a hacker could be subject to liability to other parties for a hacking incident.¹

II. Statutory Liability

1. The Computer Fraud and Abuse Act – 18 U.S.C. § 1030(g)

The Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, criminalizes a wide range of conduct that undermines the confidentiality, integrity, and availability of data, and is the primary statutory tool used by federal law enforcement to prosecute computer hackers.² The CFAA also provides many of these same tools to civil practitioners seeking to collect damages on behalf of clients victimized by computer hackers. Section 1030(g) of the statute provides:

Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B).³ Damages for a violation involving only conduct

¹ There is a growing body of scholarly work discussing this and related topics. *See e.g.*, Kevin R. Pinkney, Putting Blame Where Blame is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure, 13 Alb. L.J. Sci. & Tech. 43 (2002); Stephen E. Henderson & Matthew E. Yarbrough, Suing the Insecure?: A Duty of Care in Cyberspace, 32 N.M. L. Rev. 11 (2002); Sarah Faulkner, Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks, 18 J. Marshall J. Computer & Infor. L. 1019 (2000).

² A list of over 50 computer hacking prosecutions brought pursuant to the CFAA can be found on the Computer Crime and Intellectual Property Section of the Department of Justice’s website at <<http://www.cybercrime.gov/cccases.html>>.

³ 18 U.S.C. § 1030(a)(5)(B)(i)-(v) provides:

- (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;
- (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
- (iii) physical injury to any person;
- (iv) a threat to public health or safety; or
- (v) damage affecting a computer system used by or for a government entity in furtherance of the

(continued...)

described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 1030(g). “Damage” is defined in the statute to include “any impairment to the integrity or availability of data, a program, a system or information.” 18 U.S.C. § 1030(e)(8). “Loss” is broadly defined to include “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to condition prior to the offense, and any revenue lost, cost incurred or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11).

Accordingly, a victim of a computer hacker may sue the hacker for damages under federal law if the hacker violated one of the provisions of § 1030 and one of the factors set forth in § 1030(a)(5)(B)(i)-(v) is met. Section 1030 is quite broad and contains several subsections, each of which constitutes a separate violation under the statute:

a. 18 U.S.C. § 1030 (a)(2) - Unlawful Access to Obtain Information

Section 1030(a)(2) proscribes conduct most people think of as hacking – the unauthorized (or in excess of authorization) access to a computer to obtain information. Under § 1030(a)(2), it is unlawful to intentionally access a protected computer⁴ without authorization or exceed authorized access and thereby obtain:

(A) information in a financial record of a financial institution, or of a card issuer as defined in Section 1602(n) of Title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication.

³(...continued)

administration of justice, national defense, or national security.

18 U.S.C. § 1030(a)(5)(B).

⁴ The phrase “protected computer” is defined in the statute to include any computer which is “used in interstate or foreign commerce or communication,” and thus includes any computer connected to the Internet. 18 U.S.C. § 1030(e)(2)(B). *See also Shurgard Storage Centers, Inc. v Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (refusing to limit the definition of “protected computers” to computers storing information which could harm the public if released)

b. 18 U.S.C. § 1030(a)(4) - Unlawful Access to Obtain Something of Value

Section 1030(a)(4) prohibits knowingly accessing without authorization or in excess of authorization a computer used in interstate commerce (including any federal agency computer) and obtaining anything of value when such action was done with the intent to defraud. There is an exception if the “thing obtained” is only the use of a computer and the value of that use is not more than \$5,000 in any one-year period.

At least one court has addressed this section. In *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), the First Circuit reversed the § 1030(a)(4) conviction of an IRS employee who surfed IRS databases to which he did not have job-related access, because the government failed to prove that the information the defendant obtained (taxpayer return information) constituted anything of value as there was no evidence that the defendant intended to do anything “but satisfy idle curiosity” when he obtained the information. *Id.* at 1078.

c. 18 U.S.C. § 1030(a)(5)(A) - Unlawful Access Causing Damage

Section 1030(a)(5)(A) is probably the most commonly prosecuted subsection of the CFAA. It was used to prosecute computer hackers such as Kevin Mitnick (who gained an online cult following calling for his release), David Smith (the hacker behind the Melissa virus), and Patrick Gregory (one of the co-founders of globalHell, the hackers who hacked the White House web page).

Section 1030(a)(5)(A) describes three violations which are differentiated by the *mens rea* required for the violation. Under § 1030(a)(5)(A)(ii), an offense is committed if a person knowingly causes the transmission of a program, code, information, or command to a protected computer and *intentionally* causes damage. Section 1030(a)(5)(A)(ii) criminalizes accessing without authorization a protected computer and *recklessly* causing damage, and § 1030(a)(5)(A)(iii) criminalizes intentionally accessing a protected computer without authorization and *causing* damage.

d. Civil Litigation Under the CFAA

Most of the disputes litigated under the CFAA thus far involve allegations of unlawful “data mining” where one party complains that another has exceeded authorized access to computerized databases to obtain information that can be used for commercial purposes. For instance, in *Register.com v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D. N.Y. 2000), Verio, an Internet Service Provider (“ISP”), was using automated software to search Register.com’s publicly available “WHOIS” database in order to obtain a list of individuals and entities who had recently registered a domain name. Verio used the information to market its web site hosting services to the newly-registered domain name holders. *Id.* at 243-44. Register.com complained that this amounted to an unauthorized access to its “WHOIS” database because, the “WHOIS” database’s terms of use precluded the use of automated search programs and because Register.com specifically told Verio that it did not consent to the use of the automated tools. *Id.* at 249. The Court rejected Register.com’s assertion that the terms of use prevented the use of automated software tools, but found that Register.com’s notice to Verio that it did not consent to the use of the automated tools was sufficient to make Verio’s continued use of the tools unauthorized. *Id.* at 249, 251. The Court also held that Verio’s use of the automated tools caused or could cause Register.com diminished

server capacity and a possibility of a crash causing damages of \$5,000 or more, and thus the Court enjoined Verio's use of the automated software tools under the CFAA. *Id.* at 253.

In *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998), America Online sued a spammer for using automatic software tools to scour various America Online services for email addresses. The Court held that LCGM, Inc.'s use of the America Online service was unauthorized because AOL's terms of service prevented users from deploying automated tools to gather email addresses in order to spam them, and thus the Court granted summary judgment in favor of AOL on the § 1030(g) claims. *Id.* at 450.

Other litigants have used the CFAA as a compliment to theft of trade secret claims. In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the First Circuit affirmed an injunction entered pursuant to § 1030(g) in favor of a travel provider against several of its former employees who had formed a competing travel company and developed a "scraper" program to obtain pricing information from the travel provider's website. The Court held that use of the "scraper" program on the website constituted an unauthorized computer access because the ex-employees breached their confidentiality agreements with their former employer when they developed the program. *Id.* at 582-83.

Similarly, in *Shurgard Storage Centers v. Safeguard Self Storage*, 119 F. Supp 2d 1121 (W.D. Wash. 2000), the plaintiff combined CFAA claims with theft of trade secret claims to recover damages caused by an employee who used his computer access to gain confidential trade information for the purpose of passing that information to a new employer and competitor. Shurgard and Safeguard were business competitors in the storage industry. Safeguard offered one of Shurgard's managers a job. Instead of leaving Shurgard immediately, however, the manager began sending e-mails to Safeguard containing trade secrets and other proprietary information. Shurgard sued Safeguard under § 1030(a)(2)(C) contending that the manager's access to Shurgard's computer system was unauthorized because the manager did not have authority to gather trade secrets from the network to send to Shurgard's competitor. Safeguard, on the other hand, argued that access was authorized since the manager ordinarily had full access to this confidential information. Relying on the Restatement (Second) of Agency, the *Shurgard* Court ruled that the employee's authorization ended when he became an agent for Safeguard, and that the manager's access to Shurgard's computer system was not authorized under § 1030(g).

Safeguard also argued that Shurgard failed to prove it had suffered the requisite \$5,000 in damages required by § 1030(a)(5)(C)⁵, because the data that had been leaked to Shurgard's competitor was intact on Shurgard's computer. *Id.* at 1126-27. The Court rejected this argument noting that "damage" under the CFAA means "any impairment to the integrity" of data and that the manager's infiltration of Shurgard's computer and subsequent dissemination of confidential information sufficiently impacted the integrity of this data to meet the damage requirement under the statute. *Id.*

⁵ The provisions of 18 U.S.C. § 1030(a)(5)(C) in effect when *Shurgard* was decided are now codified at 18 U.S.C. § 1030(a)(5)(A)(iii).

The pre-Patriot Act version of the CFAA⁶ has also been used in novel ways to startling effect. For instance, in *Shaw v. Toshiba America Information Systems, Inc.*, 91 F. Supp. 2d 926 (E.D. Tex. 1999), a class of plaintiffs sued computer manufacturers when the manufacturers distributed computers with a faulty floppy disk controller. The plaintiffs contended that distributing computers with this bit of faulty code amounted to the transmission of code with the intent to cause damage in violation of § 1030(a)(5)(A), because the faulty code caused a loss of data when the floppy disk drivers were used. The computer manufacturers moved for summary judgment arguing that selling computers containing code did not fall within the ambit of § 1030. The District Court disagreed and denied the motion for summary judgment. *Id.* at 933-936. Subsequently, the parties settled for \$2.1 billion and the settlement was approved by the court. When the Patriot Act was passed in late 2001, Congress modified § 1030(g) to specifically exclude actions based on negligent design or manufacture of computer hardware, software or firmware – no doubt in response to the *Shaw* case.⁷

2. The Texas Breach of Computer Security Statute

Like federal law, Texas law contains a civil provision which creates a cause of action based on the criminal computer hacking statute. TEX. CIV. PRAC. & REM. CODE § 143.001 provides:

(a) A person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code, has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally.

(b) A person must bring suit for damages under this section before the earlier of the fifth anniversary of the date of the last act in the course of the conduct constituting a violation under Chapter 33, Penal Code, or the second anniversary of the date the claimant first discovered or had reasonable opportunity to discover the violation.

Hence, a violation of TEX. PENAL CODE § 33.02, entitled “Breach of Computer Security,” can give rise to a civil suit under § 143.001 of the TEX. CIV. PRAC. & REM. CODE. Section 33.02, in turn, makes it unlawful “to knowingly access a computer, computer network, or computer system without the effective consent of the owner.” Importantly, § 33.02 does not contain a damage threshold like the CFAA, and thus this defense is not available to defendants sued under Texas law.

The legislature used a broad brush when it defined the terms used in this statute. “Access” is defined as follows: “to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer,

⁶ Congress modified several provisions of this law in the USA - Patriot Act, passed in the wake of September 11, and the Cyber Security Enhancement Act of 2002.

⁷ In *Thurmond v. Compaq Computer Corp.*, 171 F. Supp. 2d 667 (E.D. Tex. 2001), however, the same judge who decided the *Shaw* case ruled that a class of plaintiffs suing Compaq for selling computers with allegedly faulty floppy disk controllers could not, as a matter of law, meet the “damages” requirement under § 1030, because no single plaintiff suffered \$5,000 in damages in any one-year period and the court held that § 1030 did not allow the plaintiffs to aggregate damages suffered by multiple plaintiffs to meet the \$5,000 threshold. *See also Hayes v. Packard Bell NEC, Inc.*, 193 F. Supp. 2d 910 (E.D. Tex. 2002) (granting Packard Bell summary judgment where the plaintiff failed to establish \$5,000 in damages).

computer network, computer program, or computer system.” TEX. PENAL CODE § 33.01(1). This definition appears to cover almost any communication with or by a computer, and, interestingly, as the definition includes approaching a computer, it suggests that a person could “access” another computer merely by probing or scanning the open ports on that computer.

The terms “computer,” “computer network,” and “computer system” are also broadly defined to include virtually any data processing device and any “input, output, processing, storage, or communication facilities that are connected or related to the device.” TEX. PENAL CODE § 33.01(4)-(9).

While the federal hacking statute uses the terms “without authorization” or “in excess of authorization” to describe illegal computer access, the Texas code describes such conduct as occurring “without the effective consent” of the owner of the computer. In keeping with other sections of the Penal Code, consent is not effective when:

- induced by deception, or induced by coercion;
- given by a person the actor knows is not legally authorized to act for the owner;
- given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;
- given solely to detect the commission of an offense; or
- used for a purpose other than that for which the consent was given.

TEX. PENAL CODE § 33.01(12).

The fact that consent is not effective when induced by deception is an important provision as it covers a popular hacker technique used to access systems — social engineering. Social engineering is a process by which hackers contact a company and try to trick company insiders into releasing information they can use to penetrate the system. For example, Kevin Mitnick (the only computer hacker to make the FBI’s 10 most wanted list) used this technique to convince Motorola insiders to give him access to proprietary computer code.

Section 33.01(12)(E) of the Penal Code is also important as it covers situations in which an employee has consent to use a computer system for one purpose, but then uses it for other illegal purposes – similar to the “exceeding authorized access” issue under the CFAA.

In *Mitchell v. State*, 12 S.W.3d 158 (Tex. App. -- Dallas 2000, no writ), one of the few reported breach of computer security cases, the defendant contended that she could not be guilty of breach of computer security when she accessed her employer’s computer system and corrupted computer files, because she had authority to be on the system. In a terse opinion, the Dallas Court of Appeals rejected this argument finding that the defendant “was not authorized to corrupt [her employer’s] computer files” and thus the defendant’s computer access was without the effective consent of her employer. *Id.* at 159.

The Houston Court of Appeals issued a somewhat conflicting ruling in *Oswalt v. State*, No. 14-95-01131-CR, 1998 WL 349536, *n.2 (Houston [14th Dist.] 1998, pet. for discretionary rev. ref’d) (not designated for publication). In *Oswalt*, the Court of Appeals ruled that evidence concerning an employee’s deletion of computer files off of a corporate network shortly after the employee had

been fired was admissible over defendant's Rule 404(b) objection that such testimony constituted evidence of other bad acts, because, in the Court's opinion, such evidence did not establish the defendant committed the crime of breach of computer security as the defendant had permission to access the computer system. *Id.* at *2. The Court, however, did not discuss or make reference to § 33.01(12)(E), and this provision may have been overlooked by the Court. *Id.* at *2.

Despite the somewhat contrary ruling in *Oswalt*, the clear implication of the *Mitchell* case is that computer users who are permitted to use systems (whether at work or elsewhere) for one purpose, who then use the system for other, unauthorized purposes may be guilty of breach of computer security, and correspondingly liable under TEX. CIV. PRAC. & REM. CODE § 143.001.

3. Claims under the Federal Wiretap and Stored Communications Acts

In addition to the CFAA, two other federal statutes may be used to hold hacker's accountable – the Wiretap Act and the Stored Communications Act. The Wiretap Act provides a private cause of action as follows:

(a) any person whose wire, oral or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. §2520. The prohibitions of the Act apply to any person who:

intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication, . . . intentionally discloses, or endeavors to disclose . . . the contents of any wire, oral or electronic communication, knowing or having reason to know [it was obtained illegally], . . . intentionally uses, or endeavors to use, the contents [of any illegally obtained] wire, oral, or electronic communication . . .

18 U.S.C. § 2511(1)(a), (b), (c), (d). "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

The Stored Communication Act prohibits conduct that:

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished.

18 U.S.C. § 2701. An “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). “Electronic storage” is defined as:

- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
- (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. § 2510(17). This definition has been described as “extraordinarily – indeed, almost breathtakingly – broad.” *United States v. Councilman*, 245 F. Supp. 2d 319, 320 (D. Mass. 2003).

These statutes are important in the context of hacker liability because they cover some commonly used hacker techniques. Hackers want information, and one of the primary tools hackers use to gather information is a computer program known as a “sniffer.” Sniffers are network eavesdropping programs that sit on a computer attached to a network and record keystrokes or network traffic for the hacker. Hackers capture key information like passwords and user names in this way. Hackers will also seek this information while it is in storage by attacking databases that store information waiting to be transferred – such as an email sitting on a company mail server. Hackers that deploy sniffers or have accessed stored communications have likely engaged in illegal wiretapping or violations of the Stored Communications Act, and can be subjected to both criminal liability as well as civil liability under those statutes.

The Wiretap Act and the Stored Communications Act are also important in the commercial context because they may be implicated by commonly-used technologies such as web cookies or bugs. For instance, the First Circuit recently considered Wiretap claims brought by a class of visitors to various pharmaceutical company websites against the pharmaceutical companies and a company called Pharmatrak, which provided a monitoring service called “NETcompare” which allowed the companies to track how their websites were used by visitors. *See In re Pharmatrak, Inc.*, No. 02-2138, 2003 WL 21038761 (1st Cir. May 9, 2003). Pharmatrak’s service worked via “web bugs” and persistent cookies which caused visitors to the pharmaceutical websites to send information regarding the visitors’ web sessions directly to Pharmatrak. Pharmatrak was not supposed to capture personally identifiable information about the website visitors with this technology, but it did capture at least some of this information. The NETcompare service was invisible and presumably unknown to the website visitors.

The plaintiffs in *In re Pharmatrak* contended that this capture of personally identifiable information constituted an illegal interception of electronic communications under the Wiretap Act because the NETcompare service intercepted the contents of their electronic communications without their consent. Pharmatrak and the pharmaceutical companies argued that they had consented to the use of the NETcompare service and that this brought any interception of electronic communications within the “consent exception”⁸ to the Wiretap Act. *Id.* at *8. The First Circuit

⁸ The Wiretap Act provides that no violation occurs if “one of the parties to the communication has given prior
(continued...)

disagreed finding that any consent was not effective because the pharmaceutical companies had been assured by Pharmatrak that the NETcompare service would *not* capture personally identifiable information, and thus the pharmaceutical companies had not consented to the capture of this information. *Id.* at *9.

The First Circuit made two other interesting rulings. First, the Court held that the NETcompare services amounted to an interception, even though the service worked by creating a separate communication channel between the website visitor's computer and Pharmatrak's computers. The Court held that "[s]eparate, but simultaneous and identical, communications satisfy even the strictest real-time [interception] requirement." *Id.* *11. This real-time requirement is discussed in conjunction with the *Konop* case below.

The Court also noted that Pharmatrak correctly chose not to contest the issue of whether it captured the "contents" of communications as opposed to addressing or routing information.⁹ The demarcation between content and non-content information is important, because the Wiretap and Stored Communications Acts provide much greater protection to the contents of communications and it is not clear whether various Internet-based communications, such as search terms used in search engines, constitute the contents of a communication or not.¹⁰ In *In re Pharmatrak*, the First Circuit adopted a broad definition of "contents" stating in *dicta* that the information captured by the NETcompare service clearly qualified as contents of electronic communications, thus suggesting that search terms qualify as the contents of communications. *Id.* at *8 ("this definition [of contents] encompasses personally identifiable information such as a party's name, date of birth, and medical condition.")

The Ninth Circuit recently considered the "complex, often convoluted" intersection of the Wiretap Act and the Stored Communications Act in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). In *Konop*, a disgruntled Hawaiian Airlines pilot created a private website on which he made disparaging remarks about the airline. The pilot, Robert Konop, allowed other employees access to the site by registering and obtaining a password, but Konop expressly denied access to management. Nevertheless, James Davis, a Hawaiian Airline vice president, accessed the site using the name of Gene Wong, a pilot, who consented to Davis' use of his name. Konop found out about Davis' access and sued the airline under the Wiretap and Stored Communications Acts. *Id.* at 872-873.

⁸(...continued)

consent to such interception, unless such communication is intercepted for purpose of committing any criminal or tortious act" 18 U.S.C. § 2511(2)(d).

⁹ Transactional information such as this routing and addressing data is subject to less protection than the contents of communications. *See, e.g.*, 18 U.S.C. § 3123 (authorizing the installation of a pen register device to capture non-content information regarding communications, such as the numbers dialed from a cell phone, upon only a certification that such information is relevant to an ongoing criminal investigation).

¹⁰ *See* Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*. 97 NW. U. L. REV. 607 (2003) (discussing different levels of protection provided to content and non-content information and the ambiguity that exists in separating content from non-content information in the context of network communications).

The Court first determined that Konop’s website was an “electronic communication” because the website was stored electronically on a server and was transferred to other computers when it was visited. The Court then considered whether Davis’ access was an “interception” and thus a violation of the Wiretap Act, or whether it was “an access without authorization” and thus a violation of the Stored Communications Act. *Id.* at 876-79. After a detailed analysis, the Ninth Circuit ruled that there was no Wiretap Act violation because Konop’s website was *not* intercepted contemporaneous with its transmission, and post-transmission interceptions are not covered by the act. *Id.* at 878.

With regard to the Stored Communications Act, the Court assumed, and the parties agreed, that Davis’ access to Konop’s site amounted to an unauthorized access to a stored communication. *Konop*, 302 F.3d at 879-80. Hawaiian Airlines, however, did not concede liability, but contended that it was exempt from liability as it had Wong’s consent to access the site. *Id.* at 880. Under the Act, a person may authorize a third party to access an electronic communication if the person is a (1) “user” of the “service,” and (2) the communication is “of or intended for that user.” *Id.* The Ninth Circuit disagreed with the airline’s consent argument because Wong had never “used” the website and thus could not consent to Hawaiian’s access. Accordingly, the Court reversed the trial court’s entry of summary judgment in favor of Hawaiian Airlines and reinstated the Stored Communications Act claim. *Id.* at 880.

In *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001), the Court distinguished *Konop* in deciding that an employer’s review of an email that had been opened and saved by the employee-recipient of the email was not, as a matter of law, a violation of the Stored Communications Act because the email was not within “electronic storage” as defined by the statute. *Id.* at 636, (“retrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission.”)

However, other courts have ruled unauthorized access to opened and saved emails that are stored on the computers of an electronic communications service, such as Yahoo! or Hotmail – as opposed to a company’s internal mail server – can give rise to a Stored Communications Act violation. In *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914 (W.D. Wis. 2002), a church secretary overheard a personal call between the church’s youth minister and another man concerning homosexual sex while she was trying to make an outgoing call on a cordless telephone. The church suspended the youth minister and hired a computer expert to access the church’s computer for any evidence suggesting that the youth minister used the church’s computer to have improper sexual communications with minors. The expert was able to log on to the youth minister’s personal Hotmail account and retrieve emails from the minister’s account on Hotmail’s computer when he guessed the youth minister’s password. Subsequently, the youth minister sued the church under both the Wiretap Act, for eavesdropping on his personal phone call, and the Stored Communications Act, for accessing his stored e-mail messages.

Relying on *Fraser*, the church argued that it could not have violated the Stored Communications Act because the email messages it retrieved had already been read by the youth minister and thus could not be in electronic storage under the Act. The Court rejected this argument because the youth minister’s emails, unlike the emails in *Fraser*, were stored on Hotmail’s computers and thus were stored by an electronic communication service. *Id.* at 925.

III. Tort Liability

The current statutory scheme discussed above places liability for computer hacking on the hacker, which is great if your client happens to get hacked by Bill Gates or Donald Trump, but not very helpful if the hacker turns out to be the run-of-the-mill variety.¹¹ Instead of suing the hacker, litigants may look to tort theories to hold other, deeper pockets liable. To date, courts have not wrestled extensively with tort claims brought to recover damages resulting from hacking, but several commentators have recognized the potential for liability.¹² The following discusses some of the tort theories that could be utilized to recover damages for hacking.

1. Negligence

If a hacker causes harm and the hacker is judgment proof, then hacking victims may look to recover from others whose negligence fostered the attack. This could be the ISP who failed to properly secure its network, companies whose computers were used as “bounce” sites or as “zombies” to launch attacks, or even companies that hired a known hacker and gave him or her access to high bandwidth and a computer. A negligence claim brought against any of these potential defendants will have to overcome several hurdles to be successful.

The oft-cited elements of negligence are duty, breach and damages proximately caused by the breach. *See Houser v. Smith*, 968 S.W.2d 542, 545 (Tex. App. – Austin 1998, no pet.) The threshold inquiry for any court considering a negligence claim brought to recover damages for computer hacking is the existence of a duty. Generally, “a person has no duty to protect another from the criminal acts of a third person.” *Walker v. Harris*, 924 S.W.2d 375, 377 (Tex. 1996); *Timberwalk Apartments, Partners, Inc. v. Cain*, 972 S.W.2d 749, 756 (Tex. 1998). Under this “no duty” doctrine, a company whose insecure computers were hacked and then used to launch a denial of service attack against a second company would not be liable to the second company for damages caused by the denial of service attack, even if the first company was negligent for failing to properly secure its computers, because the first company owes no duty to protect the second company from the criminal acts of third parties such as the hacker.¹³

This general “no duty” rule, however, is not absolute. Courts have identified at least three situations in which a duty to protect a person from the criminal acts of a third party may arise: (1) an owner of property who maintains control over the property owes a duty to protect invitees from

¹¹ See WINN SCHWARTAU, *CYBERSHOCK: SURVIVING HACKERS, PHREAKERS, IDENTITY THIEVES, INTERNET TERRORISTS AND WEAPONS OF MASS DISRUPTION* 36-37 (Thunder’s Mouth Press 2000) (describing hackers as: being “largely males from age 12-28,” from “dysfunctional upbringings and families,” who exhibit “Narcissistic Personality Disorder”).

¹² Stephen E. Henderson & Matthew E. Yarbrough, *Suing The Insecure? A Duty of Care in Cyberspace*, 32 N.M.L. REV. 11 (2002); Raul, Volpe & Meyer, *Liability for Computer Glitches and Online Security Lapses*, 6 BNA Electronic Commerce Law Report 31 (2001); Jane Radin, *Distributed Denial of Service Attacks: Who Pays?*, available at <http://www.mazunetworks.com/white_papers/radin-print.html>.

¹³ Jane Radin, *Distributed Denial of Service Attacks: Who Pays?*, available at <http://www.mazunetworks.com/white_papers/radin-print.html> (discussing third party liability for a DDoS attack).

foreseeable and unreasonable risks of harm from the criminal acts of third parties; (2) a person with a special relationship with a third party may owe a duty to control the conduct of that third party; and (3) a person who has created a dangerous situation owes a duty to prevent harm to others because of the situation he or she created. *See San Benito Bank & Trust*, 31 S.W.3d 312, 318-319 (Tex. App. – Corpus Christi 2000, no pet.) (discussing these exceptions); *A.H. Belo Corp.*, 52 S.W.3d 375, 382 (Tex. App. – Houston [1st Dist.] 2001, pet. denied) (discussing special relationship and creation of danger exceptions).

Courts faced with cases involving significant damages resulting from computer attacks that could have been easily prevented with proper security measures may be tempted to hold that a duty arises justifying an award of damages for a hacking incident. Courts may find, for instance, that a negligence claim based on hacking is analogous to a typical premises liability claim in which an invitee is victimized while on the property of another. In the typical premises liability case, courts will hold the property owner liable for the invitee's injuries if the property owner maintained control of the property and if the invitee suffered harm because of an unreasonable and foreseeable risk. A court may conclude an invitee injured on another's property is in a similar situation to a company whose online operations are attacked by hackers while they are being hosted at a third-party ISP. The situations are legally analogous, if we assume that both the property owner and the ISP maintain control over the location of the harm – the physical property in one case, and the virtual property in the other – and the harm (whether from a physical attack or a computer attack) is foreseeable to both.¹⁴

Even if courts were to recognize a duty, there still may be difficulty in defining the standard of care that should be applied. To date, members of the computer industry have failed to develop workable standards.¹⁵ Some commentators have suggested using the "risk-utility test" or the "reasonable prudence test" to set the standard of care.¹⁶ Under a "risk-utility test", the utility of the conduct is balanced against the likelihood and extent of harm to foreseeable plaintiffs. Under a "reasonable prudence test," the standard of care is that which a reasonably prudent person (provider, engineer or programmer, etc.) would exercise in the same or similar circumstances. One useful source for standards might be industry custom.¹⁷ Standards may also be derived from new regulations such as the Health Insurance Portability and Accountability Act of 1996 or the Gramm-Leach-Bliley Act of 1999, which require particularly sensitive information like medical records and financial data to be protected¹⁸.

¹⁴ This assumes, of course, that the online business and the ISP do not have a contract covering their relationship, which is unlikely.

¹⁵ Robin A. Brooks, *Deterring The Spread of Viruses Online: Can Tort Law Tighten The Net?*, 17 REV. LITIG. 343, 361 (1998).

¹⁶ *Id.* at 361-63.

¹⁷ Stephen E. Henderson & Matthew E. Yarbrough, *Suing The Insecure?: A Duty of Care In Cyberspace*, 32 N.M.L. REV. 11 (Winter 2002)

¹⁸ *Id.*

The “economic loss rule” may be another barrier to recovery. Where a party suffers only economic damages, he or she is barred from suing in tort because of the so-called “economic loss rule.” See *Hou-Tex, Inc. v. Landmark Graphics*, 26 S.W.3d 103, 106 (Tex. App. – Houston [14th Dist.] 2000, no pet.) (barring negligence claim based on defective seismic software because plaintiff suffered only economic loss). This rule will not apply, however, if the injured party suffers property damages. Thus, if an electronic attack damages computer hardware or corrupts or erases data, the economic loss rule may not apply.¹⁹

2. Negligent Hiring/Supervision

If a hacking victim is lucky enough to have been attacked by a hacker who works for a solvent company and the attack was launched from an officer computer, the hacker may be able to seek compensation from the hacker’s employer. Of course, if the employer authorized the hacking, the victim would be entitled to recover under the doctrine of *respondeat superior*, but this scenario is unlikely. If the employer did not authorize the hacking, the plaintiff might have viable negligent hiring or negligent supervision claims.²⁰ “An employer has a duty to adequately hire, train, and supervise employees. The negligent performance of those duties may impose liability on an employer if the complainant's injuries result from the employer's failure to take reasonable precautions to protect the complainant from the misconduct of its employees.” *Castillo v. Gared, Inc.*, 1 S.W.3d 781, 786 (Tex. App.—Houston [1st Dist.] 1999, pet. denied). If a company hires an employee, as a computer security specialist for example, when the company knows the employee has a propensity to hack computers and then provides the employee unsupervised access to a computer and a high-bandwidth connection to the Internet, the company may be liable for any hacking activities the employee engages in from work.

3. Trespass to Chattels

In addition to negligence theories, a plaintiff may be able to recover damages caused by hackers under a trespass theory. Trespass to chattels involves the wrongful interference with the use or possession of property. *Jarvis v. Southwestern Bell Tel. Co.*, 432 S.W.2d 189, 191 (Tex. Civ. App. – Houston [14th Dist.] 1968, no writ). Liability for a trespass to chattels will attach if the wrongful interference causes actual damage to property or deprives the owner of its use for a substantial period. *Zapata v. Ford Motor Credit Co.*, 615 S.W.2d 198, 201 (Tex.1981).

Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996) was one of the first cases to find trespass to chattels applied to electronic communications.²¹ In *Thrifty-Tel, Inc.*, a group of minors hacked into Thrifty-Tel’s phone system and obtained codes which allowed them to make

¹⁹ In addition, some states are recognizing the unfairness inherent in the economic loss rule. See, e.g., *People Express Airlines v. Consol. Rail Corp.*, 495 A.2d 107 (N.J. 1985) (concluding that “a defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty.”)

²⁰ Erin M. Davis, Comment, *The Doctrine Of Respondeat Superior: An Application To Employers’ Liability For The Computer Or Internet Crimes Committed By Their Employees*, 12 ALB. L.J. SCI. & TECH. 683, 694-95 (2002).

²¹ John D. Saba, Jr., Comment, *Internet Property Rights: E-Trespass*, 33 ST. MARY’S L.J. 367 (2002).

numerous long-distance calls without incurring any charges, a form of hacking known as “phone phreaking.” The large number of calls made by the phreakers overburdened the phone system and denied at least some other users the ability to make phone calls. Thrifty-Tel sued the parents of the minors for fraud and conversion. The Court was doubtful that the tort of conversion covered the phreakers’ conduct because, in its view, the phreaker’s had not converted tangible property. Instead of reversing on the conversion claim, however, the Court found the phone company could recover for trespass to chattels because the minors’ access to Thrifty-Tel’s phone codes amounted to a trespass to personal property which proximately caused damage. *Id.* at 473.

At least two federal courts have found that the trespass to chattels doctrine covers electronic trespassers. In *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Calif. 2000), the District Court for the Northern District of California granted a preliminary injunction preventing Bidder’s Edge from crawling eBay’s website to gather information on eBay auctions. The Court held that eBay was likely to succeed on its trespass to chattels claims because Bidder’s Edge’s use of a robot computer program to crawl eBay’s website was not authorized and deprived eBay of a “small amount of eBay’s computer system capacity.” *Id.* at 1071. Importantly, the Court held that an interference to another’s possessory interest did not have to be “substantial” in order to qualify as a trespass to chattels saying, “[c]onduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another’s personal property, is sufficient to establish a cause of action for trespass to chattels.” *Id.*

Similarly, in *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), the District Court for the Southern District of New York found that Verio’s use of “Search Robots” to search Register.com’s “WHOIS” database amounted to a trespass to chattels. Verio’s initial presence on Register.com’s site was permitted but became unauthorized after Register.com withdrew that permission. Like the *eBay* Court, the Court in *Register.com* required only a showing of “possessory interference” to support the trespass to chattels claim. *Id.* at 250. Accordingly, even though Verio’s presence on Register.com’s computers was “negligible,” the Court held that such presence deprived Register.com of at least some of the use of the system capacity and thus constituted possessory interference sufficient to uphold the trespass claim. *Id.* at 250-51.

Hence, under *eBay* and *Register.com*, it appears that an unauthorized access to another’s computer system that uses even a *di minimus* amount of computer capacity will support a trespass to chattels claim.²²

²² While the author has found no Texas cases addressing a trespass to chattels claim brought after an unauthorized access to a computer, at least one Texas court has considered whether sending unsolicited faxes constitutes a trespass to chattels. See *Omnibus Int’l. Inc. v. AT&T Inc.*, No. 05-01-01039-CV, 2002 WL 31618413, at *4 (Tex. App. – Dallas Nov. 21, 2002, no pet.) (not designated for publication) (finding no trespass to chattels as a matter of law because there was no evidence that the owner of the fax machines was deprived of their use for a substantial period of time).

IV. Other Avenues of Recovery for Computer Hacking

1. Contract Liability

While substantial uncertainty remains as to whether tort law provides reliable avenues of recovery to hacking victims, victims may be able to seek recovery under more determinate claims for breach of contract. This is because many companies in today's interconnected world share information across computer networks with other companies, and these companies are increasingly entering agreements which require the networks to be reasonably secure. In addition, other contracts such as terms of use agreements, terms of service agreements, and employee agreements may contain provisions that cover some forms of computer hacking. If such a contract is in force, there may be contractual liability for hacking activities.

A breach-of-contract theory of liability has several advantages over tort theories. First, there will be no issue of duty as the contract itself creates the obligation or duty. Second, well-drafted contracts will specify the standard of conduct that must be met to satisfy the contract, thus avoiding ambiguity as to the standard of care required. Third, monetary damages are routinely recoverable for breaches of contract and the "economic loss rule" does not apply.²³

In addition to contracts between businesses, insurance companies are writing policies which provide coverage for damage caused by hackers or which cover damage caused by a company's errors and omissions in maintaining secure computers.²⁴ Not surprisingly, these policies contain numerous exclusions, but the potential for coverage should be explored as another possible avenue of recovery in the wake of any loss due to hacker activity.

2. Theft of Trade Secrets

Trade secrets today are often stored digitally – as a series of ones and zeros – which, like any computer file, can be easily and quickly copied and transferred over long distances with little chance of detection. Because these digitally stored trade secrets can be so valuable, litigation involving computer hacking is likely to also involve claims for theft of trade secrets.

Under common law, "a trade secret may consist of any formula, pattern, device, or compilation of information that is used in one's business and which gives one an opportunity to obtain an advantage over competitors who do not know or use it." *Computer Assocs. Int'l, Inc. v. Altai, Inc.*, 918 S.W.2d 453 (Tex. 1996). While most civil claims for theft of trade secrets involve common law claims, there is another option – The Texas Theft Liability Act. Codified at TEX. CIV. PRAC. & REM. CODE § 134.001 *et seq.*, this statute creates a cause of action against any person who violates Section 31.05 of the TEXAS PENAL CODE, which criminalizes the theft of trade secrets. Under this

²³ There are drawbacks as well. Contract claims can generally only be brought against those "in privity" of contract, and thus third-party liability is generally not available under a contract theory. *See* Faulkner *supra* at 1026.

²⁴ *See, e.g.*, Sarah Faulkner, Comment, *Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1019, 1046 (Summer 2000) (discussing specialized insurance designed to protect businesses from losses due to computer hacking).

statute, a person who, without the owner's effective consent, knowingly: (1) steals a trade secret; (2) makes a copy of an article representing a trade secret; or (3) communicates or transmits a trade secret commits a felony offense. TEX. PENAL CODE § 31.05. The statutory definition of "trade secret" is broader than the common law definition:

the whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to have access for limited purposes.

TEX. PENAL CODE § 31.05(a)(4)

In *Schalk v. State*, 823 S.W.2d 633 (Tex. Crim. App. 1991), the Court of Criminal Appeals considered a criminal prosecution based on a factual situation similar to a typical civil theft of trade secret lawsuit. In *Schalk*, several ex-employees of Texas Instruments ("TI") were prosecuted under § 31.05 because they copied computer programs from TI's computers when they left TI to form a competing company. On appeal, the ex-employees argued that TI had not taken sufficient "measures" to protect the trade secret status of the purloined computer programs as required by § 31.05. *Id.* at 637. The defendants noted that TI had encouraged them to share information about the computer programs to others in the same research field, that numerous articles concerning the computer programs had been published, and that meetings during which information regarding TI research was discussed had been held. The defendants were even able to point to situations where the programs had been distributed to schools and government agencies involved in similar research projects. *Id.* at 637-642.

The Court of Criminal Appeals rejected these arguments finding that TI had taken sufficient measures to protect its trade secrets under § 31.05. The Court specifically discussed the following measures taken by TI:

- employee non-disclosure agreements;
- plant security;
- limited access to information; and
- other measures.

The combination of these measures, the Court held, was sufficient to overcome the limited disclosures by TI. *Id.*

If a hacker steals trade secrets electronically, the victim should consider combining claims for the hacking activity with claims under the Texas Theft Liability Act. First, as discussed above, the definition of "trade secret" under § 31.05 of the Penal Code is extremely broad. There is no requirement that the holder of the trade secret actually use it, and secrecy can be established by showing the holder has taken "measures" to prevent the trade secret from becoming known to persons other than those to whom the holder has provided access for limited purposes. Moreover, as the Court of Criminal Appeals explained in *Schalk*, if "measures" have been taken, limited disclosure of a trade secret will not vitiate trade secret status. In the right factual setting, then, a trade secret not protected by common-law misappropriation doctrines, may still be protected by this statute.

In addition, it appears plaintiffs suing under this statute have a broader range of recovery than they would under common law. Claims brought under the Texas Theft Liability Act are not subject to the standard cap on exemplary damages – two times the plaintiff’s economic damages – contained in TEX. CIV. PRAC. & REM. CODE § 41.08. This is because § 41.08(c)(13) provides that the exemplary damage cap does not apply to causes of action based on conduct which would be a felony under Chapter 31 of the TEXAS PENAL CODE.

The statute also provides a prevailing plaintiff with *mandatory* attorney’s fees and costs. Section § 134.005 states that a prevailing party under the statute “*shall be awarded court costs and reasonable and necessary attorney’s fees.*” At least one court has interpreted this provision to require an award of attorney’s fees when the plaintiff obtained a favorable ruling on the issue of theft, but no damages. *Johns v. Ram-Forwarding, Inc.*, 29 S.W.3d 635 (Tex. App.—Houston [1st Dist.] 2000, no pet.)

3. Copyright Claims

A copyright adheres instantly in “original works of authorship fixed in any tangible medium of expression.” 17 U.S.C. § 102(a) (1996). Hackers often target material protected by copyrights because of its value and because this material is increasingly created, stored, and sold in a digital format or in formats easily converted to a digital format. These products – most notably music, software, and now digital movie files – can be reproduced quickly, cheaply, and with very little, if any, loss in quality, and thus the damages caused by a hacker’s misappropriation of this material can magnify quickly. As any user of KaZaA (or former user of Napster) knows, the Internet has made it possible to easily distribute (legally or illegally) vast quantities of digital media to countless people worldwide with very little expense.

Congress has responded to mass online copyright infringement by passing new laws designed to protect copyright holders. One of these new laws, the Digital Millennium Copyright Act (DMCA), targets a traditional hacker goal – bypassing copyright protection measures designed to prevent the unauthorized use of a copyrighted work. The DMCA provides a civil cause of action to anyone injured by a violation of the statute. 17 U.S.C. § 1203.

Perhaps the best known example of the DMCA’s use against hackers is the litigation surrounding DeCSS – a program developed by a Norwegian computer programmer that circumvents the encryption used by major movie studios on DVDs. See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 440-442 (2nd Cir. 2001). In *Corley*, the publishers of *2600 – The Hacker Quarterly*, a magazine catering to computer hackers, published the DeCSS code in their magazine and on their web site and also provided numerous links on their web site to other sources for the program. The movie studios sued under the DMCA to enjoin the distribution of the code. After a bench trial, the studios obtained a permanent injunction prohibiting the distribution and publication of DeCSS. On appeal, the Second Circuit considered several constitutional challenges to the DMCA and ruled that the law was constitutional and the injunction appropriate. *Corley*, 273 F.3d at 440-442.

The DMCA also contains provisions which greatly increase copyright owners’ ability to police Internet-related infringement by utilizing the civil justice system. The DMCA allows copyright owners to obtain a federal subpoena requiring an ISP, if certain conditions are met, to “expeditiously disclose” information pertaining to the ISP’s subscribers who are allegedly infringing the owner’s copyrights. 17 U.S.C. § 512(h). This tool is akin to the most-commonly used procedure prosecutors

and cops employ to investigate computer crime – grand jury subpoenas requiring an ISP to disclose the identity and information about one or more of its subscribers.

This provision was recently subjected to judicial scrutiny in *In re Verizon Internet Services*, 240 F. Supp. 2d 24 (D.D.C. 2003). This case resulted when the Recording Industry Association of America, utilizing § 512(h), served a subpoena on Verizon requiring Verizon to disclose identifying information about one of its subscribers who had allegedly downloaded more than 600 songs in a single day using the peer-to-peer file transfer program KaZaA. Verizon refused to comply with the subpoena contending that the DMCA did not apply because the music files at issue resided on the subscriber's computer and not on any part of Verizon's network. After a thorough analysis, the District Court rejected Verizon's arguments and held that the subpoena was enforceable. *Id.*

The implications of this ruling are immense, because unlike almost any other civil litigant, a copyright owner can use the DMCA to obtain court process requiring the disclosure of information about potential infringers without having to file a lawsuit. In other words, the DMCA grants to copyright owners at least some measure of investigative power that traditionally has been reserved for law enforcement.

V. Conclusion

The concept of liability based on computer hacking is in its infancy, and precisely how and when liability will be imposed in the online arena remains to be determined. Courts faced with hacking claims will likely have to explore a myriad of issues involving the application of criminal law in civil court and the application of tort and contract law to conduct occurring online. While this area is new, it is likely to grow quickly, as more companies and individuals suffer at the hands of hackers.