The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers from Trade Secret Theft?

AUDRA A. DIAL AND JOHN M. MOYE,
KILPATRICK TOWNSEND & STOCKTON LLP*

This Article discusses the current split between the federal circuits over the scope of the Computer Fraud and Abuse Act ("CFAA") and whether it extends to employees who steal an employer's electronic trade secrets to which they were lawfully given access as employees. After discussing the legislative history of the CFAA and various appellate decisions interpreting its scope, the Authors argue that recent court decisions interpreting the statute—exemplified by the Fourth Circuit in WEC Carolina Energy Solutions, LLC v. Miller *and the Ninth Circuit in* United States v. Nosal*—are unduly narrow in their scope.*

The Authors argue that the CFAA, by its language, is broad enough to provide for civil liability when a disloyal employee misappropriates electronic trade secrets in violation of an employer's computer use policies. A contrary approach is harmful to employers and inconsistent with the statute's intent. In light of these ambiguities, clarification of the CFAA's scope—either from the Supreme Court or via legislative action—is sorely needed.

[*] Ms. Dial is a partner in Kilpatrick Townsend's Technology Litigation Team, where she focuses her practice on litigating trade secret disputes and patent infringement matters. Mr. Moye is an associate on the firm's Technology Litigation Team. He is also an adjunct professor at the University of North Carolina School of Law, where he teaches a course focused on trade secrets law. The Authors would like to thank Jeffrey H. Fisher of Kilpatrick Townsend for his invaluable assistance in preparing this Article.

Table of Contents

Introduction

One of the many changes wrought by the digital revolution is that employers—be they large companies, hospitals, or government agencies—are storing more and more of their proprietary, sensitive information on electronic servers. Visit any employer's office today—large or small, in any industry, in any part of the United States—and the chances are high that their business documents, including customer lists, formulas, pricing data, personnel records, and financial records are maintained on electronic servers rather than in physical file cabinets. The employees who work at these offices no longer simply use email to communicate with each other; they also regularly access their employer's databases to review electronic documents and data, and they use this information in their regular course of business.

Growing access to electronic information has raised a related question: How can employers protect their most sensitive, electronically stored trade secrets (such as formulas, software code, or financial data)? Many employers require their employees to follow "computer use" policies that provide, for example, that the employee will not use the electronic information to which she has access for any improper or unauthorized purpose. But what happens if the employee violates those computer use policies and, while still employed, steals the employer's most sensitive electronic records?

For example, imagine that—in the course of her work day—an employee logs onto a password-protected company server, visits an electronic directory to which she has proper access (because of her position in the company), and steals thousands of the company's most sensitive files by transferring them to an external hard drive. Days later, that employee terminates her employment, hands off the external hard drive to a competitor, and joins the competitor's operations to compete directly against the former employer using information obtained during her employment there. What remedies, if any, does the former employer have?

In addition to an action for trade secret misappropriation (assuming the information stolen involved a trade secret), the Computer Fraud and Abuse Act ("CFAA") has represented an additional method of enforcement in recent years.[1] That statute, originally passed in 1984, imposes both criminal and civil liability on a person who "intentionally accesses a computer without authorization" or "exceeds authorized access," thereby obtaining "information" from a computer that is "used in or affecting interstate or foreign commerce."[2] Until recently, the CFAA served as a powerful weapon in an employer's arsenal when the employer was faced with a deceptive employee who misappropriated electronic information in violation of the employer's computer use policies. In the last decade, companies have increasingly raised CFAA claims alongside state law claims for trade secret misappropriation in order to obtain federal court jurisdiction.[3]

More recently, however, it has become unclear whether and to what extent the CFAA remains a viable method of enforcing the theft of electronic information by internal employees. In *WEC Carolina Energy Solutions, LLC v. Miller*,[4] the Fourth Circuit Court of Appeals broadened the existing split between the federal circuits over whether the CFAA extends to rogue employees who misuse electronic information when the information was gained from a company computer to which the employee had proper access.

In *WEC*, the Fourth Circuit joined the Ninth and Second Circuits to hold that the CFAA cannot impose liability on an employee who was given lawful access to company information but later misused that information in violation of the employer's computer use policies.[5] Furthermore, the Fourth Circuit held that the CFAA can only impose liability on employees who are either *not permitted* to access certain company information but do so anyway, or who otherwise exceed the boundaries of their authorized access—perhaps by altering information

[1] 18 U.S.C. § 1030 (2012).

[2] *Id.* § 1030(a)(2)(C).

[3] *See, e.g.*, Mobile Mark, Inc. v. Pakosz, No. 11-C-2983, 2011 WL 3898032 (N.D. Ill. Sept. 6, 2011) (bringing a claim for trade secret theft alongside a CFAA claim); AssociationVoice, Inc. v. AtHome Net, Inc., No. 10-CV-00109, 2011 WL 63508 (D. Col. Jan. 6, 2011) (same); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188 (E.D. Wash. 2003) (same).

[4] 687 F.3d 199 (4th Cir. 2012).

[5] *Id.* at 207.

in a computer beyond their access level.[6] However, the court made clear that the CFAA does not extend to an employee who has permission to access certain electronic information and later misuses that information in violation of a company use policy.[7] This narrow interpretation of the statute contrasts with the Seventh, Fifth, and Eleventh Circuits, which have construed the CFAA as imposing liability in such circumstances.[8]

This circuit split—and the confusion over the scope of the phrases "exceeds authorized access" and "without authorization" in the statute—carries significant implications for all employers. First, the ability to pursue remedies under the CFAA against a misappropriating employee now depends in part on the jurisdiction in which the action is being pursued. Additionally, employers in those circuits that have taken a narrow approach will also be limited in their ability to pursue disloyal employees and will be required to take alternate measures to prevent the theft of their sensitive electronic information. Employers in these jurisdictions may be unable to obtain federal jurisdiction over trade secret misappropriation claims (absent diversity) when an employee steals electronic information from a company computer to which the employee had access. Whereas previously companies victimized by disloyal employees would typically use a federal CFAA cause of action alongside state causes of action like trade secret theft in order to obtain federal court jurisdiction,[9] that strategy may no longer be viable in certain circuits.

This Article argues that the approach to the CFAA—exemplified by the Fourth Circuit in *WEC*—is unduly narrow in its scope, and that the type of conduct involved in *WEC*—a thieving employee who violated his employer's computer use policies and stole information to which he initially had "access"—is precisely the type of conduct that the CFAA was intended to prevent. At the very minimum, courts should recognize that the CFAA is broad enough to provide for civil liability when a disloyal employee misappropriates electronic information in contravention of the employer's computer use policies. An alternate, narrow view can be damaging to employers, as it could foreclose opportunities to obtain a remedy for disloyal conduct involving electronic information, particularly if such information does not rise to the level of a trade secret.

Part I of this Article explains the history of the CFAA and its purpose. Part II provides an overview of the existing circuit split, including the recent *WEC* decision. Part III argues that the approach taken by the Fourth, Ninth, and Second Circuits is unduly narrow in

[6] *Id.* at 206.

[7] *Id.* at 207.

[8] *See* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[9] *See, e.g.*, *WEC*, 687 F.3d 199.

scope, is contrary to the intent of the CFAA, and can be harmful to employers. Part IV argues that clarification from the Supreme Court on the scope of the CFAA is sorely needed in light of the existing circuit split; the Court should recognize that the statute provides a civil remedy in the case of a disloyal employee who misappropriates electronic trade secret information in violation of an employer's computer use policies.

I. The Computer Fraud and Abuse Act

Congress passed the CFAA in 1984.[10] The statute was the first piece of federal legislation to address computer crime.[11] Originally, the CFAA was intended to be an anti-hacking statute; it narrowly imposed criminal liability on persons who accessed a computer "without authorization" or "for purposes to which [the] authorization does not extend" in order to commit three specific types of acts: (i) obtain national security secrets; (ii) obtain personal finance records; or (iii) hack into federal government computers.[12]

Subsequent amendments, however, changed and significantly expanded the reach of the CFAA.[13] In 1994, Congress amended the CFAA to permit civil actions by persons who suffered "damage or loss by reason of a violation" of the statute.[14] In 1996, Congress again amended the statute so that it was no longer limited solely to particular types of digital information.[15] Congress also expanded the definition of "protected computer," which had originally been limited solely to "Federal interest" computers.[16] Today, the CFAA definition of "protected computer" broadly encompasses any computer "which is used in or affecting interstate or foreign commerce or communication."[17]

Advocates of both the broad and the narrow view of the phrase "exceeds authorized access" in the CFAA have cited the legislative history to support their argument.[18] Those in favor of the narrow view point out that Congress originally focused the Act to prevent computer hacking.[19] In

[10] *See* H.R. Rep. No. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689. "There is [n]o specific federal legislation in the area of computer crime." *Id.* at 3691.

[11] *Id.*

[12] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (1984) (codified at 18 U.S.C. § 1030).

[13] For a thorough discussion of each amendment to the CFAA, see Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1563 (2010).

[14] Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX, 108 Stat. 2097, 2098 (1994) (codified at 18 U.S.C. § 1030(g)).

[15] Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491.

[16] *Id.* at 3492.

[17] 18 U.S.C. § 1030(e)(2) (2012).

[18] Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 Vand. J. Ent. & Tech. L. 543, 560–61 (2011).

[19] *See* Briggs v. State, 704 A.2d 904, 911 (Md. 1998); Booms, *supra* note 18, at 560–61 (citing

addition, courts adopting a narrow view of the statute have relied on the 1986 Amendment to the CFAA, which eliminated references to the hacker's "purposes" in obtaining the information and replaced them with the phrase "exceeds authorized access," suggesting that Congress continued to focus on computer hackers.[20] A 1996 Senate Report has also been interpreted to suggest that the CFAA is meant to prevent outside access to, not the misuse of, information.[21] Thus, advocates of the narrow view argue that, despite the broad language of the CFAA, it was drafted to prevent computer hacking, and that the legislative history does not suggest that Congress intended for the Act to apply more broadly to misappropriation by "inside" employees.

In contrast, defenders of the broad view assert that the legislative history of the CFAA just as strongly supports their position: The statute extends to disloyal employees who steal their employers' electronic information. These advocates point out that that the CFAA, although initially targeted at hackers, has been amended repeatedly and that each subsequent amendment has expanded the scope of the CFAA.[22] Indeed, Congress has expanded the CFAA to include a private civil cause of action where one did not initially exist, to apply to conduct well beyond the original, enumerated factors, and to expand the types of computers entitled to protection.[23] Proponents of this broad view assert that Congress intended the statute to cover a broad array of computer crimes. Moreover, as the type and scope of computer crimes have changed over the years as technology evolved and become more integral to businesses,

H.R. Rep. No. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706 ("[The CFAA] deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer.")).

[20] US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009); *see* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008).

[21] *Gast*, 535 F. Supp. 2d at 966 ("Senate report[s have] suggested a difference between access without authorization and exceeding authorized access based on the difference between 'insiders' and 'outsiders.' Insiders were those with rights to access computers in some circumstances (such as employees), whereas outsiders had no rights to access computers at all (such as hackers)." (citing S. Rep. No. 104-357, 1996 WL 492169, at *4 (1996) and Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1630 (2003)).

[22] *See* Booms, *supra* note 18, at 560 (citing Guest-Tek Interactive Entm't Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009) ("Although the majority of CFAA cases still involve 'classic hacking activities,' the CFAA's reach has been expanded in the past two decades by the enactment of a private cause of action and a more liberal judicial interpretation of the statutory provisions.")).

[23] *Id.*; *see* P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, L.L.C., 428 F.3d 504, 510 (3d Cir. 2005) ("[T]he scope of [the CFAA's] reach has been expanded over the last two decades."); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) (quoting S. Rep. No. 104-357, at *7–8) ("The proposed § 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer . . . . This [section] would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected . . . . The crux of the offense under § 1030(a)(2)(C), however, is the abuse of a computer to obtain the information.").

Congress has broadened the CFAA to cover far more than traditional computer hacking by an "outsider."[24]

Federal courts have attempted to construe the purpose of the CFAA and the meaning of key elements in the act, namely "exceeds authorized access" and "without authorization," against this complex legislative history. In doing so, however, the courts have been unable to reach a clear consensus. Although the circuit split has been unfolding for years, the recent *WEC* decision has only exacerbated the disagreement among the circuits as to whether the CFAA extends to a disloyal employee who misappropriates the electronic trade secrets of her employer.[25]

II. The Present Circuit Split

A. The Fourth Circuit's Decision in *WEC*

WEC involved a fact pattern that is all too familiar in trade secret misappropriation cases. WEC, a company providing welding services to the power industry, sued its ex-employee Willie Miller, his assistant Emily Kelley, and their new employer Arc Energy Services, after Miller downloaded a large number of electronic files, abruptly resigned from his employment, and, along with Kelley, joined a competitor.[26]

During Miller's employment, he was provided a company laptop and had been granted access to the company's servers and intranet, which contained "numerous confidential and trade secret documents," including pricing terms, information on pending projects, and other technical information.[27] WEC had written policies in place prohibiting employees from (i) using any company information without authorization or (ii) downloading it to a personal computer.[28] However, WEC's computer use policies "did not restrict Miller's authorization to access the information."[29]

Miller resigned from WEC and joined Arc, a direct competitor.[30] While still employed by WEC, Miller downloaded a number of confidential documents from the company's servers and emailed them to his personal email account.[31] He and his assistant also "downloaded

[24] Booms, *supra* note 18, at 560–61.

[25] *Compare* WEC Carolina Energy Solutions, L.L.C. v. Miller, 687 F.3d 199, 206–07 (4th Cir. 2012), *and* United States v. Nosal, 676 F.3d 854, 862–63 (9th Cir. 2012), *with* Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

[26] *WEC*, 687 F.3d at 202.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

confidential information to a personal computer."[32] Each of these actions was taken solely to benefit Arc, Miller's future employer, rather than WEC.[33] Twenty days after leaving WEC, Miller "used the downloaded information to make a presentation on behalf of Arc to a potential WEC customer," who ultimately awarded projects to Arc based upon the presentation.[34]

WEC sued in the U.S. District Court for the District of South Carolina, asserting nine state causes of action—including misappropriation of trade secrets, tortious interference with contract, and conversion—and a federal cause of action under the CFAA.[35] The district court dismissed the CFAA claim under Federal Rule 12(b)(6), finding that WEC's computer policies only limited the "*use* of information not access to that information."[36] The district court held that even if Miller and Kelley had acted "contrary to [WEC] company policies regulating use, [such conduct] would not establish a violation of company policies relevant to *access*, and, consequently, would not support liability under the CFAA."[37] In other words, the district court concluded that no liability was warranted under the CFAA because Miller had been permitted to access the information at issue as an employee.[38] The remaining state law claims were then dismissed for lack of subject matter jurisdiction.[39]

On appeal, a unanimous three-judge panel of the Fourth Circuit affirmed the district court's interpretation of the CFAA.[40] In its opinion, the court examined the scope of the CFAA and whether its provisions "extend to violations of policies regarding the use of a computer or information on a computer to which a defendant otherwise has access."[41] The court ultimately concluded that the phrases "without authorization" and "exceeds authorized access" as used in the statute mean that an employee cannot either "gain admission to a computer without approval" or gain information that is located "outside the bounds of his approved access."[42] The court declined to extend the CFAA to impose liability on employees for "the improper *use* of information validly accessed."[43]

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *See* WEC Carolina Energy Solutions, L.L.C. v. Miller, No. 0:10-CV-2775-CMC, 2011 WL 379458, at *5 (D. S.C. Feb. 3, 2011).

[36] *Id.*

[37] *Id.* (emphasis added).

[38] *Id.*

[39] *Id.* at *6.

[40] *See* WEC Carolina Energy Solutions, L.L.C. v. Miller, 687 F.3d 199, 206–07 (4th Cir. 2012).

[41] *Id.* at 203.

[42] *Id.* at 204.

[43] *Id.*

Because WEC gave Miller access to the information that he allegedly misappropriated, the Fourth Circuit concluded there was no basis for a CFAA violation (regardless of the purpose behind his access of the information).[44]

The Fourth Circuit raised concerns about reading the CFAA too broadly in light of the "rule of lenity" applicable in criminal law.[45] The court suggested that reading the CFAA more expansively could result in potential liability for any employee who "checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy."[46] Construing the statute as one "meant to target hackers," the court held that a broader view could transform the CFAA "into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy."[47]

B. Other Circuits Following *WEC*'s Narrow Approach to CFAA Liability

The *WEC* panel's decision was similar to that reached by the Ninth Circuit in the criminal case of *United States v. Nosal*.[48] *Nosal* involved a former employee of an executive search firm, Korn/Ferry International, who persuaded current employees of the firm to download confidential information from Korn/Ferry's computers and transfer the information to Nosal in order to help him start a competing business.[49] Although the employees had legitimate "access" to the employer's database and the confidential information contained therein, the company's internal computer use policies prohibited the unauthorized disclosure of such information.[50] The federal government filed criminal charges against Nosal under the CFAA, accusing him of "aiding and abetting the Korn/Ferry employees in 'exceed[ing their] authorized access' with intent to defraud."[51]

As in *WEC*, the Ninth Circuit's en banc *Nosal* decision addressed whether the phrase "exceeds authorized access" refers only to an employee who accesses files that the employee does not have permission to access, or whether it also penalizes an employee who has access to a computer by

[44] *Id.* at 207.

[45] *Id.* The Ninth Circuit raised similar concerns in *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012). Under the rule of lenity, "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *See* U.S. v. LeCoe, 936 F.2d 398, 402 (9th Cir. 1991).

[46] *WEC*, 687 F.3d. at 206.

[47] *Id.* at 207.

[48] 676 F.3d 854 (9th Cir. 2012).

[49] *Id.* at 856.

[50] *Id.*

[51] *Id.* (quoting 18 U.S.C. § 1030(a)(4)).

virtue of her employment but uses such data for unauthorized purposes.[52] The government argued that the language of the CFAA was broad in its scope and that the statute encompassed the improper use of electronic information.[53]

Specifically, the government noted that the phrase "exceeds authorized access" was defined to include accessing "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."[54] The government argued that the word "so" was defined in the CFAA as "in that manner," and that it referred to the manner in which the person accessing the information uses the information she obtains or alters.[55] According to the government, the word "so" (as defined) specifically referred to use, and a narrow reading of the statute would render the word "so" superfluous.[56] In addition, the government argued that this narrow reading ignored that the CFAA distinguished between two phrases: "without authorization" and "exceed authorized access."[57]

On appeal, the court recognized that the CFAA was "susceptible to the Government's broad interpretation" but ultimately found that the text, the rule of lenity, and the purpose of the statute supported the more restrictive interpretation.[58] The court therefore held that "the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'"[59]

Specifically, the Ninth Circuit focused on the fact that the statute was drafted to target hackers, and it read the phrase "exceeds authorized access" as applying to *inside* hackers (that is, those who may have some access to a company computer, but who go further and access—or "hack into"—files to which they have no authorized access).[60] The court also recognized that the "rule of lenity" is applicable to criminal statutes, explaining that if Congress meant for the CFAA to apply more broadly to protect electronic trade secrets, it would have used clearer language to signal its intent.[61] The court expressed concern with expanding criminal liability to conduct that, unlike hacking into a computer, is not "inherently

[52] *Id.* at 857.

[53] *Id.*

[54] *Id.* (quoting 18 U.S.C. § 1030(e)(6)).

[55] *Id.*

[56] *Id.*

[57] *Id.* at 856.

[58] *Id.*

[59] *Id.* (quoting Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)). *Accord* Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005).

[60] *Nosal*, 676 F.3d. at 857.

[61] *Id.*

wrongful."[62] Like the Fourth Circuit, the Ninth Circuit reasoned that a broad interpretation of the CFAA would mean that routine violations of employer computer use policies, such as "g-chatting with friends, playing games, shopping or watching sports highlights," could be transformed into potential criminal violations.[63] The court therefore concluded that "exceeds authorized access" in the CFAA was "limited to violations of restrictions on *access* to information, and not restrictions on its *use*."[64] Because Nosal's accomplices had been afforded access to the company's information, the court found that the government failed to satisfy the element of "without authorization, or exceeds unauthorized access."[65]

Since *Nosal* in April 2012, a number of district courts in the Ninth Circuit have followed this interpretation of the CFAA.[66] In addition, although no other circuit courts have expressly adopted the narrow approach to the CFAA taken by the Ninth Circuit in *Nosal* and the Fourth Circuit in *WEC*, a number of district courts in other circuits have adhered to the narrow view of the statute with the expectation that their respective circuits will follow. For example, district courts in the Second Circuit have construed the phrases "without authorization" or "exceeds authorized access" similarly to *Nosal*.[67] Courts in the Sixth Circuit similarly appear

[62] *Id.* at 860.

[63] *Id.*

[64] *Id.*

[65] *Id.* at 864. The Nosal case was remanded to the Northern District of California following the Ninth Circuit's ruling. On remand, the government moved forward with certain criminal charges against Nosal based on separate acts of "outsider hacking" that Nosal had allegedly committed unrelated to the CFAA charges based on the information to which Nosal had lawfully had access as an employee. *See* United States v. Nosal, CR-08-0237 EMC, 2013 WL 978226 at *6 (N.D. Cal. 2013). The United States argued that Nosal could be prosecuted under the CFAA for the "outsider counts"—in which former Korn/Ferry employees had hacked a current employee's password to access Korn/Ferry's "Searcher" database and had provided Nosal with confidential information. *Id.* The trial court allowed those charges against Nosal to proceed. *Id.* at *9. On April 24, 2013—following two days of jury deliberations—Nosal was convicted of the "outsider counts" under the CFAA. *See* Karen Gullo, *Ex-Korn/Ferry Executive Convicted of Trade-Secret Theft*, BLOOMBERGBUSINESSWEEK (Apr. 24, 2013), http://www.businessweek.com/news/2013-04-24/ex-korn-ferry-executive-convicted-of-trade-secret-theft-1. Nosal's conviction shows that the CFAA remains a helpful tool for employers faced with unauthorized acts of employee hacking, even if it is no longer viable in certain circuits as a means of preventing "inside" theft by employees with lawful access to information.

[66] *See* Incorp Servs. Inc. v. Incsmart.Biz Inc., 11-CV-4660-EJD-PSG, 2012 WL 3685994, at *3 (N.D. Cal. Aug. 24, 2012) (citing *Nosal* and stating that "the CFAA is an anti-hacking statute, and not a misappropriation statute"); Hat World, Inc. v. Kelly, CIV. S-12-01591 LKK, 2012 WL 3283486, at *5 (E.D. Cal. Aug. 10, 2012) (same); *see also* Oracle Am., Inc. v. Serv. Key, L.L.C., C 12-00790 SBA, 2012 WL 6019580, at *5 (N.D. Cal. Dec. 3, 2012) (finding that using legitimate employee access for improper purposes is "beyond the scope of the CFAA" under *Nosal*).

[67] *See* Major, Lindsey & Africa, L.L.C. v. Mahn, 10 CIV 4329 CM, 2010 WL 3959609 (S.D.N.Y. Sept. 7, 2010) (finding that the Second Circuit is likely to adopt the narrow view); Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Jet One Grp. v. Halcyon Jet Holdings, Inc., No. 08-CV-3980, 2009 WL 2524864, at *5–7 (E.D.N.Y. Aug. 14, 2009) (adopting the narrow view and

poised to follow the approach taken by the Fourth and the Ninth Circuits.[68] District courts in the Eighth Circuit[69] and the Third Circuit[70] have likewise endorsed the *Nosal* interpretation of the CFAA and the narrow reading of the phrases "without authorization" and "exceeds authorized access."

Consequently, these circuits will only impose liability under the CFAA when a disloyal employee accesses files that she has never been *authorized to access*. The mere misuse of electronically stored information (by passing information to a competitor, for example) will not satisfy the statutory threshold for civil liability under the CFAA if the employer gave the employee access to such information as part of her employment.

C. The Contrary View: *Citrin* and Its Progeny

In contrast, courts in other circuits have taken a broader approach to liability under CFAA, holding that where an employee exceeds the scope of his or her "authorized access" and downloads and misuses sensitive company files in contravention of the employer's use policies, such conduct will constitute "unauthorized access" under the statute.

The Seventh Circuit first adopted this approach in *International Airport Centers v. Citrin*.[71] That case involved a defendant, Citrin, who quit his job at International Airport Centers and started a competing business in violation of his employment contract.[72] Prior to returning his company laptop, he deleted all of the electronic data on the laptop—including data that he collected and data that would show that he engaged

stating that the "Second Circuit has implicitly adopted the narrow view").

[68] *See* Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) (suggesting that Ninth Circuit interpretation of CFAA was proper); Ajuba Int'l L.L.C. v. Saharia, No. 11-12936, 2012 WL 1672713, at *11–12 (E.D. Mich. May 14, 2012); ReMedPar, Inc. v. AllParts Med., L.L.C., 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933–36 (W.D. Tenn. 2008); Am. Family Mut. Ins. Co. v. Rickman, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008).

[69] *See* Walsh Bishop Assocs., Inc. v. O'Brien, Civil No. 11-2673 DSD/AJB, 2012 WL 669069, at *3 (D. Minn. Feb. 28, 2012) ("[S]ection (a)(2) is not based on use of information; it concerns access."); Xcedex, Inc. v. VMware, Inc., No. 10-3589, 2011 WL 2600688, at *4 (D. Minn. June 8, 2011) (adopting a narrow interpretation); Condux Int'l, Inc. v. Haugum, Civil No. 08-4824 (ADM/JSM), 2008 WL 5244818 (D. Minn. Dec. 15, 2008). *But see* NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) ("The Court concludes that the broad view can best distinguish between the CFAA's statutory language 'exceeds authorized access' and 'unauthorized access' by looking solely at the text of the statute.").

[70] *See* Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378, 407 (E.D. Pa. 2009) ("The Court is persuaded by the reasoning in the latter line of cases, and adopts the less capacious view of the legal meaning of 'without authorization' and 'exceeds authorized access' expressed therein."); Brett Senior & Assocs., P.C. v. Fitzgerald, CIV.A. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007) ("The conduct targeted by section (a)(4), however, is the unauthorized procurement or alteration of information, not its misuse or misappropriation.").

[71] 440 F.3d 418 (7th Cir. 2006).

[72] *Id.* at 419.

in improper conduct before he quit his job.[73] Citrin's former employer brought a civil action against Citrin under the CFAA, accusing Citrin of accessing "a protected computer without authorization," thereby causing damage to the company.[74]

On appeal of the district court's dismissal of the CFAA claims under Federal Rule 12(b)(6), Judge Posner wrote for the court that although Citrin had initially been given access to company information, he had breached his duty of loyalty when he quit and started a competing business.[75] The court then held that when Citrin terminated his agency relationship with International Airport Centers, his "authority" to access the company laptop was also terminated.[76] Consequently, at the time Citrin deleted the files on his laptop, he no longer had "authorization" to access the laptop. Thus, the court held that Citrin acted "without authorization" in violation of the CFAA.[77]

On different facts, the Eleventh Circuit adopted a similarly expansive interpretation of the phrase "exceeds authorized access." In *United States v. Rodriguez*, the Eleventh Circuit upheld the imposition of criminal liability on a defendant who "obtained personal information [during his employment] for a nonbusiness reason."[78] The defendant, Rodriguez, worked as a representative for the Social Security Administration and had been given access to databases containing sensitive, confidential personal information—including any person's social security number, date of birth, address, and annual income.[79] The Administration's computer use policies expressly prohibited employees from obtaining personal information from the database without a legitimate business reason.[80] In violation of this policy, Rodriguez used the agency's database to obtain the personal records of seventeen individuals for decidedly nonbusiness reasons—specifically, to obtain personal information about women for whom he had romantic interests.[81] A jury found Rodriguez guilty of seventeen violations of the CFAA.[82]

[73] *Id.*

[74] *Id.* at 420 (emphasis omitted) (quoting 18 U.S.C. § 1030(a)(5)(A)(ii)).

[75] *Id.* at 420–21.

[76] *Id.* at 421 (quoting State v. DiGiulio, 835 P.2d 488, 492 (Ariz. Ct. App. 1992)) ("Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship. . . . Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.").

[77] *Id.* at 420 (citing 18 U.S.C. § 1030(a)(5)(A)(ii)).

[78] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

[79] *Id.* at 1260.

[80] *Id.*

[81] *Id.* at 1260–62.

[82] *Id.* at 1262 (citing 18 U.S.C. § 1030(a)(2)(B)).

On appeal, Rodriguez argued that his actions did not violate the CFAA because he "accessed only databases that he was authorized to use as a TeleService representative."[83] The Eleventh Circuit rejected his argument, holding that because the Social Security Administration's computer use policy authorized Rodriguez to obtain personal information only for actual business reasons, Rodriguez had "*exceed[ed] authorized access*" when he obtained personal information for nonbusiness reasons, thereby converting his otherwise permissible access into "unauthorized access."[84]

To reach this conclusion, the Eleventh Circuit explicitly distinguished an earlier Ninth Circuit decision, *LVRC Holdings LLC v. Brekka*,[85] in which the Ninth Circuit held that a former employee did not violate the CFAA when he emailed documents that he was authorized to access to his personal email account.[86] The *Rodriguez* court explained that in *Brekka*, there was no company policy prohibiting employees from sending email to personal accounts, whereas the Social Security Administration's policy clearly prohibited Rodriguez from obtaining personal information for nonbusiness reasons.[87] Thus, the terms of the employer's use policy were pivotal to the Eleventh Circuit's finding of criminal liability.

The Fifth Circuit has likewise taken a broad approach to liability under CFAA, holding in *United States v. John* that even "authorized access" to information may not be unlimited, particularly when the defendant uses his authorized access "in furtherance of or to perpetrate a crime."[88] In *John*, the defendant was a Citigroup employee with access to Citigroup's computer system and customer account information.[89] The defendant provided confidential customer information to her half-brother, who then fraudulently charged four different Citigroup customers' accounts.[90] A jury found the defendant guilty of two counts of "exceeding authorized access" to a protected computer under § 1030(a)(2)(A) and (C) of the CFAA.[91]

On appeal, the defendant argued that she had access to Citigroup's computers and account information and that the CFAA prohibited only unauthorized access to protected computers, not unauthorized *use* of information.[92] The Fifth Circuit disagreed, finding that, although the

[83] *Id.* at 1263.
[84] *Id.* (emphasis added).
[85] 581 F.3d 1127 (9th Cir. 2009).
[86] *Id.*
[87] *Rodriguez*, 628 F.3d at 1263.
[88] 597 F.3d 263, 271 (5th Cir. 2010).
[89] *Id.*
[90] *Id.*
[91] *Id.* at 269–70.
[92] *Id.* at 271.

defendant technically had access to the confidential information, Citigroup's computer use policies expressly limited her access to certain uses.[93] Using confidential information to assist in perpetrating a fraud was not included among the permitted uses, and thus the defendant's participation in a fraudulent criminal scheme exceeded her permissible "access" to Citigroup's electronically stored information.[94]

The *John* court observed that the existence of Citigroup employee policies—and John's knowledge of such policies—established the parameters of her "authorized access."[95] Although the court recognized that violation of a confidentiality agreement should not always raise criminal charges, the court found that an employee's "access may be exceeded if the purposes for which access has been given are exceeded."[96] Given that the company's use policies prohibited the misuse of confidential information and that the defendant was aware of those policies, the court held that the defendant's actions—which involved the misuse of confidential information—violated the CFAA and satisfied the "exceed authorized access" element of § 1030(a)(2).[97]

District courts in the Fifth, Seventh, and Eleventh Circuits have followed this broader approach to CFAA liability, recognizing that when an employee violates the terms of a computer use policy and engages in an impermissible use of electronic information, that employee will be deemed to have engaged in an "unauthorized" access of company information in violation of the CFAA. In the Fifth Circuit, for example, district courts have broadly interpreted the CFAA in both civil and criminal contexts.[98] Similarly, numerous district courts in the Seventh Circuit have found that an employee's breach of the duty of loyalty severs her authority to access the employer's information and exposes the employee to liability under the CFAA.[99] However, district courts in the Eleventh Circuit have not

[93] *Id.* at 271–72.

[94] *Id.* at 271 (citing United States v. Phillips, 477 F.3d 215, 218 (5th Cir. 2007)) (holding that a student who accessed part of a system to which he had not been given a password exceeded authorized use).

[95] *Id.* at 272.

[96] *Id.* (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001)).

[97] *Id.*

[98] *See* Barnstormers, Inc. v. Wing Walkers, L.L.C., No. EP-10-CV-261-KC, 2011 WL 1671641 (W.D. Tex. May 3, 2011) (citing *John*, 597 F.3d at 269) (holding that a defendant who was authorized to access a website as a member of the public violated the CFAA by using that access for the purpose of obtaining others' advertisements and placing copies of its advertisements on the site); Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028 (N.D. Tex. Apr. 20, 2011) (citing *John*, 597 F.3d at 269) (holding that the use of information in violation of a restrictive covenant states a claim under the CFAA).

[99] *See* Deloitte & Touche L.L.P. v. Carlson, No. 11 C 327, 2011 WL 2923865, at *4 (N.D. Ill. July 18, 2011) (citing Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006)) ("Here, Carlson is claimed to have begun his solicitation of Deckter before departing Deloitte. The data destruction was done, in part, to cover his tracks in wrongfully soliciting Deckter. If, as claimed,

followed *Rodriguez* as consistently. At least one district court in that circuit has recognized that the CFAA applies to an employee's misuse of information in violation of an employer's computer use policies.[100]

In summary, the federal circuits are significantly divided as to the scope of the CFAA and the extent to which otherwise permissible access to information can be construed as "unauthorized" to warrant the imposition of CFAA liability. The Fourth Circuit exacerbated this circuit split in *WEC*. As it now stands, courts in the Second, Fourth, and Ninth Circuits—as well as, perhaps, the Third, Sixth, and Eighth Circuits—have adopted the view that the CFAA does not extend to employees who have access to electronically stored trade secrets and company information, and who misuse that information in contravention of an employer's computer use policies. In contrast, the Fifth, Seventh, and Eleventh Circuits have adhered to the view that an employee's otherwise legitimate access can be rendered "unauthorized" when she exceeds the scope of the access given or otherwise engages in improper use of such information in violation of the employer's policies. Until the Supreme Court resolves this matter, the scope of the CFAA will depend largely on the location of the dispute involving misuse of electronic information.

III. What the Circuit Split Means for Employers and Their Electronic Trade Secrets

The circuit split over the scope of the CFAA has significantly impacted employers and their ability to prevent their employees' misuse of electronic information and trade secrets. Until recently, employers

Carlson was so nakedly violating his Director Agreement, he would have been acting contrary to his employer's interests, thereby ending his agency relationship with Deloitte and making his conduct 'without authorization.'"); Jarosch v. Am. Family Mut. Ins. Co., 837 F. Supp. 2d 980, 1021 (E.D. Wis. 2011) ("The plaintiffs undeniably had authority to access American Family's customer information while acting on behalf of American Family. However, as previously found, the plaintiffs breached their respective duties of loyalty to American Family. Thus, the plaintiffs' breach of their respective duties of loyalty, namely their having taken American Family policyholder information for the benefit of their new insurance agencies, appears to have terminated their authority to access American Family's customer information."); Motorola, Inc. v. Lemko Corp., 609 F. Supp. 2d 760, 768 (N.D. Ill. 2009) ("Taking these allegations as true, as the Court must do at this stage of the case, Wu was allegedly accessing confidential Motorola computers to send Motorola's confidential information to its competitor's chief information officer. This is sufficient to describe the accessing of Motorola's computers without or in excess of Wu's authorization, satisfying the requirement that Motorola allege that Wu's unauthorized access resulted in her obtaining information from Motorola's protected computers.").

[100] *See* Amedisys Holding v. Interim Healthcare of Atlanta, Inc., 793 F. Supp. 2d 1302, 1315 (N.D. Ga. 2011) ("While there is some question of whether Plaintiff generally permitted Mack to send the Referral Logs to her personal email account, there is no question that Mack exceeded any authority she had when she sent them to herself after accepting a position at Interim for use in competing with Amedisys."). *But see* Trademotion, L.L.C. v. Marketcliq, Inc., 857 F. Supp. 2d 1285, 1290–91 (M.D. Fla. 2012) ("[T]he CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information.").

typically included a CFAA claim as a supplemental remedy—in addition to a state law claim for trade secret misappropriation—when faced with theft of electronic information.[101] Prior to the recent decisions narrowing its scope, the CFAA had been a useful tool in the arsenal of a trade secret plaintiff—particularly as it allowed a party to obtain federal court jurisdiction over trade secret claims involving the theft of electronic trade secrets. Recently, however, the narrowing of the statute has negatively impacted employers: Not only does it drastically limit the ability to obtain federal court jurisdiction over trade secret claims, but it also places the onus on employers to anticipate and prevent the electronic theft of information by their employees by narrowly defining each employee's ability to use company electronic information.

First, the narrow reading of CFAA has had the indirect effect of making it much more difficult to obtain federal court jurisdiction in cases of electronic trade secret misappropriation. Indeed, in *WEC*, the plaintiff brought a civil suit in federal district court in South Carolina, invoking federal jurisdiction under the CFAA.[102] After dismissing the CFAA claim, the court in *WEC* dismissed the remaining state law claims for lack of subject matter jurisdiction.[103] In doing so, the *WEC* panel seemed to recognize that its decision would foreclose the ability of plaintiffs (absent diversity) to bring claims involving theft of electronic trade secrets in a federal forum.[104] Thus, one harmful impact of the circuit split (and the narrow construction afforded to the CFAA by those circuits following *WEC* and *Nosal*) is that, at least in certain jurisdictions, a trade secret plaintiff will have to establish diversity jurisdiction to pursue relief for electronic trade secret theft in a federal forum or be forced to litigate these complex claims in a state court. This has made it much more difficult to pursue trade secret violations because local procedural rules vary and state case law lacks uniformity.

Moreover, employers operating in jurisdictions that have adopted a narrow approach to the CFAA will now be unable to protect their electronic trade secrets merely by implementing written computer use restrictions. The Fourth Circuit's *WEC* ruling makes clear that computer use restrictions are necessary but not sufficient to protect confidential

[101] *See, e.g.*, Mobile Mark, Inc. v. Pakosz, No. 11-C-2983, 2011 WL 3898032 (N.D. Ill. Sept. 6, 2011) (bringing a claim for trade secret theft alongside a CFAA claim); AssociationVoice, Inc. v. AtHome Net, Inc., No. 10-CV-00109, 2011 WL 63508 (D. Col. Jan. 6, 2011) (same); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188 (E.D. Wash. 2003) (same).

[102] *See* WEC Carolina Energy Solutions, L.L.C. v. Miller, No. 0:10-cv-2775-CMC, 2011 WL 379458, at *5 (D. S.C. Feb. 3, 2011).

[103] *Id.* at *6.

[104] *See* WEC Carolina Energy Solutions, L.L.C. v. Miller, 687 F.3d 199, 206 n.4 (4th Cir. 2012) (noting that, although recourse under the CFAA for the alleged conduct was no longer available, "nine other state law causes of action potentially provide relief").

electronic information because an employee's mere violation of a use restriction (such as the theft of electronic data) will not support CFAA liability if the employee's "access" to the data was otherwise permitted. Consequently, employers in these circuits will be forced to revamp their practices and take additional steps to protect their most sensitive electronic files, most likely by carving out and identifying a discrete set of employees who should be given access to categories of information, manually barring such access for all other employees, and changing access levels for employees when their job functions change. The narrow approach is very restrictive and essentially affords employers the opportunity to obtain civil liability only against employee "hackers."

The narrow approach also seems woefully inconsistent with the fundamental purpose of the CFAA, which was drafted to prohibit a range of acts of computer misuse (without regard to the type of information stolen) and which, if anything, has been substantially broadened since its initial passage in 1984.[105] In light of technological developments in the nearly thirty years since its enactment, it seems inconsistent to read the CFAA as a narrow statute—designed only to penalize hacking—when the amendments to the statute suggest that it is intended to have a much broader application, particularly in the civil context. Moreover, the plain language of the statute—with *two separate* prongs, "without authorization" and "exceeds authorized access"—can be read broadly enough to encompass both the acts of rogue employees who "hack" into areas of the company to which they have no access (the "without authorization" prong) and the conduct of thieving employees who willfully violate their employer's computer use restrictions and thereby steal electronic data and information for an improper purpose (the "exceeds authorized access" prong).[106]

In light of the statutory language and intent—not to mention the detrimental impact that the narrow *Nosal*/*WEC* approach has on an employer's ability to prohibit the theft of its electronic trade secrets in a federal forum—the reasonable interpretation of the CFAA is the one articulated by Judge Posner in *Citrin*, which has been followed by the Fifth and Eleventh Circuits.[107] Under this view, an employee with access to information should be construed as having exceeded the scope of the

[105] *See* Booms, *supra* note 18, at 560.

[106] *See* P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, L.L.C., 428 F.3d 504, 510 (3d Cir. 2005) ("[T]he scope of [the CFAA's] reach has been expanded over the last two decades."); S. Rep. No. 104-357, 1996 WL 492169, at *7–8 (1996) ("[T]he proposed § 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer. . . . This [section] would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. . . . The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information.").

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

access she was originally given when she engages in improper, unauthorized, or otherwise disloyal "use" of such information in violation of the employer's computer policies. In such cases, the proper approach is to construe the employee's access as being "*unauthorized*," given that the employer did not "authorize" its employee to engage in an improper theft or misuse of that information.

The contrary view—as reflected in *WEC*—renders civil CFAA actions of dubious efficacy for use by employers because it prohibits them from using the CFAA to prevent the internal electronic theft of information unless the employer anticipated the theft in the first place (such as by limiting access at the outset of the employment relationship). This renders the CFAA limited in reach, remedying only cases of external hacking.

Most importantly, the reasoning behind the narrow view of the CFAA focuses on concerns about proper notice to a potential defendant facing criminal liability.[108] In the civil context, where the remedies available do not include loss of civil liberties, there is no similar policy concern that requires such a narrow construction. One possible way to "bridge the split" between the two circuits—either by Supreme Court intervention or by legislative amendment—would be to adopt the broader view of CFAA liability in the context of *civil claims*, while limiting *criminal liability* solely to those cases in which an individual is plainly not permitted to access certain information and nevertheless steals it via an act of computer hacking (either internal or external).

IV. Healing the Split: Why the Supreme Court Should Clarify the Scope of the CFAA

As noted above, the circuit split has exacerbated confusion over the scope of the CFAA and its effectiveness as a tool in cases involving disloyal employees. This confusion is problematic for employers who have to take additional measures to enforce their internal computer policies and to create more individualized policies for each employee. It also creates a notable lack of uniformity among the circuits in an important (and growing) area of the law. Moreover, in those jurisdictions taking a narrow approach to the CFAA, employers are effectively barred from pursuing a trade secret misappropriation action involving the theft of electronic trade secrets in a federal forum unless diversity jurisdiction is present.

The confusion over the scope and breadth of the CFAA has had serious implications beyond the employment arena. In January 2013, for example, Aaron Swartz, a twenty-six-year-old Internet activist who was being prosecuted under the CFAA for allegedly hacking into an online

[108] United States v. Nosal, 676 F.3d 854, 860–61 (9th Cir. 2012); *WEC*, 687 F.3d at 206.

academic database and downloading journal articles (not for economic gain), committed suicide on the eve of his trial.[109] His death prompted criticism, not only of the prosecutor who zealously pursued the charges under the CFAA, but also of the CFAA itself and its broad "unauthorized access" language; some even blamed Swartz's prosecution in part on the "extremely problematic" language of the CFAA.[110] In response, the House Judiciary Committee announced on January 24, 2013, that it intended to review the breadth of the CFAA, and Representative Zoe Lofgren (D-Cal.) proposed an amendment that would drastically narrow the scope of the CFAA.[111] Such criticism, however, ignored the fact that facing civil liability for an act has drastically different ramifications than does facing criminal liability, and the fair notice required to alert individuals to potential criminal liability is much higher than the notice required for potential civil liability.[112] Moreover, this recent criticism over the vague language of the statute arguably offered a perfect opportunity for the Supreme Court to clarify the scope of the phrase "unauthorized access" in both the civil and criminal contexts.

Any immediate hopes that the Supreme Court might resolve the circuit split were dashed on January 2, 2013, when the Court issued an order denying the petition for a writ of certiorari filed by WEC in the wake of the Fourth Circuit's ruling.[113] Thus, for the time being, the split will remain between those jurisdictions—like the Fourth and Ninth Circuits—that take a narrow approach to the meaning of "exceeds authorized access" and those jurisdictions—like the Fifth, Seventh, and Eleventh Circuits—that take a more expansive approach to the CFAA. As a result, it will be imperative for employers to create more individualized computer use restrictions in order to attempt to protect the viability of a CFAA claim in any jurisdiction.

[109] *See, e.g.*, Mike Scarcella, *Hacking Defendant's Suicide Spurs Debate over Prosecutors*, FULTON CNTY. DAILY REP., Jan. 16, 2013, at 9–10.

[110] *Id.*

[111] Juan Carlos Rodriguez, *House Will Review CFAA After Pioneer Swartz's Death*, LAW 360 (Jan. 23, 2013, 6:30 PM), http://www.law360.com/articles/409186.

[112] *See, e.g.*, Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498–99 (1982) ("The Court has . . . expressed greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe."); Barenblatt v. United States, 360 U.S. 109, 137 (1959) (Black, J., dissenting) ("For obvious reasons, the standard of certainty required in criminal statutes is more exacting than in noncriminal statutes. This is simply because it would be unthinkable to convict a man for violating a law he could not understand." (footnote omitted)).

[113] *See* WEC Carolina Energy Solutions, L.L.C. v. Miller, 133 S. Ct. 831 (2013) (denying cert.).

Conclusion

Unfortunately, so long as the circuit split remains, employers, practitioners, and courts alike will continue to lack guidance as to the scope of liability under the CFAA, particularly in cases of disloyal employees who violate computer use restrictions. It seems inevitable that the Supreme Court will again be asked to weigh in on the scope of the CFAA, perhaps when a circuit that is currently silent on this matter issues a ruling that aligns with the broader view of the CFAA. When that occurs, one can only hope that the Supreme Court will exercise its discretion and agree to step into the fray and resolve the circuit split. Until that time—at least in certain jurisdictions—an employer's computer use restrictions that merely prohibit disloyal use of electronic information will be insufficient to protect confidential electronic information from internal employee theft under the CFAA.