Washington Journal of Law, Technology & Arts

Volume 6 | Issue 4 Article 4

4-1-2011

Gimme a Brekka!: Deciphering "Authorization" under the CFAA and How Employers Can Protect Their Data

Amber L. Leaders

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 4 SPRING 2011

GIMME A BREKKA!: DECIPHERING "AUTHORIZATION" UNDER THE CFAA AND HOW EMPLOYERS CAN PROTECT THEIR DATA

Amber L. Leaders[*]

Cite as: 6 Wash J.L. Tech. & Arts 285 (2011)
http://hdl.handle.net/1773.1/1036

ABSTRACT

Federal circuit courts offer conflicting interpretations of when an employee violates the Computer Fraud and Abuse Act (CFAA) by accessing an employer's computer system without authorization. Enacted originally as an anti-hacker statute, the language of the CFAA proves ambiguous when courts attempt to apply its sanctions to individuals given access to a computer (such as an employee by an employer). Circuit Courts have interpreted the statute differently, generally applying one of two theories to reach their interpretations: (1) agency theory; or (2) looking to the plain language of the statute and the rule of lenity. These differing interpretations have resulted in varying outcomes when employers seek to sanction employees for violating the Act. Employers face tough questions about when and how to seek sanctions when employees potentially violate their rights of computer access. This Article takes an in-depth look at the varying interpretations among the circuits and considers a number of district court cases and their application of the CFAA.

---

[*] Amber L. Leaders, University of Washington School of Law, Class of 2011. Thank you to my student editor, Jeff Doty, for his enduring patience and thoughtful critiques and to my faculty advisor, Anita Ramasastry, for her valuable feedback and guidance.

TABLE OF CONTENTS

INTRODUCTION

The Computer Fraud and Abuse Act (CFAA)[1] both criminalizes unauthorized access to certain private computer systems and allows parties harmed by such access to bring civil actions for compensatory damages and injunctive relief. With the growing use of computers by employees at all levels, however, companies increasingly face the loss of sensitive data through internal acts – violations by their own workers. The language of the CFAA is ambiguous about whether the Act should apply to these internal violators. Thus, federal circuits have split on what it means to be without or to exceed authorized access under the CFAA.

The principle interpretations come from the U.S. Courts of Appeals for the Seventh and the Ninth Circuits.[2] In *International Airport Centers L.L.C. v. Citrin*,[3] the Seventh Circuit used agency law to determine when authorization by an employee begins and ends; under this interpretation, an employee violates the CFAA when the agency relationship is severed and thus authorization is constructively rescinded. In contrast, the Ninth Circuit in *LVRC Holdings LLC v. Brekka*[4] interpreted the statute according to its plain language to determine when an employee lacks authorization. The

---

[1] 18 U.S.C. § 1030.

[2] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); LVRC Holdings LLC, v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

[3] *Citrin*, 440 F.3d at 423.

[4] *Brekka*, 581 F.3d at 1134.

Ninth Circuit finds a violation of the CFAA only when no authorization has ever been given or when authorization has affirmatively been rescinded by an employer.[5] For any employer seeking damages or injunctive relief against a rogue employee, it will be important to consider the branches of interpretation as well as the many offshoots in each of the district courts. This Article examines the *Citrin* and *Brekka* decisions and considers cases from the district courts to determine how these varying analyses affect employers faced with the threat of computer-system breaches.

I. THE ORIGIN AND PURPOSE OF THE CFAA

The difficulty in interpretation of the CFAA arises from the origin of the statute. Enacted in 1984 to help the federal government prosecute computer crimes, Congress designed the CFAA to target hackers who "break in" to systems.[6] But the CFAA has grown from protecting only "federal interest computers" to guarding any "protected computer."[7] Further, the original incarnation was solely a criminal statute, but the scope of the CFAA has gradually expanded through legislative enhancements to include a private right of action.[8] That private action allows an individual to seek civil remedies when he or she has suffered loss or damages as a result of someone else's improper access.

Section 1030 prohibits five categories of conduct: (1) theft of computer data; (2) unauthorized access with intent to defraud;

---

[5] *Brekka*, 581 F.3d at 1135.

[6] Fishman and McKenna, Wiretapping and Eavesdropping §26:1(2010); *see also* Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 820 (2009).

[7] A "protected computer" is any computer "which is used in interstate or foreign commerce or communication." 18 U.S.C. §1030(e)(2)(B) (West 2008). This broad definition encompasses nearly every computer since any connection to the internet satisfies this requirement; *see* Daniel J. Winters & John F. Costello, Jr., *The Computer Fraud and Abuse Act: A new weapon in the trade secrets litigation arena*, INTELLECTUAL PROPERTY, Vol. 44, No. 3 (April 2005), *available at* http://www.jenner.com/files/tbl_s20Publications%5CRelatedDocumentsPDFs1252%5C1002%5CISBA_IP_article.pdf.

[8] Winters & Costello, supra note 5.

(3) unauthorized access resulting in destruction; (4) trafficking in computer passwords; and (5) extortion by threat of damage to a computer.[9] All but the fifth category contain the qualifying language "without authorization" or "exceeds authorized access." These two phrases are the root of the dispute between the various circuits.

The CFAA states in relevant part that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information contained in a financial record of a financial institution, or of a card issuer … or contained in a file of a consumer reporting agency on a consumer" commits a federal crime.[10] Courts employ different methods in applying the language of "without authorization" or "exceeds authorized access" to a computer.

Because the original purpose of the CFAA was to keep third parties from illegally accessing others' computers and information, the language regarding authorization can be unclear when applied to an employee who has been given a degree of authorization by the employer. Courts have struggled to apply this anti-hacker statute when the offender is not a third party but someone who has been given access to the computer, such as an employee.

II. THE SPLIT BETWEEN *CITRIN* AND *BREKKA*

The circuit split centers on when employees have authorization to access computer systems. The Seventh Circuit uses agency law to define the boundaries of authorization. In *Citrin,* it held that when an employee violates his or her fiduciary duty of loyalty to the employer, all access authorization ceases.[11] The Ninth Circuit recently offered an alternative interpretation of the same statutory language.[12] Using the "plain language" of the CFAA, that court determined that the CFAA has narrower parameters for what constitutes a violation.[13] District courts have varied in their application of the two interpretations, with most following the Ninth Circuit's reasoning.

---

[9] *Id.*

[10] 18 U.S.C. § 1030(a)(2).

[11] Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).

[12] LVRC Holdings LLC, v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

[13] *Id*.

A. The Seventh Circuit and Agency Law

In *Citrin*, the Seventh Circuit applied agency theory to interpret the vague language regarding authorization in the CFAA.[14] Citrin was an employee of International Airport Centers (IAC), which loaned Citrin a laptop for work. He decided to go into business for himself, in breach of an employment contract.[15] Before departing, Citrin deleted numerous files that implicated his intent to develop a competing business using IAC's data from his loaned laptop. Beyond deleting the files, Citrin utilized a special program designed to overwrite deleted files, thus making them unrecoverable. He had been given access by IAC to the computer and to the files. IAC alleged the deleted files implicated Citrin and that was why they were deleted. The company sought civil remedies against Citrin under the CFAA for accessing data without authorization and for wrongfully transmitting information.[16]

The *Citrin* court held that an employee's authorization to access a computer ends for purposes of the CFAA when the employee violates her duty of loyalty to the employer.[17] Under agency theory, an employee violates that duty when he or she determines to act wrongfully or break loyalty (such as by taking another job) with the employer.[18] The court determined that Citrin violated his fiduciary duty of loyalty to IAC and therefore acted "without authorization" in accessing the files.[19] This decision was the primary appellate interpretation of the authorization language in the CFAA[20] until the Ninth Circuit's decision in *Brekka*.

---

[14] *Citrin*, 440 F.3d at 420.

[15] *Id*. at 419.

[16] *Id*.

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

[18] Restatement (Third) of Agency, §8.01 (2006).

[19] *Id*.

[20] The First Circuit also considers the issue, but offers a similar interpretation as the Seventh Circuit and the *Citrin* case is the one generally cited as the primary authority. *See* Nick Akerman, *Time to Review Corporate Computer Policies*, NAT'L L.J. (Feb. 3, 2010), http://computerfraud.us/files/2010/03/Time-to-Review-Computer-Policies-v1.pdf .

B. The Ninth Circuit and Plain Language Interpretation

In September 2009, the Ninth Circuit decided *Brekka*, another case involving an employee's improper use of company files. The Ninth Circuit was "unpersuaded by [the] interpretation" of the Seventh Circuit.[21] Instead, the court considered the plain language of the statute and the rule of lenity for criminal or quasi-criminal statutes.[22] LVRC Holdings employed Brekka to manage one of its treatment facilities. As part of this position, Brekka received access to the computer system and full access to any files or records. During his employment, Brekka travelled between his work in Nevada and his home in Florida. He often transmitted files between his work and home computers. He eventually decided to start his own business and dumped a number of files, including confidential information, from his work computer to his home laptop. LVRC Holdings sought civil damages against him for violation of the CFAA.

The *Brekka* court first noted that the CFAA is primarily a criminal statute, although *Brekka* was a civil case,[23] and determined that as a criminal statute the rule of lenity should be applied in interpreting any ambiguity of language.[24] The rule of lenity mandates that courts interpret ambiguous criminal statutes in favor of the defendant in order to avoid unexpected burdens.[25] According to the court, the "rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government."[26] The court specifically cited *Citrin* and stated that applying agency theory in these cases would lead to confusion for defendants because such an interpretation is not implied by the plain language of the statute.[27]

---

[21] *Brekka*, 581 F.3d at 1134.

[22] *Id*. at 1134-35.

[23] The CFAA is a criminal statute, but it provides civil remedies in addition to criminal penalties. Fishman and McKenna, Wiretapping and Eavesdropping §26:1 (2010).

[24] *Brekka*, 581 F.3d at 1134.

[25] *Id.*

[26] *Id.* at 1135(citing *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006)).

[27] *Id.*

The *Brekka* Court then considered the plain language of the statute to determine the meaning of authorization.[28] The court defined "authorization" to access a company's computer as "when the employer gives the employee permission to use it."[29] The court reasoned that the CFAA's plain language says nothing about an employee's fiduciary duty of loyalty. Authorization begins and ends with the employer, not the employee, under this view. An employee acts without authorization only if the employer never gives permission or affirmatively rescinds permission. The court determined that Brekka was not liable under the CFAA because the LVRC had authorized his access to the computer. In the court's view, this was not "without authorization" as the statute requires.

The court further opined that Brekka could not have violated the CFAA under "exceeds authorized access" because he only accessed the computer as the company had allowed. The CFAA addresses access, not use, according to the Ninth Circuit. What the employee does with materials after properly accessing them does not bring the employee's actions under the sanctions of the CFAA.[30]

The Ninth Circuit is the first federal appellate court to apply this reasoning. However, the *Brekka* Court's rationale is not new. Prior to the *Brekka* opinion, district courts had applied similar logic when interpreting the terms "authorization" and "authorized access."

The interpretations from the *Citrin* and *Brekka* decisions provide the guideposts for other interpretations of the CFAA. Other circuits have interpreted the statute similarly, with some minor variation.[31]

---

[28] *Id.*

[29] *Id.* at 1133.

[30] *Id.* at 1135.

[31] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001)(supporting the *Citrin* analysis, but noting use of "scraper" program "exceeded authorized access," assuming program's speed and efficiency depended on breach of confidentiality agreement with former employer); ReMedPar, Inc. v. AllParts Medical, LLC, 683 F.Supp.2d 605, 613 (M.D.Tenn 2010)(following the *Brekka* reasoning, but attaching legislative history analysis as well); Bro-tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378, 407 (E.D. Pa. 2009)(supporting the *Brekka* reasoning, but noting that whether an employee who had deleted emails from his company computer before discharge had exceeded authorized access is a question of fact for a jury); Cenveo, Inc. v. Rao, 659 F. Supp. 2d 312, 317 (D. Conn. 2009)(stating transmission of confidential information via computer is not enough, but can only exceed access if the information accessed was *in the computer*).

The reasoning of *Brekka* has been more widely adopted and can be found in district court cases from the Second, Third, Fourth, Sixth, Eighth, and Tenth Circuits.[32] Most of these apply an almost identical analysis to that of the *Brekka* case, though the Second and Fourth Circuits have slight variations.[33] In these cases, courts often find an employee is without authorization only when he or she never received access to particular data or systems. Once an employee receives access to a system, an employer has little recourse under the Ninth Circuit interpretation of "without authorization."

C. Beyond Citrin and Brekka: The Fifth and Eleventh Circuits' Interpretations of the CFAA

Two circuit court decisions following *Brekka* further outline the nuances of applying §1030(a)(2)(B), particularly to employees who exceed authorized access. Both decisions highlight the importance of the employee's knowledge. The Fifth Circuit in *U.S. v. John*[34] noted that "an authorized computer user 'has reason to know' that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme" and thus violates the CFAA by acting.[35] The Eleventh Circuit ruled that notice to the employee of his access limits could be dispositive in determining whether authorization was exceeded.[36] Both decisions seem to distinguish, rather than dispute, the holding in *Brekka*.

In *John*, the Fifth Circuit considered the "exceeds authorization" language of the CFAA.[37] The court held that employers have broader protections against rogue employees than under the Ninth Circuit's interpretation. Unlike many of the other cases, the actions of the

---

[32] Though this Article uses *Brekka* as a guidepost, many of the referenced district court cases applied the same line of reasoning as *Brekka* prior to the *Brekka* decision.

[33] *Cenveo*, 659 F. Supp. 2d at 316 (noting a distinction where accused did not access information "in a computer"); *Werner-Masuda*, 390 F.Supp.2d at 499 (noting distinction where the act is unauthorized disclosure of information rather than unauthorized access to information).

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

[35] *John*, 597 F.3d at 273.

[36] United States v. Rodriguez, 628F.3d, 1258, 1260 (11th Cir. 2010).

[37] *John*, 597 F.3d at 273-73.

employee in *John* were criminal both under the CFAA and separate criminal fraud statutes. The employee accessed employer information and bank account records and used the information to defraud customers. Furthermore, the employer told the defendant that such access was prohibited and beyond the scope of what was authorized.[38] The court determined that the defendant's access exceeded authorization, stating that access "to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."[39]

The Fifth Circuit drew an important distinction from the *Brekka* case; the court noted that "the Ninth Circuit may have a different view" on how it interpreted the "exceeds authorization" language.[40] In *Brekka*, the court had determined that if an employer had not affirmatively rescinded authorization, an employee "would have no reason to know" that personal use might also violate the CFAA.[41] The *John* court stated that in its case, the reasoning that the employee "had no reason to know" did not apply.[42]

The violator in *John* had not only accessed employer data but had done so in "furtherance of a criminally fraudulent scheme."[43] The Fifth Circuit stated that "when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access' within the meaning of § 1030(a)(2)."[44] This interpretation of the phrase "exceeds authorized access" broadens the application of the CFAA beyond what the Ninth Circuits and other courts apply, but stops short of the employer-friendly holding in *Citrin*. Rather than providing blanket protection for employees given access by the employer, the Fifth Circuit imposes an important limitation on employees who violate employer policies and do so as part of an illegal act. This gives employers some remedies against gross

---

38 *Id*. at 272.
39 *Id.*
40 *Id.*
41 *Id*. at 273 (citing *Brekka*, 581 F.3d at 1134).
42 *Id*.
43 *Id.*
44 *Id.*

violations by employees – even employees previously granted access – but does not extend to employees who merely disregard the employer's expectation of loyalty.

The Eleventh Circuit decided in *U.S. v. Rodriguez* that notice to the employee that accessing information, otherwise normally authorized, outside the scope of normal business reasons was prohibited met the plain language of the CFAA.[45] The employer, Teleservice, had advised Rodriguez that accessing the personal information databases was only authorized for business reasons.[46] Any access outside of that scope was prohibited. Furthermore, Rodriguez readily admitted that he was aware of this policy and had accessed "things that were not authorized."[47]

The court distinguishes its holding from both the *Brekka* and *John* decisions. The court states that this case differs from *Brekka* in that the employer there had not provided any such notice to the employee regarding the prohibited access.[48] The court distinguishes *John* on the grounds that Rodriguez's lack of criminal use of the information (as required by *John*), "is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access."[49] The court does not reach the *John* standard because, unlike in *John*, Rodriguez exceeded his authorized access by violating a known policy of the employer.

III. WHAT CAN EMPLOYERS DO? A LOOK AT PRACTICAL SOLUTIONS

Employers should be careful to consider whether an employee acted without authorization or exceeded authorized access because circuit courts interpret the terms of the CFAA differently. Courts that follow the *Citrin* approach favor a broader acceptance of contractually setting up boundaries for authorization, for instance through confidentiality, employment, and noncompete agreements. In jurisdictions following *Citrin*'s agency law approach, employers have

---

45 United States v. Rodriguez, 628F.3d, 1258, 1263 (11th Cir. 2010).
46 *Id*. at 1260.
47 *Id*. at 1262.
48 *Id*. at 1263
49 *Id*.

more power to set up the boundaries that they want individual employees to follow. Specificity in employment agreements is not as crucial because of the loyalty requirements under agency theory that give employers a remedy regardless. But a best practice will be to make employment agreements specific enough to outline employee expectations of what could break the agency relationship. The more important issue in determining liability is whether an employee acted disloyally towards the employer or acted with wrongful purpose.

Under the *Brekka* analysis or similar interpretation, employers should limit the access of lower-level employees and expand access only when necessary. The larger question for employers under the *Brekka* analysis is what to do with those employees that require extensive access to data and systems. Those types of employees leave employers most vulnerable to breaches of confidentiality and noncompete agreements. Under *Brekka*, an employer's recourse may be limited under the CFAA. Even having confidentiality agreements, employment agreements, and computer policies does not always save employers in these circuits.

The *John* court sets forth a middle ground. An employer cannot use the "without authorization" language of the CFAA as a sword to parry employees already given access. But an employer may have some remedies under "exceeds authorized access." An employee who uses information obtained from a computer system as part of a criminal scheme when subject to a detailed employee computer-use policy that states exactly when an employee exceeds access probably violates the CFAA.

Rodriguez goes one step further, stating that a detailed policy by the employer and a demonstration that the employee had knowledge of that policy is enough to show access was not authorized or exceeded authorization under the CFAA. Under those circumstances, whether an employee planned to use the information as part of a criminal scheme is irrelevant. Knowledge and violation of the employer's policy can be sufficient to demonstrate the employee exceeded authorized access.

CONCLUSION

Employers should strive to limit computer access to employees and to clearly communicate computer-use policies to those with

access. The courts generally apply the CFAA in favor of employees. However, some circuits are giving employers a fighting chance. The Fifth and Eleventh Circuit rulings give more ground to employers. The best defense for employers is not to rely on the CFAA as a remedy but to limit access of employees to sensitive data and to be clear about what those limits are through detailed policies, computer-use agreements, and records demonstrating employees' knowledge of those policies.