The Computer Fraud and Abuse Act: An Effective Tool for Prosecuting Criminal and Civil Actions in Cyberspace

Vicki M. Luoma and Milton H. Luoma, Jr.

Vicki M. Luoma, Assistant Professor Minnesota State University, Mankato
Milton H. Luoma, Jr., Assistant Professor, Metropolitan State University

Abstract

The Computer Fraud and Abuse Act became law in 1984 as the legislative response to the then relatively new phenomenon of computer hacking. Subsequent amendments strengthened the law, and in 1996 the critical Section (g) was added to the law authorizing civil actions against violators. A recent criminal case, however, may expand the application of the law to misuse of the terms of use of public Web sites. This paper examines some of the applications of the Computer Fraud and Abuse Act in both criminal as well as the civil actions. While the full impact of this statute in the future is not entirely clear, the statute will most definitely serve as a effective tool against virtually any computer misuse.

Introduction

Although hackers have been around for over 40 years, by the 1980s the problem had reached epidemic proportions. "Hacker" is the term used for people who gain unauthorized access to another's computer for the purpose of stealing or corrupting data. Originally, the term "hacker" was benign with no negative connotation. It simply referred to those who wanted to develop their computer skills and sought the challenge of accessing and exploring computers without any intention to steal or destroy anything.[1] Hackers range from bored teenagers to organized criminals.

In one of the first arrests of hackers, the FBI arrested Milwaukee-based 414s (named after the local area code) whose members were accused of 60 computer break-ins ranging from Memorial Sloan-Kettering Cancer Center [2] to the Los Alamos National Laboratory.[3] In addition to hacking, computer worms, viruses, Trojan horses, computer terrorism, phishing and pharming have become a virtual plague in the area of computer problems.

---

[1] Nick Ackerman, "CFAA as a Civil Remedy." *National Law Journal*, 2005: 10-12.

[2] Edmund Burke, *The Expanding Importance of the Computer Fraud and Ab use Act.*, 2001.

[3] Id

The Computer Fraud and Abuse Act

In 1984 in response to hacking threats, the United States Congress enacted the Computer Fraud and Abuse Act, 18 U.S.C. 1030.[4] The primary purpose of CFAA was to protect government computers and financial records and credit information on both the government's and financial institutions' computers. It became apparent soon afterward that a stronger law was needed to properly address the threats. Since its inception the act did not quite meet the needs of the government and was constantly being amended. In 1986 the Act was amended to cover any federal interest computers.[5] In 1996 the law was again amended to include the term "protected computer," which now meant any computer involved in interstate or foreign commerce.[6]

The Act went through many amendments and incarnations when, somewhat mysteriously, Section (g) appeared in 18 U.S.C. 1030 in 1996.[7] The mysterious Section (g) was unusual and atypical not only because it now provided civil remedies in a criminal statute, but it also contained unprecedented language allowing private companies to pursue violations of this law. Since there are no records, session notes or writings to explain the purpose of Section g, one can only assume that the government could augment its limited resources by enlisting private corporations to also go after hackers in civil actions. This section allows organizations to take the lead and to be the protector of personal data stored in their computers, but it also makes the stealing of data from a computer a federal crime that can be corrected through a civil lawsuit.

The text of Section (g) is as follows:

---

4 Computer Fraud and Abuse Act, 18 U.S.C. 1030

5 Id

6 Id

7 Id

> (g) 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). Damages for a violation involving only conduct 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.

One can certainly understand the notion of the government trying to obtain help from corporations with deep pockets to stop these insidious computer crimes. However, corporations have not prosecuted civil actions against these criminals probably because no matter how much damage the culprits committed or how much money they cost the companies; the perpetrators likely did not have assets from which to collect judgments.

Criminal Prosecutions

One provision that has been pursued both civilly and criminally is the provision where the defendant either accessed a computer without authorization or the defendant accessed a computer and exceeded his or her authorization. One problematic aspect of the provision "exceeding authorization" is that it has not been defined in the statute itself. As result there has been frequent litigation in both civil cases and criminal cases as to the meaning of the term "exceeding authorization." Another requirement of the statute is that if the violator is an insider, then there is an additional requirement that there be intentional damage to the computer. If the violator is an outsider he or she can be criminally liable for any intentional, reckless, or other

damage caused by the trespass. This point is illustrated in the decision in the *United States v. Czubinski.*[8]

Czubinski was an employee of the Internal Revenue Service and as a part of his employment as a contact representative for the Boston office he had access to the IRS database known as the Integrated Retrieval System (IDRS) located in West Virginia. With his password he could access any taxpayer's information stored in this database. The IRS rules clearly informed[i] employees that they were not allowed to access files on the IDRS for any purpose other than for their official employment duties. In 1992 Czubinski accessed numerous taxpayers' files for no legitimate purposes. After 1992 he did not access any more files, and continued to work for the IRS until 1995 when he was indicted for accessing files exceeding authorization. He was convicted of all four CFAA accounts by the trial court. On appeal the court found that although it was clear Czubinski had violated the portion of the statute regarding exceeding his authority, the government had not proven that Czubinski had damaged the government. It was revealed at trial that Czubinski, who was member of the Ku Klux Klan, had intended to make dossiers on potential KKK informants, but he never took steps in furtherance of that purpose in the three years after accessing the material originally for that purpose. However, in *Sawyer v. Department of Air Force*[9] the court decided under CFAA 1030(a)(3) there are no benign intrusions into government computers resulting in inconsistent interpretations of this provision.

---

[8] United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997)

[9] Sawyer v. Department of Air Force, 31 M.S.P.R. 193, 196 (M.S.P.B. 1986).

In *United States v. Morris,* [10] the defendant Morris, a first year Ph.D. student at Cornell University created a worm and released it on the Internet to show the inadequacies of computer security. Morris claimed that he meant the worm to be harmless and educational and that there should be a requirement that he intended to cause damage. Regardless of Morris' intent, damage was caused to government computers. Morris was found guilty of intentionally accessing and causing loss to federal computers. In this case the court ruled that the law requires only the intent to access and not the intent to damage.[11]

A more creative use of the CFAA is the case of *United States v. Lori Drew.* [12] In this case Drew helped create a fake MySpace account to convince Megan Meier she was chatting with a nonexistent 16-year-old boy named Josh Evans. MySpace is a social network in which participants can share information, pictures, videos and messages. To become a MySpace member and then be able to access the sites' content and communication section, members must complete registration information including name and date of birth, and agree to certain terms of service. Individuals can not become members unless they agree to those terms. Among the terms is the requirement that members provide truthful and accurate registration information and agree not to use the information obtained from MySpace to harass, abuse or harm other people.[13] In September 2006, Drew and her co-conspirators obtained an account on MySpace under a fictitious name, Josh Evans, and put up an unauthorized picture of a young man for the purpose of sending cruel messages to Megan. Drew continued to send messages from September to

---

10 United States v. Morris, 428 F.2d 504

11 United States v. Morris United States Court of Appeals, Second Circuit, 1991. 928 F.2d 504

12 United States v Lori Drew, Grand Jury Indictment Feb 2008

13 http://www.myspace.com/, retrieved March 1, 2008

October 16, 2006. [14] On October 16, 2006 Megan received a message that the world would be a better place without her. Megan hanged herself after this last message.[15] In this case the prosecutors are charging that Lori Drew's access to the MySpace Internet site violated the CFAA because by providing false information she violated MySpace's terms of use, and her access was, therefore, unauthorized. [16] The case is presently working its way through the courts, but it has definitely caused a fury of controversy. The question is whether this case agrees with the prosecution that violating a web site's terms of service could criminalize routine behavior on the Internet and allow businesses to establish the criminal standards.

Civil Actions

To bring a civil action under CFAA litigants must rely on Section (g) of the CFFA.[17] Most litigation in this area has involved employers suing employees for misuse and unauthorized access of company computers. Section (g) was a silent clause until 2000 when the attorneys, Warren Rheaume and Roanne Spiegel, for Shurgard Storage Centers Inc, drafted a complaint alleging Safeguard Self Storage for misappropriation of trade secrets, conversion, unfair competition, tortuous interference with business expectancy and violations of the Computer Fraud and Abuse Act and for injunctive relief and damages. [18] The defendant brought a motion to dismiss the complaint based on the Consumer Fraud Abuse Act.

The Shurgard Case

---

[14] Id

[15] Id

[16] Id

[17] 18 U.S.C. §1030, sec g.

[18] *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Washington, 2000)

Shurgard Storage Center is a leader in full- and self-storage facilities in the United States and Europe. Shurgard credits its success over the past 25 years to the development and construction of top-quality storage centers in "high barrier to entry" markets. [19] Shurgard has developed a sophisticated system of creating market plans, identifying appropriate development sites, and evaluating whether a site will provide a high return on an investment. As a result Shurgard invests a significant amount of company assets in creating marketing teams to carrying out these tasks for each potential market. The teams become familiar with the market, identify potential acquisition sites, and develop relationships with brokers and sellers in the market. [20]

In 1997, Safeguard began self-storage operations with its market goals in both the United States and Europe. Safeguard was a direct competitor of Shurgard Storage Center.[21] In late 1999 Safeguard Self Storage contacted Eric Leland, a regional development manager for Shurgard and offered him employment. Eric Leland had full access to Shurgard confidential business plans, expansion plans and other trade secrets. While still working for Shurgard, but after accepting a position with Safeguard, Eric Leland sent emails to Safeguard with various trade secrets and proprietary information. [22] Then, after starting to work for Safeguard, Mr. Leland continued to provide confidential information to his new employer. After hiring Eric Leland, Safeguard continued to hire additional employees of Shurguard who had proprietary information. [23]

---

19 Id.
20 Id
21 Id
22 Id
23 Id

Safeguard brought a motion to dismiss Shurguard's claim with Safeguard arguing that the employees had authorized access to the information by means of their employment with Shurgard, thus there could be no "unauthorized access " as required by the Computer Fraud and Abuse Act. [24] Under the CFFA an employer may bring suit against anyone who

(1) knowingly and without authorization transmits information and thereby intentionally causes damage to a protected computer, or
(2) Intentionally accesses a protected computer without authorization and, as a result, causes at least $5,000 in loss to one or more persons during any one year period. [25]

This case may have been just another case about trade secrets had there not been a creative litigator and an innovative judge. Safeguard argued that the Computer Fraud and Abuse Act simply did not apply to this case. Clearly, the employee had not "exceeded his authorized access" to the computer.[26] Actually, the employee had just taken advantage of the access that was provided him as part of his job responsibilities. The Computer Fraud and Abuse Act limits the meaning of "exceeding authorized access" to encompass only the obtaining or altering information that the person accessing information is not entitled to obtain or alter.[27]

Shurgard claimed that the employee had in fact accessed the computer "without authorization" in violation of Computer Fraud and Abuse Act.[28] Shurgard argued that under the common law of agency a disloyal employee who acts surreptitiously while on the employer's premises, such as acting in furtherance of his intent to go to work for a competitor and to use the employer's secret information for the benefit of a competitor has in effect terminated the

---

[24] See supra at note 14
[25] See Supra at note 14
[26] See Supra at note 15
[27] See Supra at note 14
[28] Id

authorization that was given to them.[29] Therefore, once Eric Leland became a disloyal employee, his authorization was rescinded, and when he continued to access his employer's computer by sending emails he was no better than a hacker. [30]

The court agreed with Shurgard's legal arguments. The court found that the employee's authorization ended at the time when the employee effectively became an agent for Shurgard's competitor, Safeguard. Judge Zilly cited the Restatement of Agency, "Unless otherwise agreed, the authority of any agent terminates if, without knowledge of principal, he acquires adverse interests or if her otherwise guilty of a serious breach of loyalty to the principal." [31] The court found that "the authority of the plaintiff's former employees ended when they allegedly became agents of the defendant."[32]

The court found that the employee loses authorization even if the employer still believes the employee is acting properly. Therefore, the employee could be subject to federal criminal action and the new employer could be deemed a party who is participating in a criminal conspiracy. The court ruled that there is an implicit revocation of the employer's authorization when the employee no longer acting loyal to the employer unless a contrary rule is otherwise agreed. [33]

By giving broad interpretations to these phrases the court effectively created an additional cause of action in favor of employers who may suffer the loss of trade secret information at the hands of disloyal employees who act in the interests of a competitor and future employer. The

---

[29] Id
[30] Id
[31] Id
[32] Id
[33] Id

court concluded that the extensive language in the legislative history demonstrated the broad meaning and intended scope of the terms "protected computer" and "without authorization."[34]

The court also found that the 1996 amendments to the CFAA expanded the scope of the act to cover so-called "protected computers." [35]As used in the Act, a "protected computer" includes any computer "which is used in interstate or foreign commerce or communication." [36]The court found that although earlier versions of the CFAA addressed outside hackers who attacked federal interest computers, the subsequent amendments to the CFAA broadened the scope of the Act sufficiently to cover the behavior alleged in the case, namely, that of an employee who uses his employer's computer system in a disloyal way.[37]

The judge concluded that the CFAA was "intended to control interstate computer crime, and since the advent of the Internet, almost all computer use has become interstate in nature." [38]The court had no difficulty in quickly concluding that Shurgard's computers, attached to the Internet, were indeed "protected computers" within the meaning of the CFAA.[39]

The Impact of the Shurgard Case

After the Shurgard case employers are no longer limited to traditional state and federal remedies. Employers can bring actions against employees for misappropriation of information, damage to information or even information that is not a trade secret at all if obtained or

---

[34] Id
[35] Id
[36] Id
[37] Id
[38] Id
[39] Id

transmitted through computers. Shurgard has opened the floodgates to more and more employer lawsuits. With each new lawsuit the meaning of Section (g) has expanded.

In the past, employer-employee disputes would have been litigated around the issues of covenants not to compete or restraint of trade. However, over the years these theories of law have come into disfavor with the courts. Covenants not to compete impede the full participation of a competitor, thus limiting competition.[40] Even worse, it restricts an employee from seeking or obtaining other employment. Most states now recognize and enforce reasonable covenants not to compete. However, the court will uphold a covenant not to compete only if it imposes no more than a reasonable restraint on trade. A reasonable covenant:

1. Must protect a company's legitimate business interest.
2. May not impose restraints greater than those necessary to protect the employer's legitimate business interests.
3. May not impose an undue hardship on the employee
4. Must avoid undue detriment to the public good.[41]

Shurgard has allowed employers circumvent these traditional legal requirements.

The law 18 USC 1030 was meant to stop the hackers, worm developers and other computer abuses, but creative application of the law has empowered employers in litigation against their employees. In *Nexans Wires S.A. v. Sark USA Inc.,* 319 F. Supp. 2d 468, 469 (S.D.N.Y)[42] Judge Miriam Cedarbaum granted summary judgment to the defendant on all of the CFAA claims because Nexan Wires could not establish the jurisdictional statutory threshold that

---

40 Id

41 Id

42 *Nexans Wires S.A. v. Sark USA Inc.,* 319 F. Supp. 2d 468, 469 (S.D.N.Y)

it had suffered $5,000 in loss.[43] Nexans Wires could have avoided the dismissal if they had simply hired a computer forensic specialist and incurred the jurisdictional amount in expenses.

In *EF Cultural Travel BV v. Explorica, Inc.* (U.S. Court of Appeals for the First Circuit, 2003)[44], a federal appeals court affirmed an injunction entered under the CFAA in favor of an online 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 Web site.[45] Use of the scraper program on the Web site constituted an unauthorized computer access, ruled the court, because the ex-employees breached their confidentiality agreements with their former employer when they developed the program. [46] The only way that EF cultural could meet the jurisdictional requirements is that it paid $20,944.92 to a computer forensic specialist to determine whether their site had been accessed. [47]

The interesting fact in this case is that the scraper program developed by the former employees did not require confidential information. If anyone other than the former employees had developed this program it would have been legal since all the information was on web site of EF Cultural Travel BV and fully accessible to anyone. It was considered a CFAA violation because although the information was freely available to anyone accessing the Web site, they successfully argued that only an employee would understand the value of the information he or she had scraped. .[48] A company "can easily spell out explicitly what is forbidden."[49]. Moreover,

---

43 Id

44 E*F Cultural Travel BV v. Explorica, Inc.* (U.S. Court of Appeals for the First Circuit, 2003)

45 Id

46 Id

47 Id

48 Id

49 Id at 63

any use of a Web site that goes against whatever terms the operator of that site has set forth that constitutes a negligence tort is a violation. Only a small percentage of computer hackers are ever caught and prosecuted. The biggest problem is that most victimized companies regrettably choose to hide the problem from the public due in part to negative publicity concerns.

On July 1, 2003, [50]California became the first state to enact a reporting requirement for computer hackings. The CFAA deals not only with hackers, but also with persons who have exceeded the scope of their authorized access. For example, consumers who share their passwords, competitors who use web "spiders" or other bots to gather information on your website, and current or former employees who copy files on your network that are beyond their authorization, all could be liable for exceeding the scope of their access under the CFAA. The CFAA recognizes that a cyber-attack can both damage a business directly as well as cause one to incur substantial costs in responding to the hacking or unauthorized access.

Conclusion

In conclusion, although the original purpose of the Computer Fraud and Abuse Act was limited in its scope to unauthorized access to government and financial institutions' computers, the later addition of Section (g), which authorized civil actions against violators, greatly expanded the scope of the law. Civil cases that have applied the law have centered on employer's suing employees or former employees for unauthorized access to the employer's computing resources. The recent criminal case involving improper usage of a MySpace account that led to a child's suicide has underscored the far-reaching impact of this statute in its current form. In fact, in that case Section (g) may ultimately be used in a wrongful death civil suit.

---

[50] § 1798.82, et. seq. of the California Civil Code

Further possible application of Section (g) may occur when an employee sues an employer in matters such as a sexual harassment case and the employer counterclaims with an action against the employee for computer misuse if there has been any inappropriate use of the employee's computer. Indeed, the full application of this federal statute has yet to be seen.

References

§ 1798.82, et. seq. of the California Civil Code
18 U.S.C. §1030
Nick Ackerman, "CFAA as a Civil Remedy." *National Law Journal*, 2005: 10-12
Edmund Burke, *The Expanding Importance of the Computer Fraud and Ab use Act.*, 2001.

EF Cultural Travel BV v. Explorica, Inc.,274 F.3d 577(1st Cir. 2001)
Sawyer v. Department of Air Force, 31 M.S.P.R. 193, 196 (M.S.P.B. 1986).
Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Washington, 2000)
United States v Czubinski 106 F.3d 1069 (1st Cir. 1997)
United States v Lori Drew, Grand Jury Indictment (Feb 2008)
United States v. Morris United States Court of Appeals, Second Circuit, 1991. 928 F.2d 504
http://www.myspace.com/, retrieved March 1, 2008

Published by the Forum on Public Policy