Revised interpretation of the Computer Fraud and Abuse Act; Implications for Business

Vicki Miller Luoma
Minnesota State University – Mankato

Milton H. Luoma, Jr.
Metropolitan State University

ABSTRACT

The Computer Fraud and Abuse Act, passed in 1984, as amended, originally offered a method for the United States government, and eventually, employers to have recourse against hackers. With each amendment the act broadened both the civil and criminal recourse for employers and criminalized a wide range of unauthorized actions by employees using or misusing employer computer systems. In particular, the Act prohibited unauthorized access to computer systems, defining problematic access as that which occurs "without authorization" or in a manner that "exceeds authorized access." (Computer Fraud and Abuse Act, 2010) The appellate courts interpreting the meaning of those clauses were split into two viewpoints concerning the meaning of the Act's original intention. Those championing the broad interpretation of the language argued that the CFAA "unauthorized access" should focus on purpose of the access and those supporting a narrow approach argued that the relevant inquiry should be whether permission to access existed. Ultimately, the U.S. Supreme Court granted certiorari to resolve the question and to ensure that parties were treated equally regardless of jurisdiction. The decision of the U.S. Supreme Court has left business struggling to protect their business from employee misconduct.

Keywords: Computer Fraud and Abuse Act, Exceeds Authority, Electronic Data, Trade Secrets

INTRODUCTION

Nearly three decades after the Computer Fraud and Abuse act was adopted and after eight amendments and numerous decisions, appellate courts were split in their decisions based on the meaning of the key phrase "exceeds authorized authority." (Kane, 2020) Since legislative amendments continued to expand and broaden the meaning and scope of the Computer Fraud and Abuse Act, businesses believed they had recourse against errant employees. Employers established strong computer use policies based on the Computer Fraud and Abuse Act and prohibited employees from exceeding their permitted computer use. (Jakopenek, 2014) When the Supreme Court granted certiorari in the Van Buren v. United States case, its subsequent ruling resolved the differing interpretations of the law. (Van Buren v United States, 2021) The answer Supreme Court gave by establishing the narrow view of this act has left Employers needing to establish additional internal structural safeguards to protect themselves from internal hackers from obtaining, exceeding, or misusing employer information. To better understand the full implications of this decision, a review of the history of the Computer Fraud and Abuse Act will be enlightening.

History of the Computer Fraud and Abuse Act

The computer Fraud and Abuse Act was first enacted in 1986 as an amendment to an existing Computer Fraud Act of 1984 and as a reaction to increasing computer hacking and other computer crimes. (Computer Fraud Law & Comprehensive Crime Control Act of 1984, 1984). In 1986 the Computer Fraud and Abuse Act was passed to combat more computer hacking and terrorist threats. The law included "prohibiting accessing a computer without authorization" or "in excess of authorization." (Computer Fraud and Abuse Act of 1986). Since 1986 the Computer Fraud and Abuse Act (CFAA) has been amended in 1990, 1996, 2001 and 2008 (Computer Fraud and Abuse Act, 2012) intending to strengthen and to clarify the law. In the 1996 amendments a section G was added to the law which not only provided civil remedies in a criminal statute, but also contained unprecedented language allowing employers and other entities to pursue violators of the act. (Luoma V. L., 2008) Section G of this act read as follows:

> Any person who suffers damage or loss by reason of a violation of this section many 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 these factors as 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 can be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date 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, 1986)

Regardless of what the legislaive intent was in adding Section G giving corporations the right to pursue hackers and other computer criminals, employers did not pursue these remedies. One problem was that the United States government has never had a comprehensive US cyber enforcement strategy. Under the present system the chances of arresting a cybercriminal is less

than 1%. (Mieke Eoyang, 2018) Corporations did not pursue these hackers for a variety of reasons, including the near impossibility of catching the hackers, the high cost of pursuing these criminals, and the short time frame allowed in the pursuit (two years). Further, corporations found it more economically sound to establish better security or purchase hacker insurance. As large as the hacker problem was becoming, the bigger problem for employers was employees.

According to one study 87% of employees take employer data with them when they leave. (Biscom, 2021) In the same survey Biscom found that most employees surveyed felt there was nothing wrong with taking data, especially if it were something they created as part of their employment or if they were terminated. (Biscom, 2021) Employees stealing employer data is a bigger problem for most employers than hacking. (Park, 2000) Employee theft was huge problem Employers were trying to solve when attorneys took another look at the Computer Fraud and Abuse Act using more creative view of the language.

Creative interpretation of the words in section G:

It was nearly a decade after the passage of the law when resourceful attorneys, Warren Rheaume and Roanne Spiegel, saw a potential benefit for employers with disloyal employees under the CFAA. They argued the CFAA language – "exceeds authorization" includes employees who exceeded their authority obtaining employer data and could be charged both civilly and criminally under this act. Rheaume and Spiegel were representing Shurgard Self Storage against Safeguard, a competitor of Shurgard, claiming that Safeguard was systematically hiring key employees away from Shurgard in an attempt to obtain their trade secrets. Shurgard further alleged that some of these key employees, while still working for Shurgard, used Shurgard's computers to send trade secrets to Safeguard and this exceeded their authorization. (Shurgard Storage Centers, Inc, a Washington Corp. v Safeguard Self Storage, a Louisana Corp, 2000) Shurgard claimed that Safeguard's actions were a violation of U.S.C. Sect 1030(a)(2)(c) authorizing "whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby…obtains information from any protected computer involved in interstate of foreign communication… shall be punished. (Computer Fraud and Abuse Act, 1986 as amended 1996).

In addition, Safeguard violated section (G) of the act because "a protected computer" means a computer that is used in interstate or foreign commerce or communication." (Computer Fraud and Abuse Act, 1994) Further, Shurgard claimed the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain information in the computer that accessor is not entitled so to obtain or alter." (Computer Fraud and Abuse Act, 1986). The courts allowed this interpretation of the law and the case went forward eventually finding Safeguard had violated Shurgard's rights under the Computer Fraud and Abuse Act. (Shurgard Storage Centers v Safeguard Self Storage, 2000)

This case opened the floodgates to other employers seeking to pursue employees' wrongdoings with employer's computers. In another early case, a former employee was convicted on the grounds he used a scraper program to obtain information on his former employer's web site. (Luoma V. L., 2009) In a scraper program a robot is used to gather information for a variety of purposes on web sites. In this case, the robot was only scraping data from the former employer and based on that scraping was able to obtain pricing information, specific tour information, schedules and other important data. In total, they were able to download 60,000 lines of information. Strangely, the same information could be "scraped" by

anyone in the public, but because it was former employee he was found in violation. (EF Cultural Travel BV v Explorica, Inc, 2001)

After these early cases opened the floodgates to litigation involving employees exceeding authorization, cases have included trade secrets, financial records, personal information concerning employees, customer information and intellectual property data. Employers have relied on this statute to seek retribution and punishment of errant employees. The sections most relevant to businesses involving this Section (Computer Fraud and Abuse At, 2010) makes it a crime for anyone to "Intentionally access a computer without authorization or exceeds authorized access…on a protected computer. A protected computer includes any computer that has Internet access. (Computer Fraud and Abuse Act, 2010)

Split Circuits

Defense attorneys fought back and argued that the law should be interpreted narrowly and only hackers who never had permission to use an employer's computer should be included in this law. It was not long before the appellate courts split on the meaning of "exceeds authorized access." The United Court of Appeals for the Second, Fourth and Ninth Circuits have taken the position that a person is not guilty/responsible under the principle if you have permission to use a computer or data, but have exceeded your authority, then it is not a violation of the Computer Fraud and Abuse Act, whereas the Eleventh, Fifth and Seventh Circuits have consistently found that a person is responsible if they exceed their permission. Other circuits have had varied in their decisions. (Moye, 2021)

Some circuits espoused a narrow interpretation of the Computer fraud and Abuse Act seeing the statute aimed more to outside hackers. These advocates of a narrower reading argue that the law is ambiguous and fails to define important terms such as "exceeds authority." In one case in the 9th Circuit, an employee emailed data to himself and then used the data to compete with his former employer. The district court decision was upheld by the appellate court found that the employee had permission to access the computer so therefore, he was not in violation of the Computer Fraud and Abuse Act. (Holdings LLC v Brekka, 2009)

One case that illustrates the difference is the Nosal Case (United States v Nosal, 2012) In October of 2004 David Nosal resigned from his job at Korn/Ferry a employe that did executive recruiting. The parties signed a separation agreement that stated Nosal would stay as an independent consultant for one year and agree not to compete with them for a year. They also agreed the employer would pay Nosal 12 payments of $25,000 each. Despite the agreement Nosal recruited three of Korn/Ferry's employees to come work for him to start a competing executive recruiting service. These recruited employees downloaded a large volume of materials from Korn/Ferry's computers including names, source list and contact information of executives. On June 28, 2008 Nosal and three employees were indicted by the federal government on violations of the Computer Fraud and Abuse Act. In 2013 Nosal was convicted. Nosal appealed and argued that the statute was meant for hackers. The appellate court found in a 2-1 decision that Nosal had acted with authorization. (United States v Nosal, 2012)

On October 27, 2011, the Ninth Circuit agreed to rehear the case en banc. The Court interpreted the phrase exceeds authorized access to only restrict access to information and not to the use of information. This further restricted the definition of "exceeds authority." (Harvard Law Review Association, 2013) Although the conviction was upheld the court attempted to narrow the interpretation of "exceeds authorized use." (United States v Nosal, 2012)

Yet in another case, a computer programmer Aleynikov who worked at Goldman Sachs stole proprietary computer source material and transferred it to his new employer. Aleymikov was charged with violations of the Computer Fraud and Abuse Act and other charges. Prior to the trial the judge dismissed the Computer Fraud and Abuse Act claims on the ground that the defendant was authorized to use the computer and therefore the Computer Fraud and Abuse Act was not applicable. (United States v Aleynilov, 2012)(Kane, 2020)

In yet another case, a Social Security employee accessed the employer's computers to find information on his wife, former girlfriend and others. The Social Security Agency had a computer use policy and these actions were in violation of that policy. In this case the 11th Circuit found that the employee was not authorized to obtain personal data for nonbusiness purposes, and he was convicted. . (United States v Rodriguez, 2010)

There are numerous other cases with varying decisions on the issue of misuse of computers. Those circuits that hold the Computer Fraud and Abuse Act should be viewed with a broad perspective argue the unauthorized access should focus on access purpose. Those proponents of the narrower interpretation argue the relevant question is whether the owner had granted the person permission to access the computer and not the reason why the computer was accessed. They further argued that criminalized any user action that was outside of their scope of employment, such as sending email to a friend, making Amazon order or surfing the net. (Villasenor, 2021) These split decisions left employers in a quandary – what do they do with employees who steal valuable data and why should the answer depend on what circuit court had jurisdiction of the case. Defendants were just as confused because they could be convicted in one jurisdiction and not in another.

Supreme Court grants certiorari

In response to the split in circuit opinions, the U.S. Supreme Court granted certiorari on the Van Buren case to finally answer the question of what do the following phrases mean "without authorization and "exceeds authority." (Van Buren v United States, 2021)

Georgia police officer Nathan Van Buren used his patrol car computer to access a law enforcement database to retrieve license plate information in an exchange for money. The Georgia police department had a policy against employees obtaining database information for non-law enforcement purposes. In reality the purchaser of this data was part of an FBI sting operation. Van Buren was charged with a felony violation of the Computer Fraud and Abuse Act under the provision he "intentionally accessed a computer without authorization or exceeds authorized operation." (Computer Fraud and Abuse Act, 1986) Van Buren was convicted, and his conviction was upheld by U.S. Court of Appeals for the Eleventh Circuit. (Van Buren, 2021)

Justice Amy Coney Barrett wrote the majority opinion and delivered it on June 3, 2021. The majority ruled that the Section 1030 is so broadly written that it has been used well beyond its intended purpose of punishing illegal hackers. Justice Barrett stated that if "exceeds access clause criminalizes every violation of a computer use policy, then millions of law-abiding citizens are criminals." Justice Barrett further found since most employe have a policy that electronic devices can only be used for business purposes, then an employee who does something as innocuous as sending a personal email or reading the news on her work computer has violated the Computer Fraud and Abuse Act. The majority held that an individual only "exceeds authorized" access whey they access computers with authorization but then obtain

information including files, databases, folders or other information that are off-limits to them. (Van Buren, 2021)

Van Buren was entitled to obtain the material he obtained, and, in the manner, he obtained it. The court found that although Van Buren's purpose was inappropriate it did not change the textual analysis. The court felt a person either had permission to access the computer or they did not have access. The majority of the justices felt this view of the language in the Computer Fraud and Abuse Act was more consistent with the overall structure of the Computer Fraud and Abuse Act. (Van Buren, 2021)

The Supreme Court also granted certiorari in another case also involving the meaning of exceeding authority to access a computer, certiorari Linkedin v HiQ and the issue of Hiq using a scraping program to access the information from their former employer's web site. (LinkedIn Corp v HiQ Labs, 2021) HiQ scraped data from LinkedIn of publicly available information on a social media site. LinkedIn sent a cease-and-desist order to HIQ which HiQ ignored. The appellate court found that "when a corporate network generally permits public access to its data, a users' accessing that publicly available data will not constitute access without authorization under the CFFA." (LinkedIn Corp v HiQ Labs, 2021) Linkedin argued that it had placed safeguards around its servers using a code based technical measures to block hiQ's bots and scraping activities and also by sending a cease-and-desist letter revoking access to their site. They felt that meant that HiQ was using the site without permission. (LinkedIn Corp v HiQ Labs, 2021) Rather than decide this case, the Supreme Court remanded the case back to the Ninth Circuit for review with the instructions the appellate court should review its decision based on the Supreme Court's Van Buren decision, Linkedin Case. (LinkedIn Corp v HiQ Labs, 2021)

These two cases, Van Buren and Linkedin, involve two different aspects of exceeding authority. Linkedin involved a former employer using a scraping program in the earlier case of EF Cultural Travel case found that a former employee using a scraping program was exceeding their authority. Since the Supreme Court remanded this case it will be up to the Ninth Circuit to determine if HiQ was authorized under the new interpretation set out by the Van Buren Case.

What the Supreme Court left unresolved

The Supreme Court did not resolve the issue whether an information-based policy restricting access would work rather than the current purpose-based access established by the Van Buren case. Does the Computer Fraud and Abuse Act still prohibit policy or use-based restrictions? (Townshend, 2018)

There are three main types of access control systems – discretionary access, role-based access control, and mandatory access control. The Supreme Court did not resolve the issue of whether revoking permission to someone who had access to the site is sufficient or if a different type of access makes a difference.

Further, the Supreme Court did not limit the ability of an employer to go after employees who circumvent their access to hack into restricted data, software or information. Employers simply cannot use the Computer Fraud and Abuse act as the basis of exceeding their agreed upon access, but can if the employees are in-house hackers.

The Supreme Court did not find there was anything inherently wrong with a law designed to punish employees who exceed their permission, but that the present CFAA was too broad, terms too vague, and the present interpretation was not the stated purpose of the law. There is

nothing that prevents Congress from passing a new law that would address these issues and still satisfy the needs of employers with serious breaches by their employees.

What this decision means to employers

The prior interpretation of the law was rather easy recourse for employers. They had to show their computer use policy, the access that was permitted, and that the employee exceeded that authority. Without this law it will be harder to prosecute employees who download and steal un-authorized material.

Employers must be diligent in monitoring their computers, computer users and access allowed. They must be vigilant in finding weak spots in their systems. It is no longer adequate to verbally restrict access limits to your employees. If they can find the data, they are not exceeding the limits of authorized use as defined by the Supreme Court. In addition, Employers must review and strengthen all of their computer policies concerning computer use and limiting non-essential personnel from the ability to access information. They could lobby their congressman for a new law that covers the problem when an employee exceeds their authorization. In short, businesses need to assemble key employees in the organization to determine what changes need to take place now.

15 Steps employers need to do now to prevent data theft:

1. Employers need to have a comprehensive and well written computer use policies. Even if the employer is unable to have an employee charged criminally under the CFAA, there may be other legal remedies that are available, and the employer can still terminate the employee for cause. It is important that the employer explain what exceeding the authority means.

2. Employers must have confidentiality agreements with all employees and review it at time of employees' departure.

3. Employers must have a zero-tolerance policy on computer use and employees that violate this policy must be terminated and prosecuted if appropriate.

4. Employees and managers must be educated on the digital data policy and that the information belongs to the employer. Managers should be trained to reinforce this policy with employees.

5. Employers need to set up a computer security team to review with a computer security expert how to establish an access control system. An access control system can be used to prevent unauthorized access to system resources.

6. Employers need to set stringent technology limits to employees on software, networks, digital data, and other segments of computer access.

7. Employers need to use code-based or technological-based programs to limit an employee's access.

8. Employers need to create data maps to determine what they have, who has access, what is sensitive and what limits need to be put in place. (milt explain data maps)

9. Create a strict policy of only giving access to more sensitive information or trade secrets to those employees that must have access to complete their work.

10. Employers need to review with their in-house counsel all contractual agreements including vendor agreements to determine what information they have given to vendors and if that access is necessary or can it have limits in place.

11. Employers must make a review policy that reviews all data use policies periodically to see what access has been granted and if the access is still necessary.

12. Employers must determine where the employer is vulnerable and take action to hire security experts.

13. The employer must set up a security to review the employer's infrastructure to determine if the employer needs to take additional measures to ensure the safety of its information.

14. The employer must review employer passwords and determine who has access and determine when they need to be changed and monitor access use by employees.

15. Employers must have a system that flags suspicious active on the part of employees who download or delete information unusual amounts of data.

Steps an employer must take with departing employees:

1. Employers must take all of the employees' electronic items including phones, tablets, external hard drives, back up disk and drives, and Employers must keep a chain of custody of all digital devices.

2. Employers must inquire if employees have used their personal electronic devices for work and copy and clear that information per employer policy.

3. Employers must have a system in place to be able to remotely delete, wipe devices if events seem to warrant that action.

4. Employers must send notification of revocation of access to former employees, vendors, customers and others that should no longer have access.

5. Employers must provide extra security around employees who are resigning, terminated or otherwise leaving employment.

6. When an employee, such as salesman, engineers, inventors, officers, leave employment, forensic digital images of their devices should ne obtained before wiping these devices.

7. All departing employees must sign a statement stating they have no data belonging to their employers and that they understand all data created by them as employee belongs to the employer.

8. If an employee leaves na employer without notice, an immediate forensic audit should be conducted to discover the employee's digital trails.

CONCLUSION

In conclusion, the Supreme Court needed to clarify the meaning of the Computer Fraud and Abuse Act statute because of the polar opposite opinions being found by different appellate courts, which meant parties would receive diverse results depending in what part of the country the case was decided. The Supreme Court reviewed the two opposing views – one finding a broad meaning of the term exceeds authority and the other a very narrow view. When the act was created with the that terminology, an outside hacker would have never fit the category of exceeded authority. Who else could exceed authority? This language only fits an employee who was given some authority but did more than allowed. Courts adopting the broad interpretation mainly included employees stealing trade secrets. The majority of the Supreme Court found the terminology in the Computer Fraud and Abuse Act too vague, over broad and beyond the scope of the Act's intended purpose.

The Supreme Court found under the present language and employee could be charged for sending a personal email or surfing the next, although no such case has ever arisen. The majority opinion of this case has to be disappointing to most Employers. Employees who steal data and trade secrets will be harder to prosecute unless Congress decides to clarify or make amendments to the law. At the present time, employers need to take immediate action to set up safeguards to protect their data whether that means changing infrastructure, policy, procedures or security methods. Employers must have a plan to review these policies on a regular basis and be more prepared for Employee misconduct.

Lastly, Congress needs to act to create a law whose purpose is to protect employers from employee theft that is written strictly for this crime and is neither vague nor ambiguous.

Bibliography

Computer Fraud and Abuse Ace, 18 U.S.C. 1030 (1984).
Biscom. (2021, April 16). Departing Employee creates Gaping Security Hole.
Computer Fraud and Abuse Act, Section 1030 (1986).
Computer Fraud and Abuse Act, 18 U.S.C. 1030 (e)(6) (1986).
Computer Fraud and Abuse Act, 18 1030 U.S.C. (1986).
Computer Fraud and Abuse Act, 18 U.S.C. 1020 (a)(2)(c) (United States Congress 1986 as amended 1996).
Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 g (1994).
Computer Fraud and Abuse Act, 18 U.S.C. 1030 (a)(2)(C) (2010).
Computer Fraud and Abuse Act, 18 U.S.C 1030 (2010).
Computer Fraud and Abuse Act, 18 U.S.C. 1030 (2012).
Computer Fraud and Abuse Act of 1986, 100 Stat. 1213 (99 th Congress).
Computer Fraud and Abuse At, 18 U.S.C. 1030 (a)(2)(C) (2010).
Computer Fraud Law & Comprehensive Crime Control Act of 1984, 18 U.S.C. 1030 (1984).
EF Cultural Travel BV v Explorica, Inc, 274 F. 3d 577 (United States Court of Appeal, First Circuit December 17, 2001).
Harvard Law Review Association. (2013). Use of Accessible Information did not violate the CFAA- United States v Nosal 676 F.3d 854 (ith Cir.2022). *Harvard Law Review*, 1454-1461.
Holdings LLC v Brekka, 581 F.3d 1127, 1135 (US Court of Appeals 9th Cir 2009).
Jakopenek, K. (2014). "Obtaining" the Right Result: A Novel Interpretation of the Computer Fraud and Abuse Act that provides liability for insider theft without Overbreadth. *Journal of crminal law and Criminology Northwestern University School of Law*, 606-633.
Kane, S. (2020). Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act. *The University of Chicago Law Review*, 1437-77.
LinkedIn Corp v HiQ Labs, 593 U.S. No 19-116, 593 US (United States Court of Appeal June 14, 2021).
Luoma, V. L. (2008). The Computer Fraud and Abuse Act:An effective tool for prosecuting Criminal and Civil actions in Cyber space. *Oxford Round table Forum*, 32-43.
Luoma, V. L. (2009). The Computer Fraud and Abuse Act and the Law of Unintended Consequences. *Journal of Digital Forensics*, 94-101.
Mieke Eoyang, A. P. (2018, October 29). To Catch a Hacker: Toward a Comprehensive strategy to identify, pursue and punish malicious cybe actors.
Moye, J. M. (2021, July 16). Supreme Court Narrows Scope of Computer Fraud and Abuse Act Van Buren v United States. Atlanta, Georgia.
Park, B. S. (2000). Data Theft by Departing Employees: A bigger threat than Hackers.
Shurgard Storage Centers v Safeguard Self Storage, 119 F.Supp. 2d 1121 (U.S.District Court October 30, 2000).
Shurgard Storage Centers, Inc, a Washington Corp. v Safeguard Self Storage, a Louisana Corp, 119 F. Supp. 2nd 1121 (United States District Court 2000).
Townshend, R. (2018, November 21). Access Control Models. Oahu, Hawaii.
United States v Aleynilov, No11-1126 (United States Court of Appeal 2nd Circuit 2012).
United States v Nosal, 676 F.3d 854 (United States Court of Appeal for the Ninth Circuit 2012).

United States v Nosal, 676 F.3d854 (United States Appellant Court 9th circuit 2012).
United States v Nosal, 676 F3d 854 (United States Court of Appeal 2012).
United States v Rodriguez, 628F.3d 1258 (United States Appellant Court 11th Circuit 2010).
Van Buren v United States, 19-783 (United States Surpeme Court June 3, 2021).
Van Buren v United States, 19-783 (United States Supreme Court July 3, 2021).
Villasenor, J. (2021, June 7). Reining in overly broad Intepretations of the Computer Fraud and Abuse Act. Washington D.C.