



Annual ADFSL Conference on Digital Forensics, Security and Law

2009
Proceedings

May 21st, 1:00 PM

The Computer Fraud and Abuse Act and the Law of Unintended Consequences


Milton Luoma

Metropolitan State University, St. Paul, Minnesota, milt.luoma@metrostate.edu

Vicki Luoma

Minnesota State University, vicki.luoma@mnsu.edu

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Luoma, Milton and Luoma, Vicki, "The Computer Fraud and Abuse Act and the Law of Unintended Consequences" (2009). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 6. <https://commons.erau.edu/adfsl/2009/thursday/6>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



The Computer Fraud and Abuse Act and the Law of Unintended Consequences

Milton Luoma

Metropolitan State University
700 East 7th Street
St. Paul, Minnesota 55106
651 793-1481
651 793-1246 fax
Milt.Luoma@metrostate.edu

Vicki Luoma

Minnesota State University
145 Morris Hall
Mankato, Minnesota 56001
507 389-1916
507 389-5420
Vicki.Luoma@mnsu.edu

ABSTRACT

One of the most unanticipated results of the Computer Fraud and Abuse Act arose from the law of unintended consequences. The CFAA was originally enacted in 1984 to protect federal government computers from intrusions and damage caused by hackers, identity thieves, and other cyber criminals. The law was later amended to extend the scope of its application to financial institutions', business's and consumers' computers. To aid in the pursuit of cyber criminals, one of the subsequent revisions to the law included provision "G" that gave the right to private parties to seek compensation for damages in a civil action for unauthorized computer intrusions. This amendment to the law has had the unintended consequence of bolstering, or in some cases supplanting, claims against employees and former employees for claims such as trade secret violations, intellectual property violations, and violations of covenants not to compete. This amendment has also aided employers in their defense of employee claims of sexual harassment, wrongful termination, and other claims by facilitating counterclaims against employees and former employees for computer misuse. This paper examines these developments in the law and likely unintended consequences of the original amendments to the Computer Fraud and Abuse Act.

Keywords: computer, fraud, intellectual property, law

1. INTRODUCTION

In response to a substantial increase in cybercrimes, the United States Congress passed the Computer Fraud and Abuse Act (CFAA) in 1984. The first version of the act dealt with illegal acts performed against government computers and government financial records. As soon as the act was passed it was clear that the law was not adequate to deal with the ever increasing frequency of cybercrimes and the increasing interdependence of computers. (Luoma, 2008) As a result, the act was amended several times and in 1996 the act was changed to include provision "G" that allows civil actions and civil penalties. (Computer Fraud and Abuse Act, 1984)

Section G reads as follows:

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 cases involving 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.” (Computer Fraud and Abuse Act, 1984)

The inclusion of a civil section in a criminal statute is unprecedented in federal criminal statutes, and it can only be assumed that in an effort to combat increased crime, the government was willing to empower civil litigants to fight cybercrime, too. However, the section was not used by any civil litigants until the attorneys in the Shurgard case argued that the CFAA should be applicable to cases in which an employee forwards company information to his new employer by using his company’s computer to send the information over the Internet. (Shurgard v Safeguard)

Warren Rheame and Roanne Spiegel, attorneys representing Shurgard, sued the defendants, former Shurgard employee Eric Leland and his new employer, Safeguard, with a variety of causes of action including violations of the Computer Fraud and Abuse Act. (Luoma, 2008) The defendants moved the court to summarily dismiss the alleged cause of action under the CFAA because defendant-employee Eric Leland had permission to use his company computer so long as he was still an employee of Shurgard. The court ultimately ruled that even though Shurgard gave its employees permission to use company computers, the employee loses computer authorization as soon as the employee’s actions are disloyal. (Shurgard v. Safeguard) Therefore, in the Shurgard case, as soon as Leland sent his new employer proprietary information, copied proprietary data, or did any other disloyal act using the computer, he no longer had the right to use his employer’s computer, and hence, the CFAA provisions were applicable to his misdeeds. (Shurgard v Safeguard)

2. THE IMPORTANCE OF THE SHURGARD CASE

In any cause of action alleging tort, the plaintiff has the burden of proving four points. First, the plaintiff must first prove that the defendant owed a duty to the plaintiff. Second, the plaintiff must establish that a breach of that duty occurred. Third, the plaintiff must show by a preponderance of the evidence that the breach of the duty was the proximate cause, or legal cause, of the damages that flowed from the breach. Finally, the plaintiff has to prove the nature and amount of the damages. (Restatement 2d of Torts) Proof of the existence of a duty is generally straightforward in virtually all tort cases. For some complex torts, proof that the breach of duty was the proximate cause – that the breach of duty was cause in fact and was foreseeable – can be difficult.

In civil litigation against employees or former employees that involves any computer misuse, the CFAA has become the allegation of choice because the only requirement to is to prove, first, that the defendant misused the plaintiff’s computer, and second, that the plaintiff suffered at least \$5,000 in damages. At least one court has held that the hiring of a computer forensics expert to determine whether there have been damages is, in fact, part of the damages. (EF Cultural Travel BV v. Explorica, Inc., 2003) If \$5,000 is spent on forensics experts, then the CFAA applies.

Legal actions under CFAA are beginning to replace or to bolster litigation that involved solely accusations of violations of trade secrets, employee misappropriation of information, restraint of trade, violations of covenants not to compete, and other torts. This portends a trend in litigation where allegations of violations of the CFAA will become routine. One of the primary benefits of including this cause of action in a lawsuit is that it is relatively easy to prove compared to other common causes

of action in business litigation. A brief review of some of these causes of action will illustrate this point.

2.1 Trade Secret Litigation

Trade secrets are business processes not protected under trademarks, patents or copyrights, but are still considered to be an important part of what makes the business unique and successful. (Ellis, 2005) It can include items like customer lists, pricing, marketing plans, business plans, store locations, business floor plans, and secret recipes. (Restatement 2d of Torts) One of the most significant advantages of trade secrets over other forms of intellectual property protection is the fact that the protection is perpetual so long as the secret is kept intact. The right to exclusive use does not expire after some statutory time period. (Restatement 2d of Torts)

There are strict laws against the theft of trade secrets, including the Uniform Trade Secret Act, which has been passed in part by thirty states, and the Economic Espionage Act, which makes it a federal crime to steal trade secrets. However, with all of this legal support the plaintiff must make a prima facie case to the court of each and every element of the cause of action. (Restatement Torts 757)

The difficulty in proving a violation of the trade secret law is that the plaintiff has the legal burden to establish that the information was stolen, that the information in fact was legally protected, and that the plaintiff was damaged. In, *Coco v. A.N. Clark*, the court set the standard that plaintiffs must prove to win a trade secret case as follows:

- the information itself must have the necessary quality of confidence about it;
- that information must have been imparted in circumstances imparting an obligation of confidence;
- there must be an unauthorized use of that information to the detriment of the party communicating it. (*Coco v. A.N. Clark Engineers Ltd, 1969*)

In the Restatement Second of Torts, comment b of the first Restatement lists six factors to be used to determine whether something is a trade secret of a particular person:

- the extent to which the information is known outside of his business;
- the extent to which it is known by employees and others involved in his business;
- the extent of measures taken by him to guard the secrecy of the information;
- the value of the information to him and to his competitors;
- the amount of effort or money expended by him in developing the information;
- the ease or difficulty with which the information could be properly acquired or duplicated by others. (Restatement Second Torts)

In addition, the plaintiff must prove how it was harmed. Harm can be a very difficult element to prove in the court. Attempting to prove these elements can be extremely costly and time consuming. Alternatively, bringing the action under the theory of a violation of the CFAA is much easier to prove – “Has the employee misused the computer use agreement – yes or no?” The only remaining question is how much are the damages?

2.2 Covenants not to Compete

Often employers require employees to sign a “covenant not to compete” as a condition of employment. Yet violations of these covenants not to compete are also difficult to pursue legally because courts often find them to be a restraint of trade and they are reluctant to rule in favor of the plaintiff. In a typical case alleging that defendants violated a company’s covenant not to compete, *Spiegel v. Thomas*, the court found that before the court would consider the covenant enforceable, the court must consider whether there was adequate consideration for the covenant, whether there was a threatened danger to the employer in the absence of the covenant, whether economic hardship would

be imposed on the employee, and whether the covenant is against the public policy. In addition, the employer must prove that the covenants are reasonable in time and geography before the court will uphold these agreements. (*Spiegel v. Thomas, Mann & Smith, P.C.*, 1991) Proving all of these points can represent a very difficult burden for a plaintiff. Even if a plaintiff does have convincing evidence of a breach of the covenant, courts are reluctant to prevent a person from being gainfully employed or limiting competition that violates free market principles. Again, if the employee or former employee can be shown to have violated a computer use policy in some manner, damages can be recovered from the employee.

In another case, *P.C. Yonkers*, the plaintiff, claimed that former employees not only started a competing store within their former employer's sales district but accessed their computers more than one hundred times to gather marketing, sales and other information that they used to compete with the plaintiff's business. Alleging and proving computer misuse was much easier and less costly than the requirements to prove that the plaintiff provided adequate consideration to each of these defendants for the signed covenant not to compete and that the actions of the defendant starting a competing business in their area was a danger to the plaintiff.

In addition, the plaintiff would have to prove explicitly how these actions caused economic loss to the plaintiff. Proof would require more than the plaintiff's revenue decreased. It would require proving specific customers of the plaintiff went to the defendant based on defendants' illegal action to entice them to change companies. If the customers claimed they independently changed suppliers, the plaintiff's case would evaporate.

If the plaintiff chose to pursue the defendant based on trade secret violations the plaintiff would have the burden to prove that the defendant actually established that each business process in question was in fact stolen. The plaintiff would have to prove that each of the alleged stolen trade secrets – floor plan, customer lists, marketing plan or other business process – was in fact legally protected. Defendants could argue that any given process was not unique, was common industry practice, or independently designed. Then, as with the covenant not to compete, trade secret damages must be actually proved. (*P.C. Yonkers v. Celebrations*) Again, courts generally require very convincing evidence in order to find such a violation because to do so operates against free market principles.

2.3 Intellectual Property Litigation

Another action in which litigants explored the use of CFAA occurred in an international intellectual property dispute. Laws and treaties that cover international intellectual property rights and trade secret violations exist, but they carry with them stringent evidence requirements. For example, in *Facebook, Inc. v. Studivz, Ltd.* a German company created a website almost identical to Facebook's Internet social network site. Facebook was created by Mark Zuckerberg, Dustin Moskovitz and Chris Hughes, Harvard Students, as a social network and it quickly developed into a multi-billion dollar business. (*Facebook v Studivz*, 2008) On the Facebook site members and guests are required to click on a button indicating that they have read the "Terms of Use." The Terms of Use agreement states in part that

You understand that the website is available for your personal non-commercial use only. You agree that no materials of any kind submitted through your account will violate or infringe upon the rights of any third party, including copyright, trademark, privacy or other personal rights or contain libelous, defamatory or otherwise unlawful material. (*Facebook, Inc. v Studivz LTD*, 2008)

In fact, Studivz admitted it copied the Facebook site and the only changes made on the Studivz site were to change the language to German and the background color to red. Facebook sued Studivz under CFAA. Facebook argued that anyone who uses or visits the Facebook website must signify that they have read and agreed to be bound by Facebook's "Terms of Use" whether or not they are a

registered member of Facebook. (Facebook, Inc. v Studivz LTD, 2008) This case has not yet been resolved but it shows a movement toward suing under the easier requirements of the CFAA.

The other important aspect of this case is the definition of computer misuse is also expanding. In an earlier case, EF Cultural Travel BV v. Explorica, Inc., former employees of the travel agent used a scraper program to gather data information obtain pricing information from their former employer's travel provider's website. Anyone with a scraper program could have obtained the unprotected information. Further, the website did not require users to agree not to gather the information. (Luoma, 2008) In this case the court found that the defendants violated the CFAA *even though the information gathered could have been gathered legally by any other person in the world other than the employees.* (Emphasis added) The court found that it was a violation for employees because the employees knew how to use the information scraped from the website and use it in competition with their former employer. In addition, the court ruled that a company "can easily spell out explicitly what is forbidden." (E.F. Cultural Travel v. Explorica, 2003)

Companies such as Facebook heed the court's ruling in E.F. Cultural by setting explicit terms of use. Studivz, Ltd creators obtained access to the Facebook site as a guest. The complaint alleged that Studixz creators accessed the Facebook site on servers in California from Germany and from other worldwide locations. This allegation establishes the jurisdiction of the United States court to hear and consider the suit brought by Facebook against the German company. (Facebook v Studixz)

3. DAMAGES

The second requirement for an action under CFFA is that the plaintiff must be able to prove damages sustained in the amount of at least \$5,000. The Computer Fraud and Abuse Act defines 'damage' as "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. Sec 1030 (e)(8). Likewise, the CFAA defines 'loss' as "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 its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. (Ackerman, 2005) The United States ("US") Computer Fraud and Abuse Act (CFAA), 18 U.S.C. Sec 1030 et. seq.,

The proof of damages under the CFFA is not so difficult as proving damages under trade secrets or intellectual property torts. In the E.F. Cultural case found that the cost of hiring a computer forensic expert to prove the defendants had scraped their site was sufficient to meet the damages requirement. Subsequent cases have found that merely hiring a computer forensic expert to find the breach is sufficient to meet the \$5,000 damages requirement even if the breach itself does not meet the \$5000 threshold. (Akerman, 2004)

In Charles Schwab & Co., Inc v. Brian D. Carter, Acorn Advisory Management, Schwab either transferred or terminated all employees in a division of Schwab, Soundview Capital Markets' Investment Analytics Division (IA) by November 1, 2004, for which defendant Carter worked. Carter resigned on October 22, 2004 and began working with Acorn. IA received analytical research from various companies including Acorn. When IA announced it was closing this division, Acorn offered to purchase the company. IA turned down the offer. IA then made job offers to several employees including Carter. IA claims that Acorn induced Carter to copy computer information to Acorn. IA alleged it incurred costs of at least \$5,000 in damages over a year. The court found that the plaintiff's could pursue a CFAA case and this allegation of damages over a year period is sufficient. (Charles Schwab & Co., Inc v Brian D. Carter, Acorn Advisory Management, LLC and Acorn Advisory Capital, L.P., 2005)

However, in 2008 in American Family Mutual Insurance Co. v. Rickman an employee had accessed his former employer's computer without permission and copied files; however, the court found that the employer had to prove damages to the computer system or interruption of a computer service.

(American Family Mutual Insurance Co. v. Rickman) In *Cohen v. Gulfstream Training Academy* the court required the same definition of damages as the American Family Mutual Insurance Case; however, most cases have found a much broader definition of damage. (*Cohen v Gulfstream Training Academy*) In *Creative v. Getloaded LLC* the court found that CFAA does not require the \$5,000 damages to be from a single act. (*Creative v. Getloaded LLC*, 2004) The court ruled that “reaching the damage amount could include conducting a damage assessment, restoring the data, program, system or information or other consequential damages or even upgrading the computer system to prevent future violations.” (*GetLoaded*) Another definition of loss was cited *Four Seasons* where the court determined that damages could also be revenue loss. (*Four Seasons*)

In a 2009, *Kalow & Springnut, LLP v. Commence Corporation* the federal district court in New Jersey found that plaintiff’s allegation that defendant’s software product contained a “time-bomb” causing the software to stop working after a period of time met the CFAA’s standard of intent to cause harm. The defendant argued that the plaintiff’s claim relied on faulty logic “which fails to consider other possible explanations, such as a programming error in the software.” The court turned down the motion for summary judgment using the standard set in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007) that “simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of the necessary element.”

While there does seem to be inconsistent interpretations of what may be included in determining the \$5,000 jurisdictional amount, the trend seems to be with a broader interpretation of that provision.

Use of CFAA as the Basis of a Counterclaim

Perhaps an even more important potential use of the CFAA could be as a counterclaim to a suit brought by an employee. For example, suppose an employee or a former employee brings an action for sexual harassment or wrongful discharge. Rather than being entirely on the defense, the employer could use the CFAA as a counterclaim to the plaintiff’s claim if the employee engaged in any misuse of his or her computer during employment. Misuses of company computers as benign as surfing the Internet or otherwise engaging in personal business during working hours could lead to a claim against the employee. If the misuse involved illegal activities and very serious breaches of company loyalty during employment, the plaintiff-employee may well decide that his or her original claim may not be as strong as originally thought.

Since the federal rules of civil procedure require a litigation hold if the employer has reason to believe that an employee may file a claim in litigation, it is incumbent upon employers to immediately secure and quarantine any computer used by such an employee and then obtain a forensic examination of it. Such an examination will be vital to determining whether the employee engaged in any misuse of that computer during his or her employment. Such an examination will preserve evidence that can be used to substantial advantage in any litigation that may subsequently occur.

4. CONCLUSION

In conclusion, the unanticipated results of the Computer Fraud and Abuse Act arise from the ambiguous nature of the law that only leads to the possibility of future unintended but creative uses of the act. The use of civil remedies of section “G” of CFAA have been a creative and efficient method to bring a private cause of action for misappropriation of confidential information or trade secrets against current and former employees. Even though there is an epidemic of stolen identities, hacked computers and a variety of other cyber crimes, the additional uses of the Computer Fraud and Abuse Act have been positive additional unanticipated uses. Whether employees are aware of this possible application is not as important as the fact that it is a useful addition to the prevention of computer misuse. Employees must comply with computer use policies of their companies and not conduct criminal or other unlawful activities. Future employers of these departing employees must seriously review what information their employees bring with them and where and how they obtained that information. The CFAA continues to be an effective method for employers to stop disloyal employees

from committing tortious acts against the employer's interests. However, with the recent split of authority regarding "unauthorized access," employers are advised to draft clauses into their confidentiality agreements with employees that clearly define what access is authorized and what access is unauthorized, including the precise time when authorized access becomes unauthorized. Finally, it would be appropriate to inform employees of the potential application of the Computer Fraud and Abuse Act in the event of computer misuse.

REFERENCES

- Ackerman, N. (2005). CFAA as a Civil Remedy. *National Journal*, 12.
- Ackerman, N. (2004). CFAA's \$5,000 Threshold. *National Law Journal*, 19-21.
- American Family Mutual Insurance Co. v. Rickman .
- Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007)
- Burke, E. (2001). The Expanding Importance of the Computer Fraud and Abuse Act. *Giglaw*.
- Charles Schwab & Co., Inc v Brian D. Carter, Acorn Advisory Management, LLC and Acorn Advisory capital, L.P., Case No. 04C7071 (United States District Court for the Northern District of Illinois Eastern Division 005 U.S. W. Feb. 11, 2005).
- Coco v. A.N. Clark Engineers Ltd, (1969) R.P.C. 41 at 47
- Computer Fraud and Abuse Act, 18. U.S.C.1030 (Federal 1984).
- Creative v. Getloaded LLC , No. 02-35856 (9th Circuit October 15, 2004).
- Ellis, E. (2005). Trade Secrets. *The Computer and Internet Lawyer*, 7-29.
- Facebook, Inc. v Studivz LTD, 5:2008cv03468 (California 2008).
- Four Seasons Hotels & Resorts BV v. Consorcio Barr, SA, 267 F. Supp.2d 1323-1324 (SD Fla. 2003)
- Heath Cohen v. Gulfstream Training Academy, Inc. and Gulfstream International Airlines, Inc. Case No. 07-60331-Civ-Cohn/Seltzer (S.D. Fla., April 9, 2008)
- In E.F. Cultural Travel BV v. Explorica, Inc. (U.S. Court of Appeals for the First Circuit 2003).
- Kalow & Springnut, LLP v. Commence Corporation No. 07-3442, 2009 WL 44748 (D.N.J. Jan. 6, 2009).
- Luoma, M. & Luoma, V. The Computer Fraud and Abuse Act: An Effective Tool for Prosecuting Criminal and Civil Actions in Cyberspace. *Forum on Public Policy*.(2008)
- Nexans Wires S.A. v. Sark – USA Inc., 319 F. Supp. 2d 468, 469 (Southern District of New York).
- P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore, L.L.C., 2007 U.S. Dist. LEXIS 15216 (D.N.J. 2007)
- Shurgard Storage Centers, Inc. v Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (Washington 2000).
- Spiegel v. Thomas, Mann & Smith, P.C., 811 S.W. 2d 528, 529–30 (Tenn. 1991)
- Uniform Trade Secret Acts Section I(4).

