DISLOYAL COMPUTER USE AND THE COMPUTER FRAUD AND ABUSE ACT: NARROWING THE SCOPE

GREG POLLARO[1]

ABSTRACT

Congress drafted the Computer Fraud and Abuse Act (CFAA) to protect government interest computers from malicious attacks by hackers. As computer use has expanded in the years since its enactment, the CFAA has similarly expanded to cover a number of computer-related activities. This iBrief discusses the extension of the CFAA into the employer/employee context, suggests that this goes beyond the Act's express purpose, compares the different approaches taken by the circuit courts in applying the CFAA to disloyal computer use by employees, and argues that the more recent approach taken by the Ninth Circuit provides a better model for determining if and when the CFAA should apply to employees.

INTRODUCTION

¶1 Disgruntled employees beware. Those who exit their former employment with photocopies of client lists or company financial information have traditionally been susceptible to breach of contract, fiduciary duty, and trade secrets suits in state court. More recently, those who use a computer to email or otherwise obtain digital copies of such information have found themselves susceptible to civil, and possibly criminal, sanctions in federal court under the Computer Fraud and Abuse Act (CFAA). Initially crafted in the 1980s to impede remote computer hacking, the CFAA opened the door to the federal courts for plaintiffs seeking an easier path to combat employee misconduct based on an employee's "unauthorized access" to a company computer.

¶2 The Seventh Circuit in *International Airport Centers, L.L.C. v. Citrin* held that access is unauthorized for the purposes of the CFAA when an employee decides to act contrary to his employer's interest.[2] Applying principles of agency law, the court waded into muddy waters by allowing the mental state of the employee to determine authorization. However, a recent opinion from the Ninth Circuit in *LVRC Holdings, L.L.C. v. Brekka*[3]

---

[1] J.D. candidate at Duke University School of Law, Class of 2011; B.A. Journalism 2005, Northern Kentucky University.

[2] 440 F. 3d 418, 420-21 (2006).

[3] 2009 U.S. App. LEXIS 20439 (9th Cir. Sept. 15, 2009).

rejected the Seventh Circuit's approach and held that authorization is granted by the employer and, therefore, that authorization ends when the employer rescinds it.[4] This split in authority raises questions about how broadly or narrowly the CFAA should be applied—or whether it should be applied at all—in the context of an employee's disloyal computer use.

¶3 This iBrief explores the evolution of litigation under the CFAA to include actions by employers against employees who use a computer to misappropriate, misuse or damage information belonging to the employer. Part I discusses the creation and subsequent amendment of the CFAA from a narrow tool for protecting federal interests against new crimes unique to computer use to a broad method for bringing traditional state law claims into federal court. Part II analyzes the split in authority between the Seventh Circuit and the Ninth Circuit regarding what constitutes authorized access in the context of the CFAA. Part III concludes that the CFAA was not designed to apply to employer/employee claims that are traditionally handled under state tort and contract law. Consequently, courts faced with similar suits should allow CFAA suits to proceed only when the computer use was integral, rather than incidental, to the underlying claim. In the alternative, courts should follow the Ninth Circuit's reasoning in *Brekka* and narrowly apply the CFAA to those situations in which authorized computer access has not been granted or has been rescinded by the employer.

I. COMPUTER FRAUD AND ABUSE ACT: EXPANDING THE NET

¶4 The 1983 film *War Games* starred Matthew Broderick as a computer whiz kid who unwittingly uses his home computer to hack into NORAD's computer system. Broderick's chicanery brought the United States to the brink of nuclear war with the Soviet Union.[5] *War Games* introduced much of the country to the "hacker," and its influence was not lost on members of Congress, who already were trying to decide what to do about traditional property laws that were ill-equipped to deal with network trespassers and intangible property that "may exist only in the form of magnetic impulses."[6] Recognizing that many states already had their own computer crime laws, Congress stepped in gingerly with the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (1984 Act).[7]

¶5 The 1984 Act proscribed three specific types of activity:

---

[4] *Id.* at *15.
[5] WAR GAMES (Metro-Goldwyn-Mayer 1983).
[6] H.R. REP. NO. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695. "The motion picture *War Games* showed a realistic representation of the automatic dialing and access capabilities of the personal computer." *Id.* at 3696.
[7] Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 459 (1990).

- knowingly accessing a computer without authorization or exceeding authorization to obtain classified information with intent or belief that such information would be used to harm the United States;
- knowingly accessing a computer without authorization or exceeding authorization to obtain financial or credit records from a financial institution; and
- knowingly accessing a computer used by or on behalf of the United States if such access interferes with the government's use of the computer.[8]

¶6 Penalties included fines and imprisonment for up to ten years for first offenses, twenty years for repeat offenses.[9] Operating with little data illuminating the nature and extent of the problem posed by computer crime at the time, "the 1984 Act essentially was a shot in the dark."[10]

¶7 Responding to criticisms and calls from the Department of Justice to clarify and greatly expand the 1984 Act to cover a wider range of activities, Congress adopted the Computer Fraud and Abuse Act of 1986 (1986 Act).[11] Rather than create a broad preemptive statute, as some critics suggested, legislators exercised caution and showed their continued commitment to allow states to implement their own computer crime laws:

> The Committee . . . prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature. The Committee is convinced that this approach strikes the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses.[12]

The 1986 Act expanded the number of proscribed acts to include use of a computer to steal property in an attempt to defraud; use of a computer to intentionally alter or damage data in a federal interest computer; and the trafficking of computer passwords.[13]

---

[8] *Id.* at 460.
[9] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98
Stat. 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (2008))
[10] Griffith, *supra* note 7, at 483.
[11] *Id.* at 473.
[12] S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.
[13] U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES, at 2 (2007), *available at* http://www.usdoj.gov/criminal/cybercrime/ccmanual/.

¶8 Subsequent amendments followed in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008 as Congress attempted to keep pace with changes in computer technology and use.[14] Most notable among these are the 1994 and 1996 amendments. In 1994, Congress added a private cause of action[15] that would ultimately open the door to the types of employer/employee disputes discussed below. In 1996, the phrase "federal interest computer" was replaced with "protected computer."[16] "Protected computer" is defined as one that is used by the United States Government or a financial institution; or one that is used in interstate commerce or communication.[17] These amendments, in particular, broadened the scope of the CFAA far beyond its original intent, and much of the careful consideration and debate undertaken a decade earlier about the proper role of the federal government was absent.[18] The inclusion of all computers used in interstate communication had a profound effect, intentionally or otherwise, as any computer connected to the Internet could be considered a "protected computer" under the CFAA.[19]

¶9 The seven types of activity covered by the current CFAA can be summarized as follows:

1. obtaining national security information;
2. compromising the confidentiality of a computer;
3. trespassing in a Government computer;
4. accessing a computer to defraud and obtain value;
5. transmission or access that causes damage;
6. trafficking in passwords; and
7. extortion involving threats to damage computer[20]

---

[14] *See id.* at 2.
[15] H.R. REP. NO. 103-711, at sec. 290001 (1994) (Conf. Rep.), *as reprinted in* 1994 U.S.C.C.A.N. 1839.
[16] S. REP. NO. 104-357, at 10 (1996).
[17] 18 U.S.C. § 1030(e)(2) (2006).
[18] *See* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 914-15 (2003).
[19] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000) ("[T]he original version of the CFAA did not intend to enact sweeping federal jurisdiction. However, 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.").
[20] Prosecuting Computer Crimes, *supra* note 13, at 2.

Operating "without authorization" or "exceeding authorized access" is a key element in the first five offenses.[21] "Exceeding authorized access" is defined as "access[ing] a computer with authorization and us[ing] such access to obtain or alter information in the computer that the accesser is not entitle so to obtain or alter."[22] "Without authorization" is not defined in the text of the statute, and this, in conjunction with the "protected computer" language, has led to a series of civil suits in which courts have wrestled with how to define "without authorization."[23] In a larger context, this is a question of how broadly the CFAA should be applied.

¶10 Congress decided early in the CFAA's history that it wanted a single statute to cover the field of computer crime "rather than identifying and amending every potentially applicable statute affected by advances in computer technology."[24] The price for this legislative expediency is that one relatively brief statute is applied to a range of disparate activities such as fraud, trespass, spam, phishing, worms, viruses and denial of service attacks.[25] This has inevitably forced square pegs into round holes. One area in which the courts' struggles have been particularly noticeable is in civil suits brought by employers against former employees who are accused of misappropriating or misusing information while they were still employed.[26]

II. EMPLOYEE MISCONDUCT UNDER THE CFAA

¶11 An employee, having decided to leave her current employer for greener pastures, emails confidential files from her work computer to her personal email account. She then leaves her job to join a competitor and discloses the confidential information to her new employer.[27] Undoubtedly her actions were wrong and could subject her to a number of claims under state law such as tortious interference and misappropriation of trade

---

[21] 18 U.S.C. § 1030(a).
[22] *Id.* § 1030(e)(6).
[23] *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008) (holding that computer access is "without authorization" only when initial access is not permitted).
[24] S. REP. NO. 104-357, at 5 (1996).
[25] *See, e.g.*, America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E. D. Va. 1998) (holding that defendants violated the CFAA by using AOL access to send bulk emails to AOL members).
[26] *See, e.g.*, US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189 (D. Kan. 2009) (granting defendants' motion to dismiss CFAA claim because access to confidential information was authorized during the term of employment).
[27] *See id.*

secrets,[28] but do they run afoul of the CFAA? Assuming the plaintiff can show damage or loss of the statutory minimum $5,000,[29] the answer turns on how the court defines "without authorization." There is a split of authority between the Seventh Circuit and the Ninth Circuit, the only appellate courts to have ruled on this issue. The Seventh Circuit held that the above facts presented a valid CFAA claim, while the Ninth Circuit held the opposite. The core difference between these two rulings was the circuits' interpretation of the phrase "without authorization."

A. International Airport Centers v. Citrin*: Authorization and Agency*

¶12 In 2006, the Seventh Circuit was the first appellate court to wade into the "without authorization" debate that had been ongoing among the district courts for more than five years.[30] In *International Airport Centers, L.L.C. v. Citrin*, the defendant, was employed by the plaintiff to look for and help acquire real estate.[31] Citrin decided to quit working for International Airport Centers (IAC) and start his own business.[32] Prior to leaving IAC, Citrin erased all the data on a laptop computer provided by IAC, some of which would have shown he had engaged in improper conduct and none of which IAC had any additional copies.[33] Citrin installed and used a secure-erase program to do this, which meant that the data were truly unrecoverable.[34] IAC sued under the CFAA's civil provision, § 1030(g), claiming Citrin had violated § 1030(a)(5)(A)(i), which provides that such violation occurs when one "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[35]

¶13 The court, citing congressional intent that the CFAA should reach internal as well as external actors, readily settled on a broad definition of what constitutes a transmission.[36] While not quite holding that pressing the delete key constitutes a transmission, the court nevertheless determined that installing the secure-erase program—whether installed remotely or by an

---

[28] *See id.* (denying defendants' motion to dismiss trade secrets and tortious interference claims).
[29] 18 U.S.C. §1030(c)(4)(i)(I) (2006).
[30] *See, e.g.*, Shurgard, *supra* note 19 (applying agency law to determine that defendant's authorization ended when he chose to act contrary to employer's interests).
[31] 440 F. 3d 418, 419 (7th Cir. 2006).
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] 18 U.S.C. § 1030(a)(5)(A) (2006).
[36] *See Citrin*, 440 F. 3d 418, at 419-20.

actor with direct physical access—constituted a transmission in accordance with the CFAA.[37]

¶14 The court next turned to the authorization element of § 1030(a)(5). Here, the court applied principles of agency law and determined that Citrin's authorization to access the laptop computer ended at the moment he violated his employment contract by deciding to act contrary to IAC's interests, i.e., before he erased the data on the computer's hard drive.[38] That authorization, the court said, was granted through the agency relationship Citrin had with his employer and implicitly ended when he violated his duty of loyalty to that employer.[39]

¶15 This application of agency law to the CFAA was not a novel concept, as it mirrored an earlier district court decision in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*[40] There, a rival storage company hired some of plaintiff's employees, who, before leaving their old positions, emailed confidential information about their former employer's business.[41] Shurgard sued, claiming three CFAA violations.[42] The defendants, seeking a dismissal for failure to state a claim, argued that CFAA provisions requiring that they act without authorization did not apply because they were, in the scope of their employment with plaintiff, authorized to access the information that they passed to their future employer.[43] Plaintiff raised the agency argument based on § 112 of the Restatement (Second) of Agency:

> Unless otherwise agreed, the authority of an agent terminates if without knowledge of the principal, he acquires adverse interest or if he is otherwise guilty of a serious breach of loyalty to the principal.[44]

The court accepted the plaintiff's agency argument and denied the defendant's 12(b)(6) motion.[45]

---

[37] *See id.* at 419. It should be noted that some computer operating systems, such as the widely-popular Mac OS X, contain their own secure-erase functions. Using the court's logic, then, someone who installs such an operating system and uses it to erase data on the computer without authorization could be guilty of violating the CFAA. Dan E. Lawrence, *Just Add Plaintiff: The Seventh Circuit's Recipe for Instant Liability Under the Computer Fraud and Abuse Act*, 46 WASHBURN L.J. 223, 240 (2006).

[38] *Citrin*, 440 F. 3d at 420-21.

[39] *Id.*; *see also* RESTATEMENT (SECOND) OF AGENCY § 112 (1958).

[40] 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[41] *Id.* at 1123.

[42] *Id.*

[43] *Id.* at 1124.

[44] *Id.* at 1125 (quoting RESTATEMENT (SECOND) OF AGENCY).

[45] *Shurgard*, 119 F. Supp. 2d at 1125.

¶16 Inherent in both *Citrin* and *Shurgard* is the policy judgment made by each court that these kinds of employer–employee claims should, or at least can, be handled under the CFAA. Interestingly, the Seventh Circuit did not spend much time discussing the law's legislative history other than to make conclusory remarks regarding Congress's concern with protecting against direct, internal attacks as well as external attacks.[46] The defendants in *Shurgard*, however, directly raised the policy question, and the court discussed at some length the language it finds in the legislative history supporting a narrow, and conversely, a broad interpretation of the intent behind the CFAA.[47] The court ultimately found language in the record that convinced it that the CFAA, at least since the time of the 1996 amendment, was meant to cover the present facts.[48]

> [I]ndividuals who intentionally break into, *or abuse their authority to use*, a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for *purposes of commercial advantage* or private financial gain, for the *purposes of committing any criminal or tortious act in violation* . . . of the laws of the United States or of any state, or if the value of the information obtained exceeds $5,000.[49]

The *Shurgard* court ultimately found the statutory language to be unambiguous and confirmed its conclusion through a review of the legislative history.[50]

B. LVRC Holdings LLC v. Brekka: Active Authorization

¶17 The CFAA authorization issue resurfaced at the appellate level in 2009, this time in the Ninth Circuit in *LVRC Holdings LLC v. Brekka*.[51] Brekka was hired by LVRC to oversee Internet marketing for its residential treatment facility. At the time, Brekka owned and operated two consulting companies that referred potential clients to rehabilitation facilities. Brekka was given administrative access to information related to LVRC's business including a financial statement and patient admission reports. Brekka emailed some of these documents and others he created for his work at LVRC to his personal computer. When ownership negotiations between Brekka and LVRC broke down, Brekka left the company, which

---

[46] *Citrin*, 440 F. 3d 418, at 420.
[47] *See Shurgard*, 119 F. Supp. 2d at 1127-28.
[48] *Id.* at 1128.
[49] *Id.* at 1128-29 (quoting S. REP. NO. 104-357, at 7-8 (1996)).
[50] *Id.* at 1129.
[51] 581 F. 3d 1127 (9th Cir. 2009).

subsequently sued, claiming that Brekka violated the CFAA when he emailed company records to further his own interests.[52]

¶18 LVRC argued the agency theory of authorization endorsed in *Citrin* by saying Brekka's authorization to access the confidential files ended when he began acting contrary to LVRC's interests.[53] The court held that the text of the CFAA provided no definition of "authorization," so the court turned next to its common usage. "[I]t is a fundamental canon of statutory construction . . . that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning."[54] For this, the court turned to a straightforward dictionary definition of "authorization" as "permission or power *granted by an authority*."[55] The court found no language in the CFAA that either contradicted this straightforward definition or supported LVRC's agency-based definition.[56] The former definition can be understood as active authorization, while the latter might be considered passive authorization. Active authorization is granted by one to another and ends when and where the authority chooses. In the present case, then, Brekka's authorization persisted until LVRC terminated his employment or revoked his permission to access the company's files.[57] Passive authorization, in contrast, is received and disappears when the authorized person has a change in purpose, e.g., when one chooses to act contrary to the authority's interest. The *Brekka* court expressly rejected *Citrin* and this latter definition in the CFAA context because it would lead to less clarity and notice to potential offenders, particularly when the conduct is subject to criminal penalties.[58] "The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants."[59]

¶19 Consequently, the court held that the CFAA is not applicable to factual situations such as these, where authorization to access the information in question was clearly granted and not clearly revoked.[60] Instead, it implied that the provisions of the statute containing the authorization element should be applied to a narrower range of cases "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any

---

[52] *Id.* at 1129-30.
[53] *See id.* at 1132.
[54] *Id.* (quoting Perrin v. United States, 444 U.S. 37, 42 (1979)).
[55] *Id.* at 1133 (quoting RANDOM HOUSE UNABRIDGED DICTIONARY 139 (2001) (emphasis added).
[56] *Id.* at 1133.
[57] *See id.* at 1135.
[58] *Id.* at 1134-35.
[59] *Id.*
[60] *Id.* at 1135.

permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway."[61]

III. RESTORING SOME BALANCE

¶20 Whether the Supreme Court ultimately determines how to define "authorization" under the CFAA or Congress undertakes this on its own, the implications of the ultimate decision will be far reaching.

¶21 A broad definition as in *Shurgard* and *Citrin* opens the federal courthouse to a number of scenarios not intended by the legislators who crafted the CFAA.[62] Plaintiffs would like to have this choice of venue open to them because it provides them with strategic advantages, such as a shorter wait for a trial date and less limitations on discovery.[63] Additionally, supplemental jurisdiction would allow plaintiffs to have any purely state law claims attached to the facts of their CFAA claim to be tried in federal court.

¶22 While allowing access to federal court in these kinds of cases is not problematic per se, two additional considerations weigh against adopting the *Citrin* view. First, there is the issue of clarity and notice raised by the court in *Brekka*. Under the broad, agency definition, employees could be subject to penalties under the CFAA if their employers can claim that their authorization was revoked because they did something believed to be contrary to the employers' interests. Second, scenarios exist in which the *Citrin* definition lowers the evidentiary bar for plaintiffs. Trade secret litigation is one example, where the traditional burden of showing that the information provides a competitive advantage and was kept in secrecy is nonexistent in the CFAA, and plaintiffs must show only that the information was taken from a protected computer and that they suffered the requisite damage or loss.[64] It is difficult to imagine that Congress intended the CFAA to short-circuit state law in this way.

¶23 A narrow definition, on the other hand, has the dual benefit of providing a clearer standard and being in accord with the initial spirit and purpose of the CFAA. While it would preclude cases such as *Shurgard*, *Citrin*, and *Brekka* from getting into federal court, each would be able to proceed under various state law claims. For scenarios in which the use of a computer is incidental, rather than integral, to the offense it would seem that

---

[61] *See id.* at 1135.
[62] *See, e.g.*, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (overturning a lower court CFAA conviction based on violations of a website terms of service agreement).
[63] Stephen R. Buckingham, *Court Gives New Use to 1994 Law: Trade Secrets*, NAT'L L.J., Feb. 5, 2001.
[64] *Id.*

requiring such claims to go forward in state court is in accordance with finding "the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses."[65]

CONCLUSION

¶24 The CFAA has broken free of its moorings as a criminal statute primarily aimed at penalizing the malicious computer hacking of government interest computers. The definition of a computer protected under the Act dramatically expanded to include any computer used in interstate commerce or communication, i.e., any computer connected to the Internet. Opportunistic plaintiffs have until recently found the federal courts amenable to its use in civil suits against disloyal employees. The Supreme Court ultimately may determine whether *Brekka* marks a return to a more limited application of the CFAA in line with its original purpose. In the interim, *Brekka* at a minimum provides a clearer, more workable standard by which to determine the Act's applicability to the employer–employee context.

[65] S. REP. NO. 99-432, *supra* note 9, at 4.