MLRC Media Law Resource Center

BULLETIN

2014 Issue No. 2 May 2014

Legal Frontiers in Digital Media

TABLE OF CONTENTS

MEDIA LAW RESOURCE CENTER, INC.
520 Eighth Ave., North Tower, 20 Fl.,
New York, NY 10018

STAFF

Executive Director
Sandra S. Baron
Staff Attorneys
Dave Heller, Michael Norwick
Production Manager
Jacob Wunsch
MLRC Administrator
Debra Danis Seiden
MLRC Fellow
Amaris Elliot-Engel
WSJ-MLRC Institute Free Speech Fellow
Dorianne Van Dyke

THE COMPUTER FRAUD AND ABUSE ACT – UNDERUSED? OVERUSED? MISUSED?

Jeremy D. Mishkin[*]

[*] Jeremy D. Mishkin is a partner with Montgomery, McCracken, Walker & Rhoads, LLP. Co-Chairman of the firm's Litigation Department, his practice focuses on information technology, complex commercial claims and First Amendment/media law. For seven years, he was also the managing partner of the firm. Mr. Mishkin has represented software, hardware and consulting firms, as well as other businesses and individuals, in litigation and alternate dispute resolution proceedings involving privacy, defamation and obscenity issues. He has published articles concerning defamation, e-mail, cybersquatting and privacy on the Web. Mr. Mishkin is co-chair of the Internet Law Committee of the Media Law Resource Center, chair of the editorial board of the Legal Intelligencer and was the Litigation Section member of the ABA E-Commerce and ADR Task Force. He has previously served three terms as chair of the Large Firm Management Committee of the Philadelphia Bar Association, and has been co-chair of the Philadelphia Bar Associations Bar/News Committee and a member of the editorial board of the Pennsylvania Bar Association.

1. Introduction

More of everything moves online every day. Commerce, entertainment, communication, education and even government are part of this migration. Yet the legal standards that govern our online connections were in many cases designed and implemented long ago, and not all have aged well. As a consequence, courts are struggling to apply them under new and novel circumstances. The Computer Fraud and Abuse Act (18 USC § 1030) ("CFAA") is the poster child for laws that are struggling to keep up as technology advances.

Adopted in the 1980's, at least partly in response to a popular movie's depiction of the potential risks from computer hackers making use of then-new technology that allowed remote access by modem (*War Games*, starring Matthew Broderick), the CFAA established both criminal penalties and civil remedies against those who abuse such access. The pertinent criminal law portions of the CFAA provide:

> (a) Whoever—
>
> ****
>
> (4) knowingly and with intent to defraud, **accesses a protected computer without authorization, or exceeds authorized access**, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and **the value of such use is not more than $5,000** in any 1-year period;
>
> *******
>
> (e) As used in this section—
>
> (2) the term "**protected computer**" means a computer—
>
> (B) which is **used in or affecting interstate or foreign commerce** or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
>
> *****
>
> (6) the term "**exceeds authorized access**" means **to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter**;
>
> (8) the term **"damage" means any impairment to the integrity or availability of data**, a program, a system, or information;
>
> (11) the term "**loss**" means **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; and
>
> **********

The parallel civil provision states:

> (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 [so long as the resulting "loss" is "at least $5,000.00 in value."]

For the first few years after the CFAA became effective, it was used primarily in situations involving stereotypical hacking. For instance, *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991) arose when the defendant released "the Morris worm," an early form of malware that spread widely and is thought to have infected many computers, requiring expensive fixes. Once the popularity of web browsers took off after 1995, serious issues starting cropping up about almost every major provision of the law. Because the law has both criminal and civil ramifications, it would be particularly important for its scope and application to be clear, but experience has shown the opposite. This article describes some of the controversies regarding two key provisions of the CFAA, and where the sharpest inconsistencies have arisen.

2. What Is "Authorized" Access?

In *War Games* there was no ambiguity about what Matthew Broderick used his computer for: he hacked into other computers by having his own modem dial telephone numbers and, when it "found" another computer, gaining access by using passwords that he had guessed or somehow obtained. Ally Sheedy asked him "can't you go to jail for this?" to which he presciently replied "only if you're over 18." At the time, he was in the process of trying to access a software company's network (without their permission) so he could play their new computer game (which he had not purchased) when he nearly started World War III. He was clearly not "authorized" to do any of this.

But what did Congress mean when it used that word?

Courts and scholars have been struggling to answer that question, and have come up with widely varying answers. Generally speaking, the variations fall into three types – authorization based on agency law principles; authorization based on contract law principles; and authorization based on technological barriers. (*See* Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes," 78 N.Y.U. L. Rev, 1596 (2003)

a. "Authorization" based on agency law

Under the common law of agency, someone entrusted by a principal to act on her behalf forfeits that status when they breach their duties to act as a faithful representative. Such forfeiture occurs immediately and automatically. Accordingly, while an agent may be authorized to access a principal's computer, if the agent has breached his obligations (even if the principal does not know it yet) then he is no longer authorized and according to some courts, the CFAA can apply. This was the approach taken by the Seventh Circuit in *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), where the defendant was accused of deciding to quit and go into business in competition with his employer, deleting the employer's data (along with his own) from his company-issued laptop before returning it:

> For [agent's] authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit [principal] in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee. *United States v. Galindo*, 871 F.2d 99, 101 (9th Cir. 1989); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp.2d 1121, 1124-25 (W.D. Wash. 2000); *see* Restatement (Second) of Agency §§ 112, 387 (1958).

Because of the defendant's breach of duty of loyalty, the Court held that the employee's actions were 'without authorization' and thus the CFAA claim was allowed to proceed.

b. Authorization based on contract law

The Eleventh Circuit was faced with deciding whether the CFAA was violated when defendant, employed by the Social Security Administration, was found to have accessed personal information dozens (if not hundreds) of times. The SSA had strict policy limits on employees' use of its computer system and specifically prohibited obtaining information without a business reason. In addition to the policy the Agency conducted training sessions, posted notices and displayed a banner on the user's computer's screen every day. There was no dispute that defendant was authorized to use the database as part of his job; the question was whether that authorization – as conditioned by the SSA - precluded his conviction under the CFAA. The Eleventh Circuit had no difficulty finding that his conviction was proper, on what it considered to be a plain reading of the statute:

> The policy of the Administration is that use of databases to obtain personal information is authorized only when done for business reasons. [Defendant] conceded at trial that his access of the victims' personal information was not in furtherance of his duties…and that "he did access things that were unauthorized."

U.S. v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

Similarly, the Fifth Circuit upheld a CFAA prosecution of a bank employee who was authorized to access customer records, but who did so in order to help incur fraudulent charges on the customers' accounts. Defendant was an account manager and funneled account information (along with scanned images of checks) to her relative and others, who proceeded to run up the fraudulent charges. The jury returned guilty verdicts on all counts, but defendant challenged those convictions on the basis that she was, in fact, authorized to access the bank's computer system and thus the CFAA should not apply. The defendant argued that while she may have *used* the information improperly, she did not *access* it without authorization. The Court made short work of the defendant's reasoning:

> ‘authorized access’ or ‘authorization may encompass limits placed on the use of information obtained by permitted access to a computer system and data available on that system….at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime…an employer may ‘authorize’ employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer’s business. An employee would ‘exceed authorized access’ if he or she used that access to obtain or steal information as part of a criminal scheme.

U.S. v. John, 597 F.3d 263 (5th Cir. 2010).

A recent case illustrated how such a contract theory applies in a civil context. Plaintiffs (a financial services company and its Chairman) sued defendants (the Chairman’s personal assistant and her husband, a lawyer representing the company) for an alleged fraudulent scheme to obtain equity interests in three businesses the Chairman controlled. Part of the suit alleged that defendants destroyed computer files (to cover up some purported shenanigans involving falsified documents), in violation of the CFAA.

Defendants moved to dismiss the CFAA claims, asserting that defendants were authorized to access the computer system. The Court disagreed. “But even assuming that [defendant], as [plaintiff’s] junior partner and employee, was authorize to access the files in question, there is no basis in the complaint for supposing that she was authorized to destroy files….Certainly the unauthorized deletion of files alleged here constitutes the ‘alter[ation] [of] information in the computer that the accessor is not entitled so to …alter.” *Schaeffer v. Kessler*, 2013 WL 1155587 (S.D.N.Y.)

Contrast this with the analysis by the court in *Carnegie Strategic Design Engineers, LLC v. Cloherty*, Civil Action No. 13-1112 (W.D. Pa. 2014):

> Here, plaintiff admits that each defendant was permitted to access its computer system and network and was permitted to access the data at issue….Plaintiff does not alleged that defendants “hacked into” a computer or the files that they were not otherwise permitted to access. Rather, the crux of plaintiff’s argument is that…defendants lost the right to access such information when they did so for their own or a third parties[sic] benefit, and to the detriment of plaintiff….The scope of the CFAA does not extend to employees who were authorized to otherwise access the data in question, but did so in bad faith or to the future detriment of his [sic] former employer because this Court interprets the term “authorization” narrowly and finds that it does not extend to the improper use of information validly accessed.

Slip op. pp. 15 – 16. In a similar vein, *see Beta Technology, Inc. v. Meyers*, 2013 WL 5602930 (S.D. Tex.)

c. Authorization based on technological tools

In other circuits, courts have held that the CFAA’s reach is much narrower. Given the CFAA’s criminal penalties, the Fourth and Ninth circuits have attempted to enforce what

Congress intended: to criminalize "hacking," not merely breaching a contract or violating terms of use.

In *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) the fact pattern was similar but the analysis was different.

Employees at one business cooperated with a former-employee's efforts to obtain the employer's confidential information by using their (then-valid) credentials to log in, download and transfer information to the former employee, whom they subsequently joined in a directly competing firm. The inside players were technically "authorized" to access the information at the time they did so, although their soon-to-be-ex employer had policies and contracts in place that clearly prohibited such activities.

The Ninth Circuit refused to apply the CFAA, despite such egregious facts. Out of a concern that an employer's contracts and policies were dangerous to use as triggers for criminality, the Court found that holding otherwise would permit employers "to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law." The Court declined to

> transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they sent email instead.

As another court explained:

> the Ninth Circuit expressed concern over terms of service agreements on internet sites that could change at a moment's notice, making previously legal behavior suddenly criminal through no act of Congress.

Dresser-Rand Co. v. Jones, 957 F.Supp.2d 610 (E.D. Pa. 2013).

Similarly, in *Matot v. CH*, 2013 WL 5431586 (D. Oregon), the plaintiff sought to apply the CFAA to so-called "forged" social media accounts. Plaintiff was a school official who found that someone had created a Facebook profile under his name and likeness – allegedly, students at the school. He claimed that the defendants published false and defamatory statements about him using the false profile, and asserted a claim under the CFAA on the basis that in doing so defendants were acting in contravention of Facebook's Terms of Use, and thus their access of the computer was the equivalent of "hacking" and prohibited under the Act.

The Court noted that the Ninth Circuit's "bright line" rule about access vs. use as in *Brekka* and Nosal arose in the context of an employee/employer dispute, unlike the present case. By contrast,

> defendants' relationship with the social media website was 'forged…from the ground up,' i.e., the defendants, as social media users, never were authorized because they breached the terms of use at the inception of the relationship…this court doubts that even the *Brekka* Court would enforce its 'without authorization' language to the extent

> implicated….strict adherence to *Brekka's* bright-line rule outside of the employment context appears to be in conflict with the underlying legislative purpose.

The court also analyzed the notorious *Lori Drew* case, in which the Ninth Circuit refused to permit the use of the CFAA despite defendant's violations of the applicable Terms of Use. Weighing all of these considerations, the court dismissed the CFAA claims, concluding that

> the rule of lenity precludes application of the CFAA ("access without authorization") to defendant's alleged creation of fake social media profiles in violation of social media websites terms of use.

In *WEC Carolina Energy Solutions LLC v. Miller*, 683 F.3d 199 (4th Cir. 2012) an employee downloaded confidential company information before resigning to go to work for the company's competitor. Some of that information apparently made its way into customer pitches, and the new employer was awarded work that previously had gone to plaintiff. Since the downloads happened before the employee resigned, the case was slightly different from the fact pattern in *IAC v. Citrin*. Yet the plaintiff company had broad policy/contract restrictions in place that the defendant clearly ignored, which in the Eleventh Circuit would likely have been enough to sustain a conviction elsewhere.

But the Fourth Circuit refused to adopt that analysis, recognizing that while employers may be disappointed at losing one weapon against disloyal former employees, the plain meaning of the statute compelled a more limited reading. Parsing the key provisions closely, the *WEC* court determined that accessing a computer "without authorization" is prohibited but "improper use" of data that has been acquired while the downloader was still "authorized" is not. Explaining why it was not persuaded to follow the Seventh Circuit, the *WEC* court stated that a

> cessation of agency theory…would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems….we do not think Congress intended an immediate end to the agency relationship and, moreover, the imposition of criminal penalties for such a frolic.

d. Variations on these themes

The limitations of *Nosal* were tested in *Craigslist Inc. v. 3Taps Inc.*, 2013 WL 1819999 (N.D. Calif. 2013), which involved a dispute between the popular e-classified service and other services that "harvested" (i.e. obtained and re-used) its content. Craigslist is accessible to anyone connected to the web, and everyone is "authorized" to use it. Yet Craigslist also has Terms of Use that impose restrictions, and Craigslist polices its intellectual property rights, including copyright. It claimed that defendants were violating its ToU and sent defendants a cease-and-desist letter advising them that they were no longer authorized to access the "website or services for any reason." Craigslist also took technical steps to prevent defendants from accessing its website. When defendants persisted in their conduct and evaded the technological limitations, litigation ensued, including a claim under the CFAA. In determining how to apply Ninth Circuit precedent, the District Court recognized that *Nosal* rejected contract-based triggers of CFAA claims, and instead limited such claims to "violations of restrictions on access to information, and not restrictions on its use." Craigslist's ToU only restricted "use" and not "access," depending on the user's purpose, and *Nosal's* reasoning might have precluded using the CFAA here.

But despite *Nosal*, the District Court ruled in Craigslist's favor and permitted the CFAA claims to go forward. The court found that because of the technological efforts to block defendants and the cease-and-desist letters' express declaration that defendants were no longer authorized to use the site for any purposes, Craigslist had stated a valid cause of action for "unauthorized" access under the CFAA. When (as seems inevitable) the case gets to the Ninth Circuit for review it will be interesting to see if the Court of Appeals agrees with the interpretation of its ruling in *Nosal*.

Another case that could test these boundaries is (at the time this article is being written) under consideration by the Third Circuit. In *US v. Auerenheimer*, Crim. No. 11-cr-0470 (D.N.J. 2013) defendant was convicted for exploiting a security weakness in the network used for iPad internet access when the product was first released. Defendant and a colleague figured out how to trick the network into providing them with email addresses of iPad users who had registered their new devices. But while the "trick" involved some technological sleight-of-hand, the email addresses were obtained by opening a publicly-accessible URL with a web browser. With the right combination of hardware and software, anyone with internet access could have navigated to the same URL and obtained the same information. Regardless, at the close of his criminal trial, the jury convicted defendant of violating the CFAA. On appeal, (App. No. 13-1816) he argues that the CFAA should not apply since the network computers were accessed via publicly available URL's and thus his acts could not have been legally "unauthorized." And, unlike in *3Taps*, there was no "cease and desist" letter sent to defendant notifying him that he (unlike everyone else in the world) was "unauthorized" to access the publicly-accessible sites. In response, the Government concedes that the network security was flawed and insufficient, but argues that the use of defendant's "tricks" to evade that security is sufficient to uphold the CFAA conviction.

3. What constitutes "damage or loss"?

A private cause of action under the CFAA may be brought by one "who **suffers damage or loss by reason of a violation."** The words "damage" and "loss" may seem self-explanatory and possibly even redundant, but they are themselves defined terms in the law and more than a few would-be private litigants have found their actions dismissed for failure to plead cognizable claims.

In subsection (e)(8) , the Act defines "damage" as harming the computer, or network, or data stored on them – including the impairment of the integrity or availability data. By contrast, the definition of "loss" in subsection (e)(11) focuses on the financial consequences of having been "hacked" – repairing the system or restoring the data, as well as any consequential damages flowing from the unavailability of data. Courts have wrestled with how to apply these terms in real-world contexts.

In *SBS Worldwide, Inc. v. Potts,* Civil No. 13-cv-6557 (N.D. Ill. 2014), defendant was alleged to have accessed plaintiff's network and obtained confidential information that he then sent to his personal account. Yet plaintiff did not claim that it suffered "damage" as a result of lost access to its information, and they would not have succeeded in that effort. "[D]ownloading and emailing trade secrets is not enough to satisfy the damage requirement of the CFAA." *See also Motorola v. Lemko Corp.*, 609 F. Supp.2d 760 (N.D. Ill. 2009). Rather, plaintiff claimed that defendant caused a "loss," consisting of costs relating to assessing the situation as well as steps taken to mitigate it. Unfortunately for plaintiff, however, the court found that it had failed

> to allege any facts connecting its purported loss to an interruption of service, loss of data, or even a suspected loss of service or data. Although SBS attributes certain losses to 'damage assessment and mitigation,' …it is clear from the Complaint that SBS' 'damage assessment' efforts were aimed at determining the scope of information [defendant] emailed to himself…SBS does not allege it ever lost access to any of the information contained in [defendant's] emails, notwithstanding [defendant's] attempt to conceal his conduct by deleting the emails. To be sure, assessing the extent of information illegally copied by an employee is a prudent business decision. But the cost of such an investigation is not 'reasonably incurred in responding to an alleged CFAA offense,' because the disclosure of trade secrets, unlike destruction of data, is not a CFAA offense.

Other courts disagree, even ones that apply a "narrow" interpretation of the "authorization" element.

> The term 'loss' under the CFAA is defined as 'any reasonable cost to any victim…." [and] district court decisions in the Third Circuit have held that to fall within this definition of 'loss,' the alleged 'loss' must be related to the impairment or damage to a computer or computer system. *Brooks v. AM Resorts, LLC*, 954 F.Supp.2d 331 (E.D. Pa. 2013) (quoting *Sealord Holdings, Inc. v. Radler,* 2012 WL 707075 (E.D. Pa. 2012). Therefore, loss under the CFAA is compensable if 'the cost of remedial measures taken to investigate **or** repair the damage to the computer, or loss is the amount of lost revenue resulting from the plaintiff's inability to utilize the computer while it was inoperable because of a defendant's misfeasance. *Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio,* 2011 WL 6088611 (E.D. Pa. 2011)

4. Conclusion

It should not be a surprise that courts in the twenty-first century are having difficulty in consistently applying the language of a statute dealing with technology that was passed in the 1980's. Yet because the gaps between the circuits are widening, defendants' innocence or conviction can depend in part on where a civil or criminal case is brought. It is likely that the Supreme Court will need to step in sooner rather than later to resolve these issues.