Cyber Law—Dismissing Employer's Claim Under the CFAA Against Former Employees Who Allegedly Misappropriated Trade Secrets—*WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013)

Among other things, the Computer Fraud and Abuse Act (CFAA) provides for civil and criminal penalties when a person, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer."[1] Employers have increasingly sought relief under the CFAA against errant employees who download confidential and proprietary information from the employer's network files for their own benefit or for the benefit of a competitor.[2] In *WEC Carolina Energy Solutions LLC v. Miller*,[3] the Fourth Circuit Court of Appeals determined whether WEC Carolina Energy Solutions LLC (WEC) could maintain a CFAA claim against former employees and a competitor who allegedly misappropriated WEC's proprietary information.[4] The Fourth Circuit affirmed the district court's dismissal of the CFAA claim, holding WEC failed to adequately allege that former employees accessed its confidential and proprietary information "without authorization" or "exceed[ed] authorized access" as required under the statute.[5]

WEC had employed Mike Miller as a project director.[6] Emily Kelley was his assistant.[7] While working for WEC, Miller was provided with a laptop computer, a cell phone, and authorization to access the company's intranet and computer servers, which stored confidential and proprietary trade secret

[1] *See* 18 U.S.C. § 1030(a)(2)(C) (2012) (outlining one of seven substantive offenses under CFAA). Pursuant to § 1030, a "protected computer" is defined, in part, as "a computer which is used in or affecting interstate or foreign commerce or communication . . . ." *Id.* § 1030(e)(2)(B). A civil action to obtain compensatory damages and injunctive relief may be instituted against a party in violation of § 1030 by any person who suffers damage or loss under the section, provided, however, that the offensive conduct comprises one of five factors, including loss to one or more persons aggregating at least $5,000 in value. *See id.* § 1030(c)(4)(A)(i)(I) , (g). Varying criminal penalties are also described under § 1030. *See id.* § 1030(c).

[2] *See* Molly Eichten, *The Computer Fraud and Abuse Act—A Survey of Recent Cases*, 66 BUS. LAW. 231, 231-32 (2010) (describing common fact pattern in recent cases brought under CFAA against employees); Scott R. McLaughlin & Walter M. Stella, *A Sword and Shield—The Computer Fraud and Abuse Act, and How Employers Can Protect Their Trade Secrets*, PRATT'S PRIVACY & DATA SECURITY L.J., Dec. 2006, at *1, *available at* WESTLAW, PRIVDSLJ 2006.12-2 (reporting increase in causes of action under CFAA).

[3] 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013).

[4] *See id.* at 202-03 (reviewing district court's dismissal of CFAA claim de novo).

[5] *See id.* at 206 (describing narrow reading of "without authorization" and "exceeds authorized access").

[6] *See id.* at 202.

[7] *See* 687 F.3d at 202.

information.[8] Miller resigned from WEC on April 30, 2010, and subsequently began working at Arc Energy Services, Inc. (Arc).[9] WEC suspected that prior to resigning, Miller, or Kelley acting on behalf of Miller, downloaded a substantial amount of WEC's confidential information and forwarded it to a personal e-mail address.[10] Additionally, WEC suspected that Miller used the downloaded information in a presentation on behalf of Arc shortly after resigning.[11]

In October 2010, WEC sued Miller, Kelley, and Arc in federal district court alleging violations of the CFAA and nine state law causes of action.[12] WEC claimed Miller's and Kelley's actions impaired the "integrity of its data, programs, systems or information," and that as a result, it suffered economic damages.[13] The defendants moved to dismiss the federal CFAA claim and the district court granted dismissal, finding that WEC failed to state a claim under which the CFAA provided relief.[14] On appeal, the Fourth Circuit affirmed the district court's dismissal of the CFAA claim.[15] By affirming, the Fourth Circuit adopted a narrow reading of the provisions of the CFAA, holding that an employee accesses a computer "without authorization" or "exceeds authorized access" only when the employee accesses a computer without permission, or

[8] *See id.* In an effort to protect its sensitive information, WEC maintained company policies prohibiting the use of its confidential and proprietary information without authorization, or downloading such information to a personal computer; however, these policies in no way restricted Miller's permission to access the information. *See id.*

[9] *See id.* WEC and Arc are competitors both principally located in York County, South Carolina. *See id.* at 201-02.

[10] *See id.* at 202. WEC also asserted that Miller and Kelley downloaded confidential information to a personal computer. *See id.*

[11] *See* 687 F.3d at 202 (noting Arc eventually awarded two projects).

[12] *See id.* WEC alleged three separate violations of the CFAA. *See id.* at 203 (explaining alleged violations of § 1030(a)(2)(C), (a)(4), (a)(5)(B)-(C)). In support of the CFAA claim, WEC averred that Miller and Kelley breached their fiduciary duties when they violated company policy on downloading confidential information, and that because of their breach they either lost or exceeded their authorization to access its confidential information. *See* 687 F.3d at 202. Arc's liability was premised on Miller and Kelley acting as its agents. *See id.* WEC's state law causes of action included conversion, tortious interference with contractual relations, civil conspiracy, and misappropriation of trade secrets. *See id.* at 207 n.4.

[13] *Id.* at 202.

[14] *See* 687 F.3d at 202; WEC Carolina Energy Solutions, LLC v. Miller, No. 0:10–cv–2775–CMC, 2011 WL 379458, at *7 (D.S.C. Feb. 3, 2011) (granting defendants' motion), *aff'd*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed* 133 S. Ct. 831 (2013). In reaching its conclusion, the district court reasoned that

> in this case, WEC's company policies regulated *use* of information not access to that information. Thus, even if Miller and Kelley's purpose in accessing the information was contrary to company policies regulating use, it would not establish a violation of company policies relevant to access and, consequently, would not support liability under the CFAA.

WEC Carolina Energy Solutions, LLC v. Miller, No. 0:10–cv–2775–CMC, 2011 WL 379458, at *5 (D.S.C. Feb. 3, 2011), *aff'd*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed* 133 S. Ct. 831 (2013).

[15] *See* 687 F.3d at 207.

obtains or alters information beyond their authorized level of access.[16]

Early prosecutions of computer-misuse crimes relied on traditional property law notions of theft.[17] The crime of theft, however, was poorly equipped to handle the proliferation of computer offenses where deprivation of property was lacking.[18] Unsatisfactory application of traditional property laws and the absence of specific computer-misuse legislation led to heightened congressional interest and the passage of the Counterfeit Access Device and Computer Fraud and Abuse Act in 1984.[19] The CFAA has since been amended numerous times, and its scope broadened to include both criminal and civil liability, as well as application to all computers used in or affecting commerce.[20]

[16] *See id.* at 204 (noting neither definition extended to improper use of confidential information otherwise validly accessed).

[17] *See* Lund v. Commonwealth, 232 S.E.2d 745, 748 (Va. 1977) (holding unauthorized computer access not subject to larceny statute); Ward v. Superior Court, 3 Computer L. Serv. Rep. (Callaghan) 206, 208 (Cal. Super. Ct. 1972) (transferring electronic computer impulses does not consummate theft).

[18] *Compare* United States v. Girard, 601 F.2d 69, 71 (2d Cir. 1979) (characterizing taking information from government computer files as conversion because files constituted "thing of value"), *and* United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (holding computer system constitutes property and requisite harm to company met), *with* United States v. Czubinski, 106 F.3d 1069, 1074 (1st Cir. 1997) (concluding deprivation of intangible property requires appreciable harm), *and* United States v. Collins, 56 F.3d 1416, 1421 (D.C. Cir. 1995) (per curiam) (concluding no serious interference with ownership rights from computer misuse). *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1607-13 (2003) (discussing historical use of property laws to address computer misuse).

[19] *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, §§ 2101-2103, 98 Stat. 1837, 2190 (codified as amended at 18 U.S.C. § 1030 (2012)) (establishing first federal computer-crime statute). In its original form, the CFAA made it a felony to access information in a computer without authorization, and a misdemeanor to access financial records, or to trespass into a government computer. *See id.; see also* H.R. REP. NO. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691 (acknowledging contemporaneous computer crime enforcement relying on laws designed for other offenses); JOSEPH B. TOMPKINS, J.R. ET AL., AM. BAR ASS'N TASK FORCE ON COMPUTER CRIME, REPORT ON COMPUTER CRIME 45-51 (1984) (advocating need for computer-crime legislation).

[20] *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 814, 115 Stat. 272, 382 (codified as amended at 18 U.S.C. § 1030 (2012)) (lowering amount of threshold damages needed to prove "loss"); Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX, 108 Stat. 2097 (codified as amended at 18 U.S.C. § 1030 (2012)) (providing civil liability for computer misuse); Computer Fraud and Abuse Act "18 USC 1001 note" of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)) (adding additional penalties for fraud and related computer-misuse activities). Through a series of amendments, the CFAA has been expanded to cover nearly all business, home, and laptop computers. *See* Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 U. PITT. J. TECH. L. & POL'Y 1, 3 (2012) (outlining expansion of CFAA coverage). All fifty states have also enacted computer-misuse statutes. *See, e.g.*, CAL. PENAL CODE § 502 (West 2013) (proscribing knowingly accessing computer system without permission); FLA. STAT. ANN. § 815.04 (West 2013) (prohibiting unauthorized access to trade secrets existing internal or external to computer); MASS. GEN. LAWS ANN. ch. 266, § 120F (West 2013) (knowing unauthorized access to computer punishable by imprisonment, fine, or both). Congress was concerned with the scope of the CFAA even in its early days. *See* S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.

> [T]he Committee has been especially concerned about the appropriate scope of Federal jurisdiction

Although the original focus of the CFAA was primarily to deter computer hacking, it has been increasingly used by employers against "employee-hackers" who access and use confidential information in an anticompetitive or fraudulent manner.[21] The CFAA is an attractive alternative (or complement) to state law claims because it creates a basis for federal jurisdiction, provides injunctive relief, and does not require an employer to prove that the information accessed was secret.[22] While there is little debate on the damage employers face as a result of employees' hacking activity, courts have struggled to both uniformly apply the CFAA in the employment context and to interpret key provisions of the statute—namely, when do employees access information "without authorization" or "exceed[] authorized access?"[23] Consequently, a circuit split has emerged.[24]

Courts broadly interpreting the CFAA have based employee violations on agency principles.[25] Other courts, unwilling to embrace an agency approach,

> in this area. . . . The Committee rejects this approach [to enact a sweeping Federal statute on computer crime] and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, . . . or where the crime itself is interstate in nature.

Id. Statutes comprising both criminal and civil applications, such as the CFAA, have generally been construed strictly, according to the rule of lenity. *See* United States v. Lanier, 520 U.S. 259, 266 (1997) (stating rule resolves statutory ambiguity by proscribing only clearly covered conduct).

[21] *See* Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003) ("Employers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."); S. REP. NO. 99-432, at 7, 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485, 2488 (explaining new subsections aimed at "outsiders"); *see also* A.V. v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009) (describing CFAA as primarily criminal statute aimed at hackers).

[22] *See* 18 U.S.C. § 1030(g) (2012) (providing for injunctive relief); Matthew Kapitanyan, *Beyond Wargames: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 J. L. & POL'Y FOR INFO. SOC'Y 405, 417-18 (2012) (considering employer benefit in bringing CFAA claim); Alan W. Nicgorski, *Employees Exceeding Authorized Access? Trends in Interpreting the Computer Fraud and Abuse Act,* 30 WESTLAW J. COMPUTER & INTERNET 1, 1 (2013), *available at* WESTLAW, 30 No. 18 WJCOMPI 1 (describing advantages of seeking relief under CFAA).

[23] *See* Robert C. Kain, *Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, but Illegal in Miami, Dallas, Chicago, and Boston*, FLA. B.J, Jan. 2013, at 36, 36 (explaining circuit split revolves around interpretation of "exceed[] authorized access"); Nicgorski, *supra* note 22, at 1 (noting varying judicial interpretations of authorization phrases in CFAA).

[24] *See* 687 F.3d at 207 (rejecting theory of CFAA liability based on violation of use policy); United States v. Nosal, 676 F.3d 854, 863-64 (9th Cir. 2012) (en banc) (holding CFAA violation hinges on restrictions to access not use). Other circuits have held that violating an employer's policy can be considered "exceeding authorized access." *See* United States v. Rodriguez, 628 F.3d 1258, 1263-64 (11th Cir. 2010) (obtaining information contrary to use policy results in exceeding authorized access); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (concluding "authorized access" encompasses limits on use of information obtained with permitted access to system). Still, other circuits have not resolved the issue and have instead relied on agency principles. *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (breaching duty of loyalty terminates agency relationship and rescinds authorized access); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001) (opining contract terms may provide parameters of authorized access).

[25] *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (holding termination of

have determined that employers can define the limits of employee authorized access through company policies and other employment contracts.[26] Finally, courts reluctant to extend CFAA liability to employees have adopted a narrow interpretation of the key statutory provisions, finding violations only in instances where initial access to information was not permitted.[27] This conflict has left employers with different remedies in different jurisdictions, and has led to much academic debate over which interpretation of the CFAA most closely follows Congress's intent.[28] However, a clear trend is emerging towards adopting the narrower interpretation of the statute, making it difficult for employers to succeed on such claims.[29] Furthermore, Congress has introduced legislation to amend the CFAA, which is colloquially referred to as "Aaron's Law Act," attempting to codify the more narrow interpretation of the statute.[30]

In *WEC Carolina Energy Solutions LLC v. Miller*, the Fourth Circuit

agency relationship similarly terminates access to computer); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (concluding authority ends when employee allegedly becomes agent for new employer). These courts have reasoned that when an employee accesses a protected computer and uses the information in a way that is adverse to the employer, the employee breaches their duty of loyalty, terminates the agency relationship with the employer, and loses their authorized access to such information. *See* Int'l Aiport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) ("Citrin's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship.").

[26] *See* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (concluding CFFA violations may result when employee violates computer-use policy to further criminal scheme); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-82 (1st Cir. 2001) (concluding confidentiality agreement can limit parameters of authorized access).

[27] *See* 687 F.3d at 206 (adopting narrow interpretation of statute); United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (holding CFAA liability does not extend to violations of use restrictions); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (finding no violation where employee entitled to access information).

[28] *See* Goldman, *supra* note 20, at 37-38 (recommending "plain meaning" approach in interpreting CFAA); Kerr, *supra* note 18, at 1668 (suggesting correction to expansive interpretations found by reviewing mechanics of existing crimes); Andrew T. Hernacki, Comment, *A Vague Law in a Smartphone World: Limiting the Scope of Unathorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1583 (2012) (suggesting liability only in traditional hacking cases); David J. Rosen, Note, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access,"* 27 BERKELEY TECH. L.J. 737, 766 (2012) (advocating rejection of employer-policy based approach to interpreting statute).

[29] *See, e.g.,* Dresser-Rand Co. v. Jones, No. 10-2031, 2013 WL 3810859, at *5 (E.D. Pa. July 23, 2013) (finding narrow interpretation of CFAA true to plain language of statute and congressional intent); Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc., No. CV413-55, 2013 WL 3422779, at *8 (S.D. Ga. June 28, 2013) (concluding CFAA provides for liability only where employee exceeds authorized access or lacks initial authorization); Advanced Micro Devices, Inc. v. Feldstein, No. 13-40007-TSH, 2013 WL 2666746, at *5 (D. Mass. June 10, 2013) (distinguishing *EF Cultural* and reasoning narrow interpretation of statute preferred); Wentworth-Douglas Hosp. v. Young & Novis Prof'l Ass'n, No. 10-cv-120-SM, 2012 WL 2522963, at *3 (D.N.H. June 29, 2012) (distinguishing *EF Cultural* and interpreting statutory phrase "exceeds authorized access" narrowly); Sebrite Agency, Inc. v. Platt, 884 F. Supp. 2d 912, 917-18 (D. Minn. 2012) (endorsing narrow interpretation of CFAA and reasoning such interpretation maintains consistency with rule of lenity).

[30] *See* Aaron's Law Act of 2013, H.R. 2454, 113th Cong. § 2(a) (2013) (striking term "exceeds authorized access" and adding statutory definition for "access without authorization"); Aaron's Law Act of 2013, S. 1196, 113th Cong. § 2(a) (2013) (introducing companion legislation in Senate).

decided, as a matter of first impression, whether an employer could maintain a CFAA claim against former employees who downloaded and used confidential information in violation of the employer's policies.[31] The court reviewed the divergent interpretations of the statute by its sister circuits and agreed with the literal and narrow approach promulgated by the Ninth Circuit in *United States v. Nosal*.[32] In support of this approach, the court recognized that the CFAA provided for both criminal and civil penalties, thus necessitating observation of the rule of lenity.[33] Additionally, in reviewing the ordinary meaning of the terms "without authorization" and "exceeds authorized access" the court noted that neither definition extends to offensive use of information otherwise validly accessed.[34]

In furtherance of its holding, the court declined to adopt an interpretation of the conjunction "so"—as used in the definition of the term "exceeds authorized access"—to mean "in that manner," reasoning that such an interpretation would impute CFAA liability to employees who violate use policies despite commendable intentions.[35] Moreover, the court expressly rejected a theory of employee liability under the CFAA premised on cessation of agency.[36] The court acknowledged that its holding would "disappoint" employers and that Miller and Kelley may very well have misappropriated WEC's confidential information; however, the court was reluctant to disregard congressional intent by adopting an interpretation of the CFAA that could extend to rather innocuous uses of computers and information.[37]

In light of the CFAA having both criminal and civil penalties, the Fourth Circuit properly followed the rule of lenity and adopted a narrow construction

[31] *See* 687 F.3d at 203 (reviewing district court's dismissal of CFAA claim). "We particularly examine whether these terms ["without authorization" and "exceeds authorized access"] extend to violations of policies regarding the use of a computer or information on a computer to which a defendant otherwise has access." *Id.*

[32] *See id.* (recalling narrow interpretation of statute in *Nosal*); United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (holding employees exceeding authorization do not violate CFAA when downloading information and transferring to competitor).

[33] *See* 687 F.3d at 203-04 (giving ordinary meaning to words absent different indication from Congress); *see also* United States v. Lanier, 520 U.S. 259, 266 (1997) (setting forth canon of strict construction of criminal statutes); *supra* note 20 (noting civil liability under CFAA not present until 1994 amendment).

[34] *See* 687 F.3d at 204.

[35] *See id.* at 205-06. As an illustration, the court noted that if an employee downloaded confidential information to a personal computer in violation of a company use policy so that he could conduct work for the employer over the weekend, the employee could be subject to CFAA liability with such interpretation of the conjunction "so." *See id.* at 206.

[36] *See id.* at 206. Although the court recognized the Seventh Circuit's application of the agency-based theory extended to clearly egregious employee behavior, it cautioned that such an approach may result in violations Congress did not intend. *See id.*

[37] *See* 687 F.3d at 207. "[W]e are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy." *Id.*

of the statute.[38] Despite employers bringing claims with increased frequency, the CFAA remains a predominantly criminal statute focused on deterring hackers from accessing protected computers.[39] Given a choice between the differing approaches to statutory interpretation among the sister circuits, the Ninth Circuit's approach represents the narrowest construction.[40]

Nonetheless, the approach approved in *Nosal*, and adopted in *Miller* by the Fourth Circuit, yields ambiguity insofar as the remaining relevance of the term "exceeds authorized access."[41] The narrow interpretation hinges on whether the employee was ever permitted access to the confidential information, and dispenses with the notion that employees can exceed their authorized access when using the confidential information in a way that violates company policy.[42] Thus, the narrow construction of the statute does not appear to regulate employees who exceed their authorization in any way, but rather only applies to employees lacking any access.[43] The cessation-of-agency approach directly addresses this concern by subjecting employees to liability any time they breach the duty of loyalty and use the confidential information in a way that is adverse to the employer.[44] Yet, what cessation-of-agency liability theory makes up for in regards to the narrow approach, it loses from a statutory vagueness perspective because this approach does not provide clear notice to employees of when they will be subject to liability.[45]

With notable shortcomings to each of the existing methods of interpreting the CFAA, it is imperative that either the Supreme Court or Congress take action to further clarify the scope and parameters of liability under the statute in

[38] *See id.* at 203-04 (following strict construction of criminal statute); *see also* United States v. Lanier, 520 U.S. 259, 266 (1997) (requiring "strict construction of criminal statutes"); United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc) (fearing expansive interpretation would criminalize "minor dalliances").

[39] *See* S. REP. NO. 99-432, at 7-8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484-86, 2488 (1986) (stating amendments aimed at "outsiders"); *supra* note 21 and accompanying text (conveying original intent of CFAA articulated in legislative history).

[40] *See* 687 F.3d at 203 (acknowledging Ninth Circuit's narrow interpretation of statute); Kain, *supra* note 23, at 36-37 (describing Ninth Circuit's narrow interpretation of CFAA in *Nosal*).

[41] *See* Goldman, *supra* note 20, at 13-14 (suggesting plain language interpretation offers incomplete resolution of CFAA claims); Rosen, *supra* note 28, at 748-49 (arguing uncertain application of phrase "exceeds authorized access" remains with narrow code-based approach).

[42] *See* 687 F.3d at 205 (admitting interpretation of CFAA fails to mandate liability for violating use policy); Goldman, *supra* note 20, at 23-25 (describing shortcomings of plain meaning approach); Rosen, *supra* note 28, at 748-49 (arguing narrow interpretation reads phrase "exceeds authorized access" out of statute).

[43] *See* 687 F.3d at 204 (noting interpretations of key provisions do not extend to improper uses of information validly accessed); Goldman, *supra* note 20, at 24-25 (arguing narrow interpretation fails to proscribe fraudulent behavior Congress intended statute to cover).

[44] *See* Nicgorski, *supra* note 22, at 2 (noting agency approach supports liability any time employee acts contrary to employer interests).

[45] *See* Kerr, *supra* note 18, at 1633-34 (arguing agency theory of liability strikingly broad); Rosen, *supra* note 28, at 750-52 (suggesting agency approach frustrates congressional intent with respect to CFAA).

the employment context.[46] Congress has been quick to amend the CFAA in an attempt to keep pace with the proliferation of computer-misuse crimes and is perhaps in the best position to provide a resolution, especially considering that pending legislation to amend the CFAA is already being circulated.[47] Until the High Court rules on the matter or new legislation is adopted, however, employers will need to assume the responsibility of clearly defining the scope of employee access to confidential information through policy or contract, and continue to pursue employee violations through existing state law remedies.[48]

In *WEC Carolina Energy Solutions LLC v. Miller*, the Fourth Circuit Court of Appeals determined whether an employer could maintain a federal CFAA claim against former employees who violated company policies regarding the use of computers and confidential information. Acknowledging that its interpretation applied uniformly to the criminal and civil provisions of the statute, the court correctly followed the rule of lenity by adopting a narrow construction of the key provisions "without authorization" and "exceeds authorized access." However, questions remain as to whether the Fourth Circuit's approach functionally excludes from liability employees who exceed their authorized access through violations of employer policies. Considering the current circuit split, and the shortcomings of the varying approaches to interpreting the CFAA adopted by the courts, it is prudent for Congress to properly articulate and clarify its intentions regarding employee liability under the CFAA.

Abbey P. Coffin

[46] *See* Nicgorski, *supra* note 22, at 5 (acknowledging CFAA interpretation discord ripe issue for Supreme Court); *see also supra* note 24 and accompanying text (describing circuit split present in interpreting CFAA in employment context).

[47] *See supra* note 20 and accompanying text (outlining series of legislative amendments to CFAA); *see also supra* note 30 and accompany text (describing legislation: striking "exceeds authorized access" from CFAA and instituting definition for "access without authorization").

[48] *See* Eichten, *supra* note 2, at 236 (recommending reexamining policies in light of continued controversy in interpreting CFAA); McLaughlin & Stella, *supra* note 2, at *8 (suggesting employers be proactive by including restrictive provisions in employment agreements); *see also* 687 F.3d at 207 n.4 (acknowledging adequate remedies available under state law).