American University Law Review

Volume 62 | Issue 5

Article 9

2013

Reining in the Rogue Employee: The Fourth Circuit Limits Employee Liability under the CFAA

Danielle E. Sunberg
American University Washington College of Law

Recommended Citation

Sunberg, Danielle E. "Reining in the Rogue Employee: The Fourth Circuit Limits Employee Liability under the CFAA." American University Law Review 62, no.5 (2013): 1416-1439.

Reining in the Rogue Employee: The Fourth Circuit Limits Employee Liability under the CFAA

Keywords

America the Virtual: Security, Privacy, and Interoperability in an Interconnected World, United States. Court of Appeals (4th Circuit), United States. Congress, Ambiguity, Labor laws & legislation -- United States, Liability (Law) -- United States, Computer fraud -- Law & legislation, Actions & defenses (Law) -- United States, Statutes -- United States -- States

REINING IN THE ROGUE EMPLOYEE: THE FOURTH CIRCUIT LIMITS EMPLOYEE LIABILITY UNDER THE CFAA

DANIELLE E. SUNBERG[*]

The Fourth Circuit's opinion in WEC Carolina Energy LLC v. Miller *reflects a growing trend among the courts to adopt a narrow code approach to employee liability under the Computer Fraud and Abuse Act. The case exacerbates the existing circuit split and reinforces the need for reconciling when an employee accesses a computer "without authorization." While resolution from the judiciary remains remote, Congress is engaged in a lively debate over the proper interpretation of the term "without authorization." Recent legislative proposals suggest that Congress has united in support of limiting liability for unauthorized access under the CFAA to the circumvention of technological barriers. Support for this restrictive interpretation signifies that until the ambiguity in the law is clarified, future undecided courts should follow in the Fourth Circuit's footsteps and adopt the code approach to determine employee liability under the CFAA.*

TABLE OF CONTENTS

[*] Senior Federal Circuit Editor, Volume 62, *American University Law Review*. J.D. Candidate, May 2013, *American University Washington College of Law*; B.A., Politics and American Studies, 2009, *Brandeis University*. My sincere thanks goes to Brian Shearer, Estefania San Juan, Meghan Quinn, Emily Gianetta, Giulia di Marzo, and the *American University Law Review* staff for their meticulous efforts and assistance in perfecting this Note. Above all else, I am immensely grateful for my family's authorization to access their unconditional support, guidance, and encouragement.

INTRODUCTION

On January 2, 2013, the Supreme Court dismissed the petition for writ of certiorari in *WEC Carolina Energy Solutions LLC v. Miller*,[1] leaving unresolved the vexing question of employee liability under the Computer Fraud and Abuse Act[2] (CFAA). The case involved Mike Miller, former Project Director for WEC Carolina Energy Solutions (WEC), who used WEC's proprietary information to benefit a competing business.[3] WEC permitted Miller to access the company's confidential and trade secret documents stored on his employer-provided laptop computer.[4] On April 30, 2010, only twenty days after resigning from his position with WEC, Miller used the confidential information to make a pitch to a potential client on behalf of a competitor, Arc Energy Services, Inc. (Arc).[5] Arc won the client's business, and WEC sued Miller and another participating colleague, asserting nine state-law charges as well as several violations of the CFAA.[6]

The CFAA, codified at 18 U.S.C. § 1030, is the nation's first and leading cybercrime statute. The statute grants employers a private right of action to hold employees liable for accessing a company computer "without authorization" or for "exceeding authorized access."[7] Penalizing this conduct grows more imperative: a 2009 study conducted by the Ponemon Institute revealed that six out of every ten departing employees steal company data and described this figure as a growing problem of "malicious insiders."[8] Unsurprisingly, following this expansion in the computer

[1] 133 S. Ct. 831 (2013) (dismissing the petition pursuant to Supreme Court Rule 46.1, which requires dismissal when all parties file an agreement to dismiss the case), *dismissing cert. from* 687 F.3d 199 (4th Cir. 2012).

[2] 18 U.S.C. § 1030 (2006 & Supp. V 2012)).

[3] *WEC*, 687 F.3d at 201, *cert. dismissed*, 133 S. Ct. 831.

[4] *Id.* at 202.

[5] *Id.*

[6] *Id.*

[7] 18 U.S.C. § 1030(a)(1)–(2), (4), (g) (2006 & Supp. V 2012).

[8] *See* Brian Krebs, *Data Theft Common by Departing Employees*, WASH. POST (Feb. 26, 2009, 12: 15 PM), http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html (reporting that the most frequently taken information includes e-mail lists, non-financial business data, customer contact lists, and employee records); Maggie Shiels, *Workers 'Stealing Company Data,'* BBC NEWS (Feb. 23, 2009, 2:12 PM), http://news.bbc.co.uk/2/hi/technology/7902989.stm (suggesting that malicious

protection statute, employers have increasingly used the CFAA as a means to hold rogue employees accountable for using information obtained from a company computer in a manner that conflicts with the employer's interests.

WEC attempted to hold Miller liable under the CFAA precisely for his misuse of the company's confidential data.[9] The Fourth Circuit affirmed that WEC failed to file a viable claim under the CFAA because WEC did not "allege that Miller . . . accessed a computer or information on a computer *without authorization*."[10] This decision exacerbates the existing circuit split with respect to applying the CFAA to the employer-employee context. The Fourth Circuit aligns itself with the Ninth Circuit, which has adopted the narrow code approach to interpreting employee liability under the CFAA.[11] In contrast, the Fifth, Seventh, and Eleventh Circuits have embraced a broader and more employer-friendly approach.[12] The widening division among the circuits creates enormous problems for employers, as the CFAA's mandate directly affects what types of employee actions are culpable and what computer authorization protections the employer must implement to protect against intellectual property theft. Many scholars and commentators hoped that the Supreme Court would grant writ of certiorari to hear *WEC* and thus provide guidance to employers and unify the courts.[13] Such resolution, however, remains elusive—on January 2, 2013,

insiders are motivated to steal the information for a variety of reasons, including "to get a new job, start their own businesses or for revenge"); *see also* Kevin Parrish, *Ex-Intel Employee Jailed for Stealing Company Secrets*, TOM'S HARDWARE (Aug. 9, 2012, 5:20 PM), http://www.tomshardware.com/news/Biswamohan-Pani-Intel-AMD-Prison-FBI,16771.html (recounting the case of a former Intel employee who was sentenced to three years in prison and two years of probation, as well as given a $17,500 fine, for downloading company secrets worth an estimated $200 to $400 million).

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

[10] *Id.* at 207 (emphasis added).

[11] *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (interpreting the CFAA's "exceeds authorized access" language narrowly to encompass only improper access to information, not violations of use restriction); *see also infra* Part I.B.3 (describing the narrow, pro-employee code approach).

[12] *See* United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010) (finding that a Social Security Administration employee exceeded his authorized access when he violated the Administration's computer-use policy by using databases for non-business purposes), *cert. denied*, 131 S. Ct. 2166 (2011); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (affirming that the employee's authorization did not extend to using the accessed information to perpetrate a fraud), *cert. denied*, 133 S. Ct 1237 (2013); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (finding that the employee's authorization automatically terminated when he breached his duty of loyalty and his agency relationship with the company).

[13] *See* Russell Beck, *CFAA: The Wait for the Supreme Court Continues*, FAIR COMPETITION L. (Jan. 6, 2013), http://faircompetitionlaw.com/2013/01/06/cfaa-the-wait-for-the-supreme-court-continues (expressing disappointment that WEC's petition for writ of certiorari was dismissed and hoping that another case will soon afford the Supreme Court an opportunity to resolve the circuit split); Orin Kerr, *Thoughts on the Oral Arguments in* United States v. Nosal, VOLOKH CONSPIRACY (Dec. 19, 2011, 12:46 AM), http://www.volokh.com/2011/12/19/thoughts-on-the-oral-arguments-in-united-states-v-

the Court dismissed WEC's petition for certiorari.[14] In the midst of the jurisprudential confusion, Congress seeks to amend the CFAA to mitigate some of the statutory interpretation issues at the heart of the circuit split.[15]

In the wake of the Supreme Court's dismissal of *WEC*, this Note explores the deepening circuit split that has engulfed the debate over employee liability under the CFAA as well as the potential future developments of the CFAA. Part I of this Note follows the development of the CFAA and the divergence among the courts' approaches to interpreting "without authorization." Part II discusses the practical implications of the Fourth Circuit's decision in *WEC* on employers who seek to hold rogue employees accountable. Part III compares the multiple congressional attempts to reconcile the ambiguity in the statute and argues that despite Congress's inability to enact an amendment, the legislative proposals indicate that Congress has endorsed the Fourth Circuit's narrow code approach to interpreting employee liability under the CFAA.

I. BACKGROUND

Until the 1980s, the United States had no specific federal legislation addressing cybersecurity and computer crimes.[16] In 1984, Congress addressed the growing integration of computers into everyday life and the increasingly critical component they played in national security, financial transactions, and information sharing by passing the Comprehensive Crime Control Act, the first iteration of the CFAA.[17] Since its enactment,

nosal/ (asserting that the issue of whether the CFAA criminalizes violations of use policies has "caused so much uncertainty in the lower courts" that Supreme Court review may be justified unless Congress steps in to clarify the definition of "exceeds authorized access"); Thomas O'Toole, *Cyberlaw Predictions: High Court Dismissal of* WEC Carolina Energy Solutions *Petition Will Sting*, BLOOMBERG BNA (Jan. 4, 2013), http://www.bna.com/cyberlaw-predictions-high-b17179871695/ (noting that the Court's petition dismissal "dashed the hopes" of a number of expert attorneys eager for a circuit split resolution).

[14] WEC Carolina Energy Solutions LLC v. Miller, 133 S. Ct. 831 (2013), *dismissing cert. from* 687 F.3d 199.

[15] *See* Cyber Crime Protection Security Act, S. 2111, 112th Cong. § 8 (2012) (proposing to expressly exclude from CFAA liability any access violating a non-governmental employer's acceptable use policy if it is the sole basis for the unauthorized access allegation); REP. ZOE LOFGREN, 113TH CONG., AARON'S LAW MODIFIED DRAFT § 2 (2013), *available at* http://lofgren.house.gov/images/stories/pdf/aarons%20law%20revised%20draft%20013013.pdf (proposing to amend the CFAA by excluding violations of employer use policies from the meaning of "access without authorization" and by removing the "exceeds authorized access" language altogether).

[16] Matthew Kapitanyan, *Beyond* WarGames*: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 405, 409 (2012); *see* Obie Okuh, Comment, *When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access*, 21 ALB. L.J. SCI. & TECH. 637, 647 (2011) ("Prior to 1984, Congress and the courts had relied on mail-and-wire fraud statutes to combat computer crimes, but this proved to be an inadequate mechanism . . . .").

[17] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L.

Congress has amended the CFAA several times in an attempt to expand its mandate, incorporating criminal and civil penalties for improper access to both government and private computers.[18] Despite the multiple rounds of amendments and modifications, the CFAA continues to be plagued by statutory interpretation and constitutional vagueness concerns.[19]

A. Development of the CFAA

Congress enacted the initial version of the CFAA in 1984, which included the original mandate for law enforcement to protect against computer hackers attempting to infiltrate and obtain national security information, sensitive information contained in financial records, or access a government computer.[20] Legislative history reveals that the House enacted the provision because "traditional theft/larceny statutes [we]re not the proper vehicle to control the spate of computer abuse and computer assisted crimes."[21] Although a substantial step, enforcing only these limited crimes did not provide a comprehensive statute for cybercrime prosecution.

Congress's narrow focus in its first endeavor to criminalize computer crimes has led to multiple amendments addressing the increasing scope of cybercrimes, creating "one of the most far-reaching criminal laws in the United States Code."[22] In 1986, Congress overhauled the statute and added three new felony offenses.[23] Similar to the traditional crime of wire fraud,

No. 98-473, §§ 2102–2103, 98 Stat. 2190, 2190–92 (codified as amended at 18 U.S.C. § 1030 (2006 & Supp. V 2012)); *see* H.R. REP. NO. 98-894, at 8 (1984) (attributing the passage of the statute to the ubiquity of computers in both the private and public sectors and the surge of crimes committed electronically).

[18] *See, e.g.*, Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified as amended in scattered sections of 18 U.S.C.) (expanding coverage from only federal interest computers to any protected computers); 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 (2006 & Supp. V 2012)).

[19] *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1572, 1574 (2010) (emphasizing that the CFAA's expansion has led to vagueness challenges that the statute neither gives fair notice to citizens about what conduct is prohibited, nor "establish[es] minimal guidelines to govern law enforcement"); Andrew T. Hernacki, Comment, *A Vague Law in A Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1563 (2012) (arguing that the vagueness challenges arise from the unsettled definitions of "authorization" and "access"); Letter from Laura W. Murphy, Dir., Wash. Legislative Office, ACLU, et al., to Senate Judiciary Comm. (Sept. 21, 2011), *available at* https://www.cdt.org/files/pdfs/CFAA_signon_ltr_2.pdf ("Our primary concern—that this will lead to overbroad application of the law—is far from hypothetical.").

[20] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–91 (codified as amended at 18 U.S.C. § 1030(a)(1)–(3) (2006 & Supp. V 2012)). The statute was renamed the CFAA in 1986. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213.

[21] H.R. REP. NO. 98-894, at 9 (1984).

[22] Kerr, *supra* note 19, at 1561.

[23] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(d), 100 Stat. 1213, 1213–

§ 1030(a)(4) criminalizes unauthorized access with intent to defraud.[24] The second felony, codified at § 1030(a)(5), prohibits altering, damaging, or destroying another's data without authorization.[25] The third addition is subsection 1030(a)(6), which criminalizes tracking computer passwords.[26] In addition, the Computer Abuse Amendments Act of 1994 amended the CFAA by providing a private right of action in § 1030(g) for victims of CFAA offenses to recover damages in a civil suit.[27]

Liability under the CFAA requires a person to violate one of the enumerated offenses by accessing a computer either "without authorization" or by "exceeding authorized access."[28] While Congress has not provided a definition for "without authorization," it has clarified that "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[29] The purposeful inclusion of the two distinct phrases in different sections of the CFAA indicates that Congress intended to target different groups of people.[30] Those "without authorization" are non-employee "outsiders"

14 (codified as amended at 18 U.S.C. § 1030(a)(4)–(6) (2006 & Supp. V 2012)).

[24] 18 U.S.C. § 1030(a)(4) (2006) ("Whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . . shall be punished . . . .").

[25] *Id.* § 1030(a)(5)(A) (Supp. V 2012) ("Whoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished . . . .").

[26] *Id.* § 1030(a)(6) ("[K]nowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States . . . .").

[27] Pub. L. No. 103-322, tit. XXIX, 108 Stat. 2097 (codified as amended at 18 U.S.C. § 1030 (2006 & Supp. V 2012)). Also notable is the expansion of "protected computers" under the PATRIOT ACT of 2001 and the Identity Theft Enforcement and Restitution Act of 2008 to include virtually all computers. Pub. L. No. 110-326, tit. II, 122 Stat. 3560 (codified in 18 U.S.C. §§ 1030, 2332b, 3663 (2006 & Supp. V 2012)); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.).

[28] 18 U.S.C. § 1030(a)(1)–(6) (2006 & Supp. V 2012).

[29] 18 U.S.C. § 1030(e)(6) (2006). The amendment also provided that access must be knowing or intentional, indicating that negligent or accidental access is not actionable under the CFAA. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(a), 100 Stat. 1213, 1213; *see* Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 172–73 & n.252 (2011) (stating that accidental or mistaken access does not violate the CFAA and providing the example of a case in which the defendant's unauthorized but "mistaken origination of the plaintiff's bank account" did not constitute a CFAA violation).

[30] *See* United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (reasoning that if the phrases refer to two separate groups of hackers—as opposed to one referring to

who hack into the computer, whereas those who "exceed authorized access" are considered employee "insiders" who are permitted to use or access the computer to a certain extent.[31]

Although Congress originally considered "insiders" and "outsiders" from the perspective of protecting national security secrets and not in the employer-employee context, the distinction directly translates to the rogue employee scenario that has become increasingly common in CFAA lawsuits.[32] Despite Congress's clear intentions to target different groups of people through these terms, significant litigation has arisen from confusion over the definition and scope of employee "authorization."[33] The following section provides an overview of the deepening circuit split that has resulted from this confusion.

B. Approaches to Employee Liability Under the CFAA

Over the last decade, the circuit courts have diverged in their approach to balancing employees' rights and obligations granted by their authorization with protecting employers' confidential information, resulting in a three-way circuit split. Depending on which one of the three developed theories a court adopts, the definition of "without authorization" shifts to benefit either the employee or the employer. Consequently, the jurisdiction in which the employer chooses to file suit influences who will likely prevail, and thereby encourages forum shopping.[34]

hackers and the other referring to people who misuse accessed information—the focus of the CFAA properly remains on hacking "rather than turning it into a sweeping Internet-policing mandate").

[31] *Id.*; *see* United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (explaining that Congress "condition[ed] the nature of the intrusion in part on the level of authorization a computer user possesses" and specifically aimed § 1030(a)(3) and (a)(5) at outsiders and § 1030(a)(1), (a)(2), and (a)(4) at both insiders and outsiders (citing S. REP. NO. 104-357, at 11 (1996); S. REP. NO. 99-432, at 10 (1986))).

[32] ROBERT B. FITZPATRICK, COMPUTER FRAUD AND ABUSE ACT: CURRENT DEVELOPMENTS 1 (2010), *available at* http://www.robertbfitzpatrick.com/papers/cfaa CurrentDevelopments.pdf (noting that the increased use of the CFAA in the employment context was made possible by the Act's sweeping definition of "protected computer," which could arguably encompass any computer that is connected to the internet and owned by an employer); *see also* Douglas A. Winthrop, *How Broad is the Reach of the Computer Fraud and Abuse Act? The Circuits Diverge, in* INTELLECTUAL PROPERTY LAW 2013: TOP LAWYERS ON TRENDS AND KEY STRATEGIES FOR THE UPCOMING YEAR 121 (2013).

[33] *See* Tuma, *supra* note 29, at 178–82 (reviewing the nuanced approaches the courts of appeals for the First, Fifth, Eleventh, and Ninth Circuits have taken on the "authorization" issue).

[34] *See* Alan Nicgorski, *Employees Exceeding Authorized Access? Trends in Interpreting the Computer Fraud and Abuse Act*, WESTLAW J. COMPUTER & INTERNET, Feb. 8, 2013, at 1, 5–6 (discussing lessons for employers when seeking redress against employees); Winthrop, *supra* note 32, at 121.

1. Pro-employer: Agency approach

The agency approach to interpreting employee liability under the CFAA embodies the notion that the authorization is defined by the employee's use of information.[35] The Seventh Circuit adopted and solidified this approach in the civil suit, *International Airport Centers, LLC v. Citrin*.[36] *Citrin* involved an employee-defendant who deleted an enormous amount of data from his company's computer and subsequently went into business for himself in breach of his employment contract.[37] Instead of focusing on whether Citrin had permission to access the computer, the court focused on Citrin's motivation to delete the files. While recognizing that "[t]he difference between 'without authorization' and 'exceeding authorized access' is paper thin," Judge Posner pronounced that Citrin's authorization automatically terminated when he decided to go into business for himself and "resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty."[38] By considering Citrin's motivation, the court adopted a permissive and broad interpretation of "authorization" that advantages the employer.

Citrin was sued by his employer under § 1030(a)(5), which is violated when a person "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage *without authorization*."[39] To trigger liability in a section aimed solely at non-employee "outsiders," the court needed to characterize Citrin's actions in a manner that terminated his authorization. Focusing on legislative intent, Judge Posner pointed to Congress's concern with attacks by both hackers and "disgruntled programmers who decide to trash the employer's data system on the way out."[40] In an attempt to reconcile the apparent conflict that Congress characterized employees as "insiders" who "exceed authorized access" while targeting solely those "without authorization" in § 1030(a)(5), the Seventh Circuit adopted the broad agency approach.[41] The far-reaching interpretation of "without

[35] *See* Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (asserting that the employee's purpose to misuse the information constituted a breach of the duty of loyalty, which terminated the agency relationship between the employee and the employer, and in turn ended the employee's authorization to access that information, even though he had previously been authorized to access it while still in the agency relationship).

[36] 440 F.3d 418 (7th Cir. 2006).

[37] *Id.* at 419 (explaining that the employee, Citrin, not only deleted the files from the computer, but also uploaded a "secure-erasure program" to overwrite the deleted files, thereby preventing his employer from recovering them).

[38] *Id.* at 420; *see* RESTATEMENT (THIRD) OF AGENCY § 8.01 (2006) (outlining the duty of loyalty in agency law requiring agents to act in the interests of the principal).

[39] 18 U.S.C. § 1030(a)(5)(A) (Supp. V 2012) (emphasis added).

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

[41] *Id.*; *see* RESTATEMENT (SECOND) OF AGENCY § 112 (1958) ("Unless otherwise

authorization" allowed the court to hold accountable a rogue employee who misused the information he was permitted to access and severely damaged his employer.[42]

2. *Pro-employer: Contract approach*

The First, Fifth, and Eleventh Circuits have adopted the contract approach to interpreting "without authorization" under the CFAA. Under the contract approach, an employer can restrict the employee's authorization to access a computer through an employer-employee agreement or policy, such as an employment, confidentiality, or terms of service (TOS) agreement.[43] Therefore, any information obtained from a computer that exceeds the scope of the agreements thereby exceeds or terminates the employee's authorization under the CFAA.[44]

Courts have applied the contract approach in a similar manner as the agency theory; thus, they are sometimes characterized as a singular approach.[45] Opposite from the narrow and more employee-friendly code approach, which ignores the employee's motivation to access computer information,[46] both the agency and contract approaches focus on the purpose for using the information and whether the employer has proscribed such use. For example, the First Circuit in *EF Cultural Travel BV v. Explorica, Inc.*[47] held that disclosure of proprietary information, a breach of

agreed, the authority of an 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.").

[42] Only the Seventh Circuit has adopted the agency approach, although district courts in other circuits have applied the theory. Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PITT. J. TECH. L. & POL'Y 1, 6 & nn.27–28 (2012) (citing examples of cases following the broad approach); *see, e.g.*, Am. Family Mut. Ins. Co. v. Hollander, No. C 08-1039, 2010 WL 2851639, at *2 (N.D. Iowa July 20, 2010) (concluding, without explanation, that misusing information in a manner contrary to an employer's interests can constitute either access without authorization or access exceeding that which was authorized); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 45–46 (D. Mass. 2009) (denying defendant's motion to dismiss because First Circuit precedent favors the broader agency approach to interpreting "without authorization" and "exceeding authorized access); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1057–58 (S.D. Iowa 2009) (adopting the broad view based on the plain text and legislative history of the CFAA and because this view best distinguishes between "exceeds authorized access" and "unauthorized access").

[43] *See* Goldman, *supra* note 42, at 7 (asserting that the contract approach allows the parties to construe the parameters of authorization).

[44] *See id.* at 7 (advising that by accessing or using information outside in violation of the employee's contract, the employee has acquired information that he or she was "not entitled to obtain" (internal quotation marks omitted)).

[45] *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012) (combining the agency and contract approaches into one school of thought, represented by *Citrin* and defined by an employee who *misuses* information in a manner that "further[s] interests that are adverse to his employer"), *cert. dismissed*, 133 S. Ct. 831 (2013).

[46] *See infra* Part I.B.3 (discussing the code approach in the Ninth and Fourth Circuits).

[47] 274 F.3d 577 (1st Cir. 2001).

the employer's confidentiality agreement, constituted exceeding authorized access under § 1030.[48] In *United States v. Rodriguez*,[49] the Eleventh Circuit found an employee criminally liable for using information accessed through the employer's computer databases for personal benefit and in direct violation of the employer's policy.[50] Similarly, in 2010, the Fifth Circuit upheld the criminal convictions in *United States v. John*.[51] The defendant, a former Citigroup employee, misused customer account information for a fraudulent scheme, thereby exceeding her authorization.[52] The court supported its holding by stating that although the employee was authorized to access the customer account information, the use of the information was a clear violation of the employer's policies.[53]

3. Pro-employee: Code approach

The theory behind the code approach to the CFAA relies on the plain meaning canon of statutory interpretation, which provides that "unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning."[54] With this canon in mind, the Ninth Circuit first weighed in on the debate about employee liability under the CFAA in *LVRC Holdings LLC v. Brekka*.[55] The court adopted the code approach in this civil suit and provided a description for the otherwise undefined term "without authorization." Invoking the plain meaning canon, the court defined "authorization" as "permission," which indicates that an employee acts "without authorization" when the employee lacks the requisite password or login credentials to access the employer's computer or the specific information.[56] The court recognized the potential misuse of the information obtained by the employee; however, the court rejected a broad approach as inconsistent with the statute's plain language, as permission has no bearing on information *use*.[57] Instead, the court

[48] *See id.* at 582–84. The violation "might reasonably be construed to be contrary to the interests of EF." *Id.* at 583.

[49] 628 F.3d 1258 (11th Cir. 2010), *cert. denied*, 131 S. Ct. 2166 (2011).

[50] *See id.* at 1260–61 (involving an employee of the Social Security Administration who accessed, for personal reasons, private information about several women).

[51] 597 F.3d 263 (5th Cir. 2010), *cert. denied*, 133 S. Ct. 1237 (2013).

[52] *Id.* at 269.

[53] *See id.* at 271–72 (finding that John exceeded her authorized access because her actions were both an explicit violation of company policy and part of an illegal scheme that was not an intended use of the computer system).

[54] Perrin v. United States, 444 U.S. 37, 42 (1979).

[55] 581 F.3d 1127 (9th Cir. 2009). *Brekka* involved an employee who e-mailed a number of documents to his and his wife's personal e-mail accounts to build a competing business. *Id.* at 1129–30.

[56] *Id.* at 1133.

[57] *See id.* at 1133–35 (declining to adopt such an expansive interpretation and noting the Supreme Court's cautions against interpreting criminal statutes in ways that impose unexpected burdens).

employed a narrow interpretation of the statute wherein the user-employee can be held liable under the CFAA by circumventing the computer's privileges or passwords to access and obtain information.[58]

The Ninth Circuit addressed the issue again, this time in a criminal suit in *United States v. Nosal*,[59] which allowed the court to solidify its interpretation of the CFAA and further clarify the code approach. The case involved David Nosal, an employee of an executive search firm who convinced fellow colleagues to start a competing business.[60] Nosal and his colleagues used their log-in credentials to obtain proprietary information from the employer's computer, including source lists and contact information downloaded from the company's confidential database.[61] The government indicted Nosal on multiple counts, including a violation of § 1030(a)(4) for aiding and abetting his colleagues in exceeding authorized access with intent to defraud.[62] Although the employees had authorization to access the source lists and contact information, the employer had implemented a policy that limited use of confidential information solely to business purposes.[63] Consequently, the employees benefitted from the court's use of the code approach because it ignored the employees' motivations and focused solely on whether the employee had permission to access the information. Had the court adopted the broad agency or contract approaches, the government would have most likely prevailed.

In a rehearing en banc, the Ninth Circuit affirmed its reversal of the district court's decision and held that Nosal's and his colleagues' log-in credentials permitted them to access the information, thereby granting them authorization under § 1030(a)(4).[64] Although the company policy restricted the employees' *use* of the information, the court held that the purview of "the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*."[65] Consequently, the court upheld the dismissal of the government's charges of violating the CFAA.[66]

[58] *See id.* at 1135 (holding that access without authorization takes place when an individual has no permission to use the computer for any purpose, or when an employer rescinds an employee's permission and the employee continues to use the computer).

[59] 676 F.3d 854 (9th Cir. 2012) (en banc).

[60] *Id.* at 856.

[61] *Id.*

[62] *Id.*

[63] *See id.* at 856 & n.1 (detailing that company policy also prohibited employees from disclosing confidential information).

[64] *Id.* at 864. On remand, the district court denied Nosal's motion to dismiss the remaining CFAA counts, rejecting his argument that the en banc decision of the case limited liability to technical hacking crimes where technological barriers are circumvented. United States v. Nosal, No. CR-08-0237, 2013 WL 978226, at *8 (N.D. Cal. Mar. 12, 2013). Nosal argued that because the log-in information was voluntarily provided, there could be no hacking and thus no liability under the CFAA. *Id.* at *9.

[65] *Nosal*, 676 F.3d at 864. The court referenced several lower court opinions that illustrate the same plain-meaning interpretation of the CFAA. *See, e.g.*, Orbit One

The court rejected its sister circuits' broad interpretation of the CFAA for several reasons. First, the court noted that the narrow code approach is more faithful to the CFAA's text and its legislative history, as the statute's "general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere."[67] The Ninth Circuit substantiated its interpretation with the rule of lenity, which requires courts to narrowly construe ambiguous criminal statutes to prevent "making criminal law in Congress's stead."[68] The court explained that if Congress intended to hold employees accountable for misusing information, "it must speak more clearly."[69]

II. THE CODE APPROACH IN THEORY AND IN PRACTICE

A. The Fourth Circuit Adopts the Code Approach

On July 26, 2012, the Fourth Circuit addressed employee liability in a civil context under the CFAA and further divided the courts. In *WEC Carolina Energy Solutions LLC v. Miller*,[70] the defendant and WEC's former Project Director, Mike Miller, downloaded confidential documents from his company laptop to his personal e-mail account.[71] While working for WEC, Miller was subject to WEC's computer-use policies that protected its confidential information and trade secrets by prohibiting the unauthorized use of the information including downloading it to a non-WEC computer.[72] After resigning, Miller used the information in these documents for the benefit of a competitor, Arc.[73] WEC sued Miller under § 1030(a)(2), (a)(4), and (a)(5), contending that by downloading information

Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (advancing that "[t]he plain language of the CFAA supports a narrow reading" and adoption of the code approach); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (standing for the proposition that the CFAA "target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation" (quoting Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007)) (internal quotation marks omitted)); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005) (asserting that the CFAA does "not prohibit the unauthorized disclosure or use of information, but rather unauthorized access").

[66] *Nosal*, 676 F.3d at 864.

[67] *Id.* at 863.

[68] United States v. Santos, 553 U.S. 507, 514 (2008); *see Nosal*, 676 F.3d at 863 (explaining that the rule of lenity is a longstanding principle used by courts to look at the defendant's behavior with the understanding that millions of citizens as well as Congress must have "fair notice of what conduct [the] laws criminalize").

[69] *See Nosal*, 676 F.3d at 863 ("We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals.").

[70] 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013).

[71] *Id.* at 202.

[72] *Id.*

[73] *Id.*

to his personal computer in violation of WEC's policies, Miller breached his duty of loyalty to WEC and thereby either terminated or exceeded his authorization to access the computer.[74]

Judge Floyd delivered the opinion of the court, rejecting WEC's arguments and finding that employers cannot use the CFAA to impose liability on employees for *misusing* information obtained from a company computer when the employee had permission to access and obtain the information.[75] Agreeing with the district court's interpretation of the CFAA and the Ninth Circuit's interpretation in its en banc rehearing of *Nosal*, the unanimous three-judge panel held that employees are not "without authorization" and do not "exceed[] authorized access" when employers have provided them with permission to access a computer.[76]

Similar to the Ninth Circuit, the Fourth Circuit had constitutional vagueness concerns with respect to the incredibly broad reach of the statute.[77] The court focused on statutory interpretation and resolved any ambiguity in congressional intent through the rule of lenity.[78] Because Congress did not provide a definition for the term "without authorization," the court turned to the Oxford English Dictionary, which defines "authorization" as "formal warrant, or sanction."[79] According to the court, this definition suggests that the phrase does not extend to the *use* of

[74] *Id.* WEC argued that Miller's actions impaired the integrity of the company's computer systems and data, resulting in economic damages of at least $5000. *Id.*; *see* 18 U.S.C. § 1030(a)(4) (2006) (requiring minimum damages in the amount of $5000 to trigger liability under the CFAA).

[75] *WEC*, 687 F.3d at 206; *see* Audra A. Dial & John M. Moye, *Fourth Circuit Widens Split over CFAA and Employees Violating Computer Use Restrictions*, KILPATRICK TOWNSEND & STOCKTON LLP (Sept. 10, 2012), http://www.kilpatricktownsend.com/en/Knowledge_Center/Alerts_and_Podcasts/Legal_Alerts/2012/09/Fourth_Circuit_Widens_Split_Over_CFAA_and_Employees_Violating_Computer_Use_Restrictions.aspx (explaining that under the Fourth Circuit's interpretation of the CFAA, "the CFAA may be used to impose civil liability on employees either who are not permitted to access certain information but do so anyway, or who go 'beyond the bounds' of their authorized access; however, . . . the CFAA's prohibitions do not impose liability on an employee who has permission to access electronic information but then 'improper[ly] use[s]' that information" (alterations in original) (quoting *WEC*, 687 F.3d at 204, 207)).

[76] *WEC*, 687 F.3d at 206. Pursuant to Rule 12(b)(6), the U.S. District Court for the District of South Carolina dismissed the government's CFAA claim and rejected the Fifth Circuit's broad interpretation of the CFAA in *United States v. John*, 597 F.3d 263 (5th Cir. 2010), *cert. denied*, 133 S. Ct. 1237 (2013). WEC Carolina Energy Solutions LLC v. Miller, No. 0:10-cv-2775, 2011 WL 379458 (D.S.C. Feb. 3, 2011), *aff'd* 687 F.3d 199, *cert. dismissed*, 133 S. Ct. 831. Adopting a narrow reading of the statute, the district court found that an employee acts "without authorization" and triggers liability only when an employee accesses a computer without permission, which Miller possessed. *Id.* at *4–5.

[77] *WEC*, 687 F.3d at 206 (agreeing with the *Nosal* court that Congress did not intend for a CFAA violation and imposing criminal penalties when an employee violates a use policy).

[78] *Id.* at 204–06.

[79] *Id.* at 204.

information that is otherwise accessed with authorization.[80] Following in the footsteps of the Ninth Circuit, the Fourth Circuit concluded that the broad interpretation of the CFAA conflicts with the rule of lenity and imposes a harsh interpretation that could find millions of unsuspecting employees subject to criminal sanctions.[81] The court rationalized that the agency and contract approaches would inadvertently trap employees and find them criminally liable for technically violating a company policy through innocuous activity, such as e-mailing work to a personal computer for the purpose of working from home or using the computer to check Facebook or the scores of a football game.[82]

B. WEC *Impacts Employers and Rogue Employees*

By handing down its opinion in *WEC*, the Fourth Circuit intensified the debate over employee liability under the CFAA that continues to plague the courts. The court recognized that the opinion will "disappoint employers hoping for a means to rein in rogue employees," as the *WEC* decision does, in fact, have significant repercussions on employers seeking to bring claims against their employees.[83]

WEC has significant implications for employers and how they draft their computer policies. Employers enjoy having the CFAA in their arsenal of statutes used to charge rogue employees because (1) it immediately provides the option of bringing suit in federal court and (2) it is easier to prove the elements of CFAA charges than trade secret claims.[84] As the CFAA provides subject matter jurisdiction to bring suit in the federal court system, the employers need only determine which venue is proper.[85] The appropriate federal circuit will determine the level of control the employer's policy has over the employee. With potential litigation in mind, employers are able to craft broad use policies that ensnare employees, turning them into potential felons. If an employer is able to bring suit in a circuit that has adopted the contract or agency approach, then the policy dictates liability. As a result, the broad approaches to employee

[80] *Id.*

[81] *See id.* at 205–06 (concluding that a harsher interpretation would have "far-reaching effects unintended by Congress").

[82] *See id.* at 206 (emphasizing that an employee who e-mails work to a personal computer "has no intent to defraud his employer."); United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc) (stating that "[m]inds have wandered since the beginning of time," and "minor daliances" such as g-chatting and online shopping may be in violation of company use policies and subject unwary employees to criminal liability)

[83] *WEC* , 687 F.3d at 207.

[84] *See* Nicgorski, supra note 34, at 5 (emphasizing that attorneys in the Seventh Circuit should include CFAA charges in their "arsenal" of claims against rogue employees, while such cases would collapse in the Fourth and Ninth Circuits).

[85] 18 U.S.C. § 1030(g) (2006).

liability under the CFAA allow private contracts to dictate federal law.[86] The CFAA in large measure protects national security and private companies who oversee the country's infrastructure—surely Congress did not intend for private contracts to trump the federal statute.

WEC suggests that, at least in a growing number of circuits, the rise in employer actions against employees for trade secret misappropriation claims as well as other computer fraud claims may significantly decrease. For example, the U.S. District Court for the Southern District of New York agreed with the Fourth Circuit's narrow interpretation in *JBCHoldings NY, LLC v. Pakter*.[87] In *Pakter*, the employer sued the defendant-employee for breaching her employment contract by using proprietary information obtained through the company computer to set up a competing business.[88] The court recounted the opposing approaches to interpreting employee liability under the CFAA, noting that the district courts have adopted both views because the Second Circuit had not yet weighed in on the issue.[89] Citing to *WEC*, the court adopted the code approach, finding it "considerably more persuasive."[90]

As the CFAA becomes a less viable option, employers will need to find alternative theories to hold employees accountable (e.g., contractual, tort, and state statutory remedies).[91] The CFAA may only protect employers against circumvention of technological barriers to proprietary information, requiring additional provisions to protect against the misuse of such information.[92] These limitations on employee liability indicate that the statute requires further consideration and modification to provide a holistic protection mechanism. However, because the Supreme Court has dismissed the case, any resolution through the judiciary remains elusive. Consequently, any immediate clarification of the definition and the scope of the term "authorization" must emerge from the legislature.

[86] *See* Letter from Laura W. Murphy, Dir., Wash. Legislative Office, ACLU, et al., to House Comm. on the Judiciary (Apr. 2, 2013), *available at* https://www.eff.org/sites/default/files/cfaa_letter_to_judiciary.pdf; Letter from Laura W. Murphy et al. to Senate Judiciary Comm., *supra* note 19.

[87] No. 12 Civ. 7555, 2013 WL 1149061 (S.D.N.Y. Mar. 20, 2013).

[88] *Id.* at *2.

[89] *Id.* at *4–5.

[90] *Id.* at *5.

[91] *See id.* at *7 (finding that the broad agency approach "create[s] a federal cause of action for incidents and injuries traditionally governed by state contract and tort laws"); *see also Nosal*, 676 F.3d at 859–60 (explaining that interpreting "exceeds authorized use" broadly transforms contract and tort law claims into federal crimes).

[92] *See e.g.*, Nicgorski, supra note 34, at 5 (raising legislative amendments that limit liability by precluding violations of use policies).

III. RECENT LEGISLATIVE PROPOSALS REFLECT THE CODE APPROACH

Congress is considering several legislative proposals intended to resolve the ambiguities in the CFAA. In September 2011, the Senate Judiciary Committee supported an amendment to the CFAA sponsored by Senators Chuck Grassley (R-IA), Al Franken (D-MN), and Mike Lee (R-UT) ("Grassley/Franken/Lee amendment"), which addressed the constitutional vagueness concern illustrated by the Fourth Circuit.[93] This bipartisan amendment shielded employees from liability under the CFAA for violations of TOS agreements and company policies.[94] In effect, the Grassley/Franken/Lee amendment adopted the narrow code approach and at least in part solves the problem discussed in *WEC* and *Nosal* in which employees unwittingly expose themselves to liability under the CFAA by downloading information to their personal computers or by checking the weather and the latest news headlines.[95] This legislative effort, however, left unresolved if and how employers could hold rogue employees accountable for accessing information that is then used for purposes that conflict with the interests of their employer, as was the case in *WEC* and *Citrin*.

On February 15, 2012, chairman of the Senate Judiciary Committee, Senator Patrick Leahy (D-VT), proposed a more comprehensive CFAA amendment called the Cyber Crime Protection Security Act,[96] which attempted to place limitations on the types of information that must be obtained by the employee to trigger liability and to clarify the term "exceeds authorized access."[97] Additionally, the amendment sought to

[93] *See* S. REP. NO. 112-91, at 12 (2011) (recounting the approval of the Committee to narrow the definition of "exceeds authorized access" in the CFAA).

[94] *Id.*; *see* Letter from Laura W. Murphy et al. to Senate Judiciary Comm., *supra* note 19 (indicating that the amendment would "fix a large part of the overbreadth problem in the CFAA"); Greg Nojeim & Jake Laperruque, *Why Fibbing About Your Age Is Irrelevant to the Cybersecurity Bill*, CTR. FOR DEMOCRACY & TECH. (July 30, 2012), https://www.cdt.org/blogs/greg-nojeim/3007why-fibbing-about-your-age-relevant-cyber security-bill (calling the Franken/Grassley/Lee amendment "an important step forward for security and civil liberties" (internal quotation marks omitted)).

[95] *See* S. REP. NO. 112–91, at 12 (noting that the amendment would exclude from the CFAA liability conduct that only involves a TOS violation); Laura W. Murphy et al. to Senate Judiciary Comm., *supra* note 19 (stating that the amendment would remove the possibility of felony prosecutions where TOS violations are the sole basis to determine whether access was authorized); *see also* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) (explaining the problem with an agency approach that would remove an employee's authorization instantaneously for viewing Facebook or checking sports scores), *cert. dismissed*, 133 S. Ct. 831 (2013).

[96] S. 2111, 112th Cong. § 8 (2012) (including some provisions previously approved by the Senate Judiciary Committee in the Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (as reported by the S. Comm. on the Judiciary, Sept. 22, 2011)).

[97] *See id.* §§ 4, 8 (providing examples of trafficking in passwords as one type of information to trigger liability, and excluding contractual or terms of service violations from the definition of unauthorized access).

impose harsher penalties for CFAA violations, including an added asset forfeiture provision and an "aggravated damage" section.[98] In July 2012, Leahy submitted the Cyber Crime Protection Security Act, along with four additional amendments, to the Cybersecurity Act, a bill already in deliberations by the Senate.[99] The Department of Justice (DOJ) supported Leahy's changes to enhance penalties, but opposed the narrow code approach to interpreting authorization included in section 8 of the amendment, which would limit the government's prosecutorial authority.[100]

The bill faced opposition from several Republican senators as well as the prominent U.S. Chamber of Commerce, and despite aggressive support from the White House, it ultimately failed in the Senate by a 52–46 vote to end debate and move forward with legislation.[101] Those who voted in favor of the bill remarked that instead of focusing on the pressing need to increase cybersecurity and the pleas from the Executive branch to increase the nation's safety, the bill became "another vehicle for partisan ideological shots."[102]

The Senate may also consider the Republicans' competing proposal, the

[98] *Id.* §§ 6–7.

[99] 158 CONG. REC. S5404 (daily ed. July 25, 2012). The four additional amendments are SA 2576, 2577, 2578, and 2580. The revised Cybersecurity Act of 2012 with these amendments (and others) is the "Revised Cybersecurity Act of 2012" or "CSA2012." S. 3414, 112th Cong. (2012).

[100] *See Cyber Crime: Updating the Computer Fraud and Abuse Act To Protect Cyber Space and Combat Emerging Threats: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 6 (2011) (statement of James Baker, Associate Deputy Att'y Gen of the United States) ("[R]estricting the statute [by prohibiting claims bases solely upon a violation of terms of use or contractual agreements] would make it difficult or impossible to deter and address serious insider threats through prosecution."); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. § 110 (as reported by the S. Comm. on the Judiciary, Sept. 22, 2011) (incorporating the proposed Grassley/Franken/Lee amendment and limiting the definition of unauthorized use to exclude any violation of use policy or TOS agreements); Nojeim & Laperruque, *supra* note 94 (indicating that the DOJ opposes the Grassley/Franken/Lee amendment portion proposed by Senator Leahy); *see also* Orin Kerr, *Recent Developments—Both in the Courts and in Congress—on the Scope of the Computer Fraud and Abuse Act*, VOLOKH CONSPIRACY (July 30, 2012, 11:35 PM), http://www.volokh.com/2012/07/30/recent-developments-both-in-the-courts-and-in-congress-on-the-scope-of-the-computer-fraud-and-abuse-act (noting that the DOJ supported various amendments, including the asset forfeiture and additional punitive damages provisions).

[101] Ramsey Cox & Jennifer Martinez, *Cybersecurity Act Fails Senate Vote*, HILL (Aug. 2, 2012, 10:36 AM), http://thehill.com/blogs/hillicon-valley/technology/241851-cybersecurity-act-fails-to-advance-in-senate (reporting that the bill required 60 votes to continue and quoting the White House Press Secretary's characterization of the bill's failure as "a profound disappointment").

[102] *Id.* (addressing Republican Senators' belief that the bill placed too heavy of a burden on the business community to improve their private cyber infrastructures). Following Congress's failure to pass legislation, President Obama signed a Cybersecurity Executive Order that promotes strengthened cyber defenses for the nation's infrastructure and information sharing between the public and private sectors. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013). This executive order, however, does not impact any privacy laws and regulations.

SECURE IT Act of 2012,[103] which provides more consideration from the business community.[104] The SECURE IT Act, supported by Senators John McCain (R-AZ) and Kay Bailey Hutchinson (R-TX), includes the same code approach to defining "exceeds authorize access" as included in the Grassley/Franken/Lee amendment and Senator Leahy's proposal.[105] Although the bill has not yet been considered in the Senate, it will most likely face the same opposition from the DOJ as the Cybersecurity Act for limiting prosecutorial discretion. If Congress cannot find a balance with respect to who bears the burden of implementing cybersecurity measures to prevent hacking, then enacting legislation remains as out of reach as judicial resolution.

A compromised solution may lie in "Aaron's Law," a legislative effort drafted by Congresswoman Zoe Lofgren (D-CA).[106] The new bill follows the death of Aaron Swartz, an Internet activist who downloaded millions of articles in violation of JSTOR's TOS agreement and faced thirteen felony charges, including several violations of the CFAA.[107] Faced with the possibility of spending thirty-five years in prison, Swartz committed suicide before trial was set to begin.[108] Swartz's tragic death incited Internet activists and lawmakers who believe that the government had overreached its prosecutorial authority and brought disproportionate charges against Swartz.

The public outcry resulted in Aaron's Law, which seeks to eliminate vagueness concerns by tightening the overbroad language of the CFAA.[109]

[103] H.R. 4263, 112th Cong. (2012).

[104] *See id.* (providing a more conservative approach, for example section 410 holds the government accountable for implementing a cybersecurity strategic research and development plan).

[105] *Compare id.* (excluding from unauthorized use "access in violation of a contractual obligation or agreement . . . if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized"), *with* Cyber Crime Protection Security Act, S.2111, 112th Cong. § 8 (2012) (using identical language), *and* S. REP. NO. 112-91, at 12 (2011) (same).

[106] REP. ZOE LOFGREN, 113TH CONG., AARON'S LAW MODIFIED DRAFT (2013), *available at* http://lofgren.house.gov/images/stories/pdf/Aarons%20law%20revised%20draft%20013013.pdf.

[107] Swartz wrote a script to gather the academic articles from the archive database, although his intended motivation behind the script remains unknown. *See* Lawrence Lessig, *Aaron's Law: Violating a Site's Terms of Service Should Not Land You in Jail*, ATLANTIC (Jan. 16, 2013, 4:38 PM), http://www.theatlantic.com/technology/archive/2013/01/aarons-law-violating-a-sites-terms-of-service-should-not-land-you-in-jail/267247. With respect to the CFAA, Swartz was indicted for computer fraud under § 1030(a)(4), (b); unlawfully obtaining information from a protected computer under § 1030(a)(2), (b), (c)(2)(B)(iii); and recklessly damaging a protected computer under § 1030(a)(5)(B), (c)(4)(A)(i)(I), (VI). Superseding Indictment, United States v. Swartz, No. 1:11-cr-10260 (D. Mass. Sept. 12, 2012), ECF No. 53.

[108] Press Release, U.S. Attorney's Office, District of Mass., Alleged Hacker Charged with Stealing over Four Million Documents from MIT Network (July 19, 2011), *available at* http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html (discussing the terms of Swartz's indictment).

[109] REP. ZOE LOFGREN, 113TH CONG., AARON'S LAW MODIFIED DRAFT § 2 (2013), *available*

Lofgren proposes amending the CFAA by eliminating the term "exceeds authorized access," which may have required the court to dismiss the government's CFAA charges against Swartz, had it been in effect.[110] The resulting language of the bill circumvents the interpretation issue of "exceeds authorized access" addressed in Grassley/Franken/Lee amendment and the Cybersecurity Act by eliminating the term from the CFAA entirely.[111] In addition, the current version of Aaron's law eliminates violations of TOS agreements and breaches of contract from the statute's mandate.[112]

Lofgren may hope to have the amendment pass swiftly in both houses, but the bill may stall due to similar resistance faced by the previous efforts.[113] Swartz' death has reignited bipartisan efforts to amend the CFAA and competing bills are in circulation, although they are in the early drafting stages.[114] Each legislative proposal has faced fierce opposition

at http://lofgren.house.gov/images/stories/pdf/aarons%20law%20revised%20draft%20013013.pdf.

[110] *See Congresswoman Introduces "Aaron's law" To honor Swartz*, RT (Jan. 17, 2013, 2:38 AM), http://rt.com/usa/swartz-cfaa-aaron-law-148 (using Lofgren's statement that "using the law in this way could criminalize many everyday activities and allow for outlandishly severe penalties").

[111] *Compare* REP. ZOE LOFGREN, 113TH CONG., AARON'S LAW MODIFIED DRAFT § 2 (2013), *available at* http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20revised%20draft%20013013.pdf ("[S]triking 'exceeds authorized access' and all that follows . . . ."), *with* Cybercrime Protection Security Act, S. 2111, 112th Cong. § 8 (2012) ("[A]lter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized."), *and* Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. § 110 (as reported by the S. Comm. on the Judiciary, Sept. 22, 2011) (same).

[112] REP. ZOE LOFGREN, 113TH CONG., AARON'S LAW MODIFIED DRAFT § 2(a)(2)(B) (2013), *available at* http://www.lofgren.house.gov/images/stories/pdf/Aarons%20law%20revised%20draft%20013013.pdf.

[113] *See e.g.*, Letter from Laura W. Murphy et al. to House Comm. on the Judiciary, *supra* note 86; EXEC. OFFICE OF THE PRESIDENT, LEGISLATIVE LANGUAGE: LAW ENFORCEMENT PROVISIONS RELATED TO COMPUTER SECURITY (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-section-by-section-analysis.pdf (proposing enhanced criminal penalties among other increased prosecutorial leverage to previous legislative efforts to amend the CFAA); Declan McCullagh, *Senate Readies for Fight over Cybersecurity Surveillance*, CNET (Apr. 2, 2013, 10:45 AM), http://news.cnet.com/8301-13578_3-57577520-38/aarons-law-rewrite-backfires-reformers-now-on-defensive (quoting Senator Mitch McConnell's spokesman's hope that "Sen[ator] Reid will not block the amendments like he did last time").

[114] Jennifer Martinez, *Draft House Judiciary Cybersecurity Bill Would Stiffen Anti-Hacking Law*, HILL (Mar. 25, 2013, 11:02 AM), http://thehill.com/blogs/hillicon-valley/technology/290103-draft-cybersecurity-bill-aims-to-stiffen-computer-hacking-law; H. COMM. ON THE JUDICIARY, 113TH CONG., DISCUSSION DRAFT (2013), *available at* http://www.scribd.com/doc/132249133/House-Judiciary-Committee-discussion-draft (proposing to amend § 1030 (e)(6) by "inserting after 'alter' the following: ', even if the accesser may be entitled to obtain or alter the same information in the computer for other purposes'").

from Congress, agencies, and the business community. Republicans want to block legislation that they fear is too onerous on the business community by forcing businesses to carry the burden of securing their computer systems and data. Most recently, a group of organizations and individuals including the ACLU, Electronic Frontier Foundation, and Professor Orin Kerr wrote a letter to Congress opposing Aaron's Law.[115] They warn that the draft actually expands the scope of the Act by increasing penalties and increasing "the scope of conduct punishable," including adding computer crimes as a form of racketeering.[116]

Notwithstanding Congress's inability to pass a clarifying amendment, the similarities in its several proposals are revealing.[117] Despite the political disagreement over the practical implementation of cybersecurity safety measures, proponents of all four bills supported restricting the interpretation of "exceeds authorized access" in their amendments, suggesting that Congress is unified in support of limiting employee liability. Republicans and Democrats read employee liability under the CFAA narrowly, precluding from liability employees with permission to access their employer's computer. Congress supported the narrow definition of "exceeds authorized access" originally included in the Grassley/Franklin/Lee amendment that precluded liability for violating a contractual agreement, such as a TOS agreement. The language of this legislative proposal was adopted by Leahy's Cyber Crime Protection Security Act, the Cybersecurity Act, McCain and Hutchinson's SECURE IT Act. Lofgren's current draft of Aaron's Law builds upon these attempts by eliminating the troublesome term entirely.

Thus, despite disagreement over many aspects of cybersecurity amendments, Congress remains unified about employee liability under the statute. An added motivation for limiting the CFAA's overbroad reach is Congress's constitutional vagueness concerns pertaining to the DOJ's exercise of prosecutorial discretion when investigating potential charges

[115] Letter from Laura W. Murphy et al. to House Comm. on the Judiciary, *supra* note 86.

[116] *Id.*; *see* Trevor Timm, *Congress' New CFAA Craft Could Have Put Aaron Swartz in Jail for Decades Longer than the Original Charges*, ELECTRONIC FRONTIER FOUND. (Mar. 27, 2013), https://www.eff.org/deeplinks/2013/03/congress-new-cfaa-draft-could-have-put-aaron-swartz-jail-decades-longer-he-was (suggesting that Aaron's Law expands the CFAA's mandate and has the opposite effect than Congresswoman Lofgren intended because it increases the maximum sentence under § 1030(a)(4) from five years to twenty years).

[117] *See* Orin Kerr, *House Judiciary Committee New Draft Bill on Cybersecurity Is Mostly DOJ's Proposed Language from 2011*, VOLOKH CONSPIRACY (Mar. 25, 2013, 2:30 PM), http://www.volokh.com/2013/03/25/house-judiciary-committee-new-draft-bill-on-cyber security-is-mostly-dojs-proposed-language-from-2011 (explaining that Aaron's Law is "mostly copied from a bill that Senator Leahy offered . . . back in November 2011).

under the CFAA.[118] While the DOJ has stated that it does not intend to target employees who unwittingly violate the statute, precedent yields valid concern regarding whether the DOJ will abide by this policy.[119] By continually proposing to amend "exceed authorized access" under § 1030(e)(6) to preclude any charges based solely on TOS agreement violations or contract breaches, Congress has indicated that it agrees with the *WEC* court that the statute in its current form is overbroad. Until Congress passes an amendment or the Supreme Court provides unifying guidance, undecided courts in future cases should follow the lead of the Fourth and Ninth Circuits and adopt the code approach.

CONCLUSION

By entering the debate about employee liability under the CFAA, the Fourth Circuit exacerbates the existing circuit split and the need for resolution from the Supreme Court or Congress. Unfortunately, any resolution from the judiciary remains a remote possibility, and litigants and judges alike must wait for another employee liability case to reach the Supreme Court. Meanwhile, Congress is engaged in a lively debate over the proper interpretation of "without authorization" under the CFAA and has drafted multiple proposals to reconcile the ambiguities that plague the statute. Although Congress has not yet enacted a bill, it has united with respect to limiting liability under the CFAA strictly to obtaining information without permission. The restricting language in these legislative efforts indicate that Congress has endorsed the code approach as the preferred judicial interpretation of the CFAA.

[118] *See* S. REP. NO. 112–91, at 9 (2011) ("During the Judiciary Committee hearing, several Members of the Committee, including the Chairman, raised concerns about the Justice Department's decision to bring criminal charges in *United States v. Lori Drew*, which involved a [CFAA] charge based solely upon a violation of a MySpace [TOS] agreement.").

[119] *Id.* at 9–10 ("In his testimony before the Committee, Associate Deputy Attorney General James Baker Responded to concerns about the *Drew* prosecution by noting that the case was an anomaly . . . .").