American University Business Law Review

Volume 4 | Issue 3 Article 3

2016

A Threat To Or Protection Of Agency Relationships? The Impact Of The Computer Fraud And Abuse Act On Businesses

Jessica Milanowski
American University Washington College of Law

NOTE

A THREAT TO OR PROTECTION OF AGENCY RELATIONSHIPS? THE IMPACT OF THE COMPUTER FRAUD AND ABUSE ACT ON BUSINESSES

JESSICA MILANOWSKI*

The Computer Fraud and Abuse Act of 1986 ("CFAA") criminalizes unauthorized access to information stored on computers and allows for those who are damaged by such unauthorized access to bring a civil suit against the abuser. Currently, the Seventh and Ninth Circuits have split regarding the proper interpretations of the terms "authorization" and "exceeds authorized access" on employer-provided computer use. The Seventh Circuit adopted a broad reading of the statute in International Airport Centers, LLC v. Citrin, *holding that when the employee decided to quit his job in violation of his employment contract, he violated his duty of loyalty and therefore no longer had authorization to use his work laptop. In contrast, the Ninth Circuit developed a narrow reading of the statute in* United States v. Nosal, *finding that the employee misused confidential information when he took, downloaded, and copied a confidential source list of information and data from the search firm's computer system. However, since the employee did not access the information himself, he could not be held liable under the CFAA. This Comment first analyzes the background and history of the CFAA and cases that have contributed to the circuit-split. Next, this Comment addresses a hypothetical scenario of an employee who searches through his employer's confidential files and*

* J.D. Candidate, May 2016, American University Washington College of Law; B.A. Political Science and International Studies, *cum laude*, minor in French, 2013, Stonehill College, Easton, Massachusetts. Many thanks to Professor Kenneth Anderson for sparking my interest in this topic and for providing invaluable insight into the legal analysis of the issue. Further thanks are due to the American University Business Law Review staff who devoted countless hours and incredible effort to editing and preparing this piece for publication. Finally, I want to extend my sincere thanks to my family and friends who supported me throughout this process. Your patience did not go unnoticed.

trade secrets to build a competing business. Finally, it recommends the Ninth Circuit interpretation be adopted either by Congress or the United States Supreme Court.

INTRODUCTION

The Computer Fraud and Abuse Act of 1986 ("CFAA") criminalizes unauthorized access to confidential information stored on computers,[1] and it is often applied to employer-employee trade secret disputes.[2] However,

---

1. *See* 18 U.S.C. § 1030 (2010) (prohibiting certain computer use "without authorization" or that "exceeds authorized access" as defined in the statute).

2. *See* Cynthia Augello, *Circuit Split: How Does the CFAA Apply to Employment Cases?*, JDSUPRA (Oct. 15, 2012), http://www.jdsupra.com/legalnews/circuit-split-how-does-the-cfaa-apply-t-93612/ (explaining that the CFAA provides a potential avenue for employers to seek redress in conflicts with employees); Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 820

today, the Seventh and Ninth Circuits are split concerning the proper interpretation for the terms "authorization" and "exceeds authorized access" as it pertains to employee use of an employer-provided computer within the context of the CFAA.[3] The Seventh Circuit adopted a broad interpretation of the statute in *International Airport Centers, LLC v. Citrin*. The Court held that when the employee decided to quit in violation of his employment contract, he violated his fiduciary duty of loyalty, and therefore he no longer had authorization to use his work laptop.[4]

The Ninth Circuit and the Fourth Circuit have developed a correspondingly narrow reading in determining whether the CFAA applies only when an employee improperly accesses business information or also when an employee uses that information in pursuit of his own business and to the detriment of his employer.[5] In *United States v. Nosal*, the Ninth Circuit upheld the employee's misuse of confidential information from the search firm's computer system as lawful.[6] Similarly, the Fourth Circuit, in *WEC Carolina Energy Solutions, LLC v. Miller*, held that an employee does not violate the CFAA when he downloads information to a personal computer, violates company policy, and subsequently uses that information to develop a competing business.[7]

(2009) (noting that even though computers increase employee productivity, they also make confidential information more easily accessible to employees).

3. *See* Stuyvie Pine, *The Computer Fraud and Abuse Act: Circuit Split and Efforts to Amend*, BERKELEY TECH. L.J. BOLT (Mar. 31, 2014), http://btlj.org/?p=3260 (comparing the Ninth Circuit's "access-only" interpretation with the "use-and-access" interpretation).

4. *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (explaining that the employee's breach of his duty of loyalty terminated his agency relationship and, with it, his authority to access the employer-provided computer because the only basis for his continued use of the computer had been that established agency relationship); *see also* Anderson, *infra* note 9, at 431 (noting that an agency relationship ends when an employee violates his duty of loyalty).

5. *See* Audra A. Dial & John M. Moye, *Fourth Circuit Widens Split Over CFAA and Employees Violating Computer Use Restrictions*, KILPATRICK TOWNSEND LEGAL ALERT (Sept. 10, 2012), http://www.martindale.com/matter/asr-1585570.CFAA.pdf (discussing the importance of employers implementing strict guidelines governing which employees may access certain information).

6. *See* United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (refusing to interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty).

7. *See* WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012) (rejecting an interpretation of the CFAA that imposes liability on employees who violate a use policy, choosing instead to limit such liability to "individuals who access computers without authorization or who obtain or alter information beyond the bounds of their authorized access"); *id.* (explaining the court's holding that the CFAA *cannot* be used to impose liability on an employee who is given lawful access to company information but later misuses that information).

This Comment will conduct a thorough exploration of the history of the CFAA, detailing the rationales of the opposing circuits, and addressing the theory of agency law and its application to the CFAA and cases concerning the statute.[8] This Comment will then delve into a hypothetical scenario of an employee who searches through his employer's confidential files and trade secrets to build a competing business. It will subsequently apply each circuit's different rationales and approaches to the issue, which will result in different outcomes in what actions the employer can bring over her stolen information.[9] The first result will be more employee-friendly, while the second result will be more employer-friendly. Finally, this Comment will recommend that the United States Supreme Court adopt the Ninth Circuit's broader interpretation of the CFAA. In the alternative, Congress could revamp the statute for clarification in the modern world or instead create a whole new piece of legislation that specifically addresses this technological issue, particularly in the employment context.

I. A THOROUGH EXPLORATION OF THE HISTORY OF THE CFAA AND THE OPPOSING CIRCUIT RATIONALES

A. The Computer Fraud and Abuse Act

The CFAA criminalizes unauthorized access to information stored on computers, and it allows for those damaged by such unauthorized access to bring a civil suit against the abuser.[10] The CFAA prohibits a person from "intentionally access[ing] a computer without authorization" or "exceed[ing] authorized access," thereby obtaining "information" from a computer that is "used in or affecting interstate or foreign commerce."[11] The CFAA's definition of "exceeds authorized access" is "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [*sic*] is not entitled so to obtain or alter,"[12] which is distinguished from the term, "without authorization."[13] The CFAA provides that whoever knowingly causes the transmission of a program, information, code, or command, and as a result

8. *See generally* WILLIAM T. ALLEN ET AL., COMMENTARIES AND CASES ON THE LAW OF BUSINESS ORGANIZATIONS (4th ed. 2009) (discussing the convalescence of business, corporate, and agency law).

9. *See* Alden Anderson, *The Computer Fraud and Abuse Act: Hacking Into the Authorization Debate*, 53 JURIMETRICS J. 447 (2013) (explaining that competing interpretations of the CFAA can lead to vastly different results).

10. *See generally* 18 U.S.C. § 1030 (2010).

11. *Id.*

12. *Id.* § 1030(e)(1), (6).

13. *Id.* § 1030(a)(1), (2), (4).

of such conduct, intentionally causes damage without authorization to a protected computer violates the Act.[14] If one is found to have "exceeded authorized access" and violated the Act, the CFAA allows for the enforcement of criminal sanctions when additional aggravating factors are met,[15] and it permits private parties who suffer "damage or loss by reason of a violation" to bring a claim for damages.[16]

Congress originally enacted the CFAA to combat computer hacking, which targeted third parties accessing private computer systems without permission and/or authorization.[17] However, employers have recently attempted to use the CFAA's broad language to cover a range of issues well beyond hacking, such as individuals stealing trade secrets from employers or employees misusing employer information gathered from employer-provided computers. Thus, the circuits have split concerning the statute's reach and how it ought to be currently applied to employees as third parties who exceed the scope of their authorized use of work computers.[18]

B. The Theory of Agency Law

Agency law has a substantial influence on the CFAA.[19] The theory of

---

14. *Id.* § 1030(a)(5)(A)(i).

15. *See id.* § 1030(a)(2)(C) (making it a crime to attempt or to commit any of the enumerated offenses); *see also id.* § 1030(c)(2)(B) (explaining that a violation or attempted violation of § 1030(a)(2)(C) is a felony if one of these aggravating factors is present: "(a) committed for commercial advantage or private financial gain, (2) committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or (3) the value of the information obtained exceeds, $5,000"); H. Marshall Jarrett et al., *Prosecuting Computer Crimes*, DEPARTMENT OF JUSTICE COMPUTER CRIMES AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION, 20 http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (stating that if the aggravating factors apply, a violation is punishable by a fine, up to five years' imprisonment, or both).

16. See 18 U.S.C. § 1030(g); *see also* Dial, *supra* note 5 (providing background on the various CFAA interpretations).

17. *See* United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (explaining that Congress enacted the CFAA primarily to address the growing problem of computer hacking); Orzechowski, *infra* note 18. *See generally* CHARLES DOYLE, CONG. RESEARCH SERV., RL97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS (2014) (showcasing Congress' intent when it created the CFAA).

18. *See* Daren M. Orzechowski et al., *A Widening Circuit Split in the Interpretation of the Computer Fraud and Abuse Act,* WHITE & CASE LLP (Sept. 13, 2012), http://www.whitecase.com/articles-09132012/#.VHp5P75UFVs (noting that the Circuit Courts of Appeals have not provided clear guidance on the proper CFAA interpretation).

19. *See* Restatement (Third) of Agency § 1.01 (defining "agency"); *see also* Thomas E. Geu, *A Selective Overview of Agency, Good Faith, and Delaware Entity*

the duty of loyalty, which is a subset of the fiduciary duty theory, requires all corporate fiduciaries to exercise their authority in a good faith attempt to advance corporate purposes.[20] Agency law can be used as an aid to give meaning to statutes that either establish agency relationships or govern behavior that falls within the law of agency.[21] This type of relationship is especially apparent in the employer-employee setting where the duties of good faith, loyalty, and due care are ever present.[22]

Some jurisdictions find that partnership duties exceed written agreements. For example, in *Meinhard v. Salmon*, the Court of Appeals of New York held that the partnership contract did not entirely encompass the obligations between the parties, pushing partnership duties beyond the scope of the agreed terms.[23] For example, a co-adventurer has the duty to concede and reveal any chance to compete and any chance to enjoy the opportunity for benefit that had come to him alone by virtue of his agency.[24] The Court determined that in such a relationship, loyalty must be undivided and unselfish, and that a breach of fiduciary duty can occur by something less than fraud or intentional bad faith.[25]

C. Seventh Circuit Analysis

Some circuit courts have adopted a broad reading of the CFAA.[26] Initially, the First Circuit in *EF Cultural Travel v. Explorica*, held that an employee "exceeded authorized access" by violating restrictions on both use and access of employers' computers.[27] The Seventh Circuit later joined

---

Law, 10 DEL. L. REV. 17, 18 (2008) (discussing the concept that agency law influences and interacts with more specific laws where agency relationships inherently develop).

20. *See* ALLEN, *supra* note 8 (explaining the academic theories behind agency law).

21. *See* Geu, *supra* note 19 (noting that CFAA interpretation demands analysis of traditional agency fiduciary duties).

22. *See* Field, *supra* note 2, at 823 (explaining that the employer-employee agency relationship imposes "special duties on the part of both the employer and the employee which are not present in the performance of other types of contracts.").

23. *See* Meinhard v. Salmon, 249 N.Y. 458, 464 (1928) (noting "a trustee is held to stricter morals than that of a marketplace").

24. *See id.* (stating that those who engage in joint ventures owe to one another the finest duty of loyalty).

25. *See id.* (holding that one partner may not appropriate a renewal of a lease for himself, even when its term begins at the end of the partnership agreement).

26. *See* Augello, *supra* note 2 (detailing that the Fifth, Seventh, and Eleventh Circuits have adopted a broad statutory interpretation of the CFAA finding that an employee acts "without authorization or in excess of his authority when the employee acquires an interest adverse to his employer or breaches a duty of loyalty owed to the employer.")

27. *See* EF Cultural Travel v. Explorica, 274 F.3d 577, 583-84 (1st Cir. 2001)

in *International Airport Centers, LLC v. Citrin*, stating that once the duty of loyalty has been violated, accessing computer files that had previously been authorized transforms into unauthorized access under the CFAA.[28] This means that an employee can "exceed authorized access" by violating a company's terms of service policy and by breaching the duty of loyalty under agency law.[29] In *International Airport Centers, LLC*, the employee quit his job and started a competing business, which was in violation of his employment contract.[30] The employee deleted files from his work laptop before he left, including information that he wanted to resign and develop a competing business, because the company's employee policy allowed for data deletion.[31] However, the Seventh Circuit held that, since he violated his contract when he decided to quit, he breached his duty of loyalty and lost his authorized access to the work laptop.[32]

The Fifth,[33] Eleventh,[34] and Eighth[35] Circuits have since joined the Seventh Circuit's interpretation.[36] In *United States v. John*, the Fifth Circuit Court held that an employee exceeded her authorized access by

---

(explaining that while the employee's use of a company website was public, so he was authorized, he exceeded his authorization by providing proprietary information about the structure of the website to a competing entity).

28. *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d at 420-21 (7th Cir. 2006) (finding that the employee's breach of his duty of loyalty terminated his agency relationship with the employer).

29. Orzechowski, *supra* note 18; *see e.g.*, Lawrence Lessig, *Aaron's Law: Violating a Site's Terms of Service Should Not Land You in Jail*, THE ATLANTIC (Jan. 16, 2013), http://www.theatlantic.com/technology/archive/2013/01/aarons-law-violating-a-sites-terms-of-service-should-not-land-you-in-jail/267247/ (explaining that terms of services have been interpreted as rules of contract. When one young man exceeded those limits, the government charged that he had breached an implied contract and therefore was a felon under the CFAA).

30. *See Int'l Airport Ctrs.*, 440 F.3d at 421 (rejecting the employee's argument that he did not violate the CFAA when he destroyed data because the employee policy allowed data deletion, and ultimately finding it unlikely that the provision was intended to authorize employees to destroy data that they knew the company had no duplicates of and would have wanted to have).

31. *See id.* at 420-21 (listing actions adverse to the employer as reasons for CFAA violation).

32. *See id.* at 421; *see also* Orzechowski, *supra* note 18 (concluding that courts who follow the *Citrin* approach provide the broadest protection to employers).

33. *See* United States v. John, 597 F.3d 263 (5th Cir. 2010).

34. *See* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

35. *See* United States v. Teague, 646 F.3d 1119, 1124 (8th Cir. 2011).

36. *See* Elkhan Abramowitz & Barry Bohrer, *Different Strokes: Interpreting Computer Fraud and Abuse Act*, 24 N.Y. L.J. 45 (2012) (suggesting that the CFAA circuit split in employment cases brought against employees, alleged to have misappropriated information from an employer's computer, is presently widely publicized).

using a customer's personal information to make fraudulent credit card charges.[37] In *United States v. Rodriguez*, the Eleventh Circuit held that an employee's use of the Social Security Administration's database exceeded authorized access when the employee used it to retrieve personal information about potential romantic partners.[38] In *United States v. Teague*, the Eighth Circuit rejected the notion that an employee did not exceed authorized access to obtain President Obama's student loan records.[39] These cases further explain the broad reading rationale of the CFAA.

D. Ninth Circuit Analysis

Conversely, some circuits have developed a narrow reading of the CFAA.[40] The Ninth Circuit in *United States v. Nosal* held that an individual "exceeds authorized access" by violating a restriction on access but not by violating a restriction on use of a work computer and its contents.[41] In this case, an individual employee convinced some of his former colleagues to download confidential information from the search firm they worked for and have them send the information to him.[42] Even though his colleagues had authorized access to the confidential information, they violated company policy, which prohibited "(1) using confidential information for nonbusiness purposes and (2) transferring the information to third parties."[43] This means that an individual "exceeds authorized access" by violating a restriction on access but not by violating

37. *See John*, 597 F.3d at 267 (concluding that "when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime," he has exceeded authorized access, even though he may have been permitted authorization).

38. *See Rodriguez*, 628 F.3d at 1263-64 (finding that an employee exceeds authorized access when his interest in acquiring the confidential information is to the detriment of his employer).

39. *See Teague*, 646 F.3d at 1127 (determining that to convict a person under the CFAA, it must be proven that he or she intentionally exceeded authorized access).

40. *See* United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (rejecting the argument that the CFAA should be read to incorporate corporate policies addressing information use); *see also* Orzechowski, *supra* note 18 (explaining that along with the Ninth and the Fourth Circuits, district courts in the Second, Fourth, Sixth, Eighth, and Tenth Circuits have also adopted similarly narrow interpretations of the CFAA).

41. *See Nosal*, 676 F.3d at 862 (holding that the employees did not "exceed their authorized access" by violating company policy against using the database for non-company business).

42. *See id.* at 856.

43. *Id.* at 862.

a restriction on use of a work computer and its contents.[44] The Ninth Circuit has decided to interpret the statute narrowly and only apply it to those who access an unauthorized computer. However, the CFAA does not apply to those who have the authorized access and later use that information to the detriment of their employer.[45] This sentiment holds whether or not the action violates the employer's computer use policies.[46]

The Fourth Circuit has since sided with the Ninth Circuit.[47] In *WEC Carolina Energy Solutions, LLC v. Miller*, the Court held that an employee, who downloaded information to a personal computer, violated company policy, and used that information to develop a competing business, did not violate the CFAA because he did not access the files without authorization or illegally.[48] This case further explains the broad reading rationale of the CFAA.

E. Comparing and Contrasting the Broad and Narrow Interpretations of the CFAA and How It Applies to Agency Law

There are vast differences between these two interpretations of the CFAA.[49] Under a Seventh Circuit regime, any employee that accesses information on a computer to use that information to the detriment of his employer has violated a duty of loyalty under agency law, which terminates the agency relationship and no longer gives that employee proper

---

44. *See id.*

45. *See id.* 856-57 (reasoning that the government's interpretation would change the CFAA from "an anti-hacking statute to an expansive misappropriation statute").

46. *See id.* at 860-61 ("Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And Sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their Sudoku skills behind bars. The effect this broad construction of the CFAA has on workplace conduct pales by comparison with its effect on everyone else who uses a computer, smart-phone, iPad, Kindle, Nook, X-box, Blu-Ray player, or any other Internet-enabled device.").

47. *See* WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 199 (4th Cir. 2012).

48. *See id.* at 204 (ruling that an employee only exceeds authorized access by hacking); *see also* Dial, *supra* note 5 (interpreting the Fourth Circuit's position to mean that CFAA liability may be imposed when an employee goes "beyond the bounds" of his authorized access").

49. *See* Orzechowski, *supra* note 18 (arguing that further CFAA interpretation is an issue that should be closely monitored); Abramowitz, *supra* note 36 (comparing the potentially detrimental effects of a Ninth Circuit CFAA interpretation with a Fourth Circuit CFAA interpretation).

authorization.[50] Any rights of authorization that the employee had were governed by the agency relationship, so once the relationship has been destroyed, authorized access is also destroyed.[51]

In addition, the Fifth and Eleventh Circuits focused on what the employer's terms-of-use policy consisted of as well as the employee's knowledge about the policy.[52] Based on the holdings in *John* and *Rodriguez,* liability under the CFAA may attach if a court finds that an employee accessed a protected computer in a way that was prohibited[53] or in excess of limitations set by a contract or a clearly communicated employer policy.[54] Conversely, the Ninth Circuit limits application of the term "exceeds authorized access" to situations relating to improper access of a computer and any information stored thereon, but it does not include the use of information that has been derived.[55] The Ninth Circuit explained that, based on legislative intent and legislative history, the CFAA was not meant to remedy misappropriated trade secrets where an employee is still authorized to access confidential information.[56] Under such a reading, nor

---

50. *Contra WEC Carolina Energy Solutions, LLC*, 687 F.3d at 206 (rejecting the idea that an employee who uses his computer access for a purpose that is not in sync with the employer's interest could be held liable under the CFAA).

51. *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d at 418 (7th Cir. 2006) (holding that an employee's authorization ends when he or she violates the duty of loyalty owed to the employer).

52. *See* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (condemning the employee's violation of the employee policy); United States v. Rodriguez, 628 F.3d 1258, 1260, 1265 (11th Cir. 2010) (holding that accessing confidential information for nonbusiness purposes exceeded the employee's authorized access).

53. *See Rodriguez*, 628 F.3d at 1260 (explaining that although Rodriguez, the employee, never signed a written acknowledgement of the policy warning employees that they faced criminal penalties if they violated policies on authorized use of databases, the court ultimately concluded that even though there was no formal written agreement in place, accessing information in violation of a corporate computer-use policy equated to "exceeding authorized access" under the CFAA).

54. *See John*, 597 F.3d at 273 (holding that John, the employee, exceeded her authorized access by violating her employer's clearly communicated and well-established policies that prohibited accessing customer data in furtherance of a criminally fraudulent scheme).

55. *See e.g.*, United States v. Nosal, 676 F.3d 854, 856-57 (9th Cir. 2012) (explaining the two schools of CFAA interpretation: the narrower interpretation believes "exceeds authorized access" refers to someone who is authorized to access only certain data or files but accesses unauthorized data or files; and those circuits that interpret the CFAA more broadly find "exceeds authorized access" refers to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information).

56. *See id.* at 857 (rejecting the government's broad interpretation of the CFAA that would "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute.").

does the CFAA apply to situations where an employee uses that confidential information, but did not access the computer and/or the information in excess of his or her access.[57]

Currently, employers have to be aware of which circuit court controls the jurisdiction in which their business is located so that they can properly protect trade secrets and confidential information.[58] However, most employers are unaware of the potentially devastating issues they may face in light of the CFAA.[59] In *Nosal*, the Ninth Circuit recognized that there is an extreme discrepancy in the application of CFAA law throughout the country because certain jurisdictions find CFAA-related behavior criminal, while others find it completely innocent.[60] Moreover, employee contracts and company policies are significantly affected by different interpretations of the CFAA throughout the country.[61] The Seventh Circuit provides employers with the broadest protections,[62] whereas the Ninth Circuit focuses more on the potential damage caused to average citizens by the broad interpretation, instead requiring employers to enforce meaningful restrictions on authorization and access for the CFAA to apply.[63]

There are several tools that can be used to properly interpret the CFAA, one of which is the rule of lenity.[64] The rule of lenity is a canon of statutory construction requiring all penal laws to be construed strictly in the

---

57. *See id.* (emphasizing that to adopt a narrower reading would result in millions of unsuspecting individuals finding that they are engaging in criminal conduct).

58. *See* Orzechowski, *supra* note 18.

59. *See id.* (suggesting that technical and physical security measures are more important in jurisdictions that interpret the CFAA under a Ninth Circuit analysis).

60. *See Nosal*, 676 F.3d at 862-63 (rejecting the broader interpretation of the CFAA promulgated by its sister circuits because these courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens).

61. *See id.* at 862 ("Not only are the terms of service vague and generally unknown—unless you look real hard at the small print at the bottom of a webpage—but website owners retain the right to change the terms at any time and without notice."); Stephanie Greene & Christine N. O'Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act*, 50 AM. BUS. L. J. 281 (2013) (arguing that restrictions on computer use policies have become blurry ever since more people have started to work from home).

62. *See generally* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 418 (7th Cir. 2006).

63. *See generally Nosal*, 676 F.3d at 862.

64. *See* Samantha Jensen, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 95-102 (2013) (discussing the relevant doctrines and canons of statutory construction that can be used to interpret the CFAA, including: the void for vagueness doctrine, the overbreadth doctrine, the rule of lenity, the plain language rule, and others).

name of fairness and notice because of the gravity of what is at stake.[65] The CFAA makes some actions criminally punishable by law, and therefore, where there is ambiguity in the language of this statute, the rule of lenity should apply.[66] The Ninth Circuit has adopted this narrow interpretation to prevent, "[making] criminals of large groups of people who would have little reason to suspect they [were] committing a crime."[67]

According to the Act's legislative history, the CFAA defined "exceeds authorized access" as an event where an individual accessed a "computer with authorization but used this access for purposes for which this authorization does not extend."[68] Legislative history suggests that this broad language was later replaced to "remove[] from the sweep of the statute one of the murkier grounds of liability, under which a[n] . . . employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances."[69] This statement exemplifies Congress's intent for the statute to be read narrowly and supports the Ninth Circuit's interpretations.[70]

III. A HYPOTHETICAL SITUATION THAT ILLUSTRATES THE POSITIVE AND NEGATIVE OUTCOMES OF THE DIFFERENT SCHOOLS OF THOUGHT CONCERNING THE CFAA

The following hypothetical exemplifies the confusion and ambiguity found within the circuit courts' respective interpretations.[71]

---

65. *See id.* at 98-99 (explaining that the rule of lenity embodies two important policies: (1) "citizens should be given fair warning in easily understood language of behavior that can result in criminal sanctions;" and (2) "laws with criminal penalties are a reflection of society's condemnation and should be defined by legislatures, not courts"); *see also* Greene, *supra* note 61 ("The rule of lenity, a rule of statutory construction for criminal statutes, requires a restrained, narrow interpretation.").

66. *See* Greene, *supra* note 61 (iterating that before applying the rule of lenity, a court must conclude that there is serious ambiguity or uncertainty in the statute that normal methods of statutory construction cannot resolve).

67. *See Nosal*, 676 F.3d at 862 (considering the dangers of turning the CFAA into a catch-all statute).

68. *See generally* S. Rep. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479 (adopting the narrower interpretation of the CFAA followed by the Ninth Circuit).

69. *See id.* at 21.

70. *See* Abramowitz, *supra* note 36 (addressing the Senate Judiciary Committee's approval of the amendment in 2011).

71. *See* Augello, *supra* note 2 (suggesting that CFAA resolution will not come soon); Orzechowski, *supra* note 18 (explaining that U.S. circuit courts have not provided clear guidance on the proper interpretation of the CFAA); *see also* Greene,

GWEN, Inc., a high-end fashion clothing and accessories company, serves clients primarily in the music and movie industries with its one-of-a-kind couture creations. Karen has been a well-respected employee of GWEN, Inc. for the past ten years, and now she wants to quit her job as the company's Senior Global Ambassador. Karen's duties included meeting with high-end clients, styling them for major red carpet and Hollywood events, traveling all over the world marketing the GWEN, Inc. brand, and looking for new and innovative styles that GWEN, Inc. could use in future clothing collections. Karen supervises many people, and most of her managerial work consists of training young and future global ambassadors for GWEN, Inc.

Since joining GWEN, Inc., Karen has developed priceless relationships with Hollywood clients, designers, stylists, photographers, and magazine editors for the high-end clothing company. She is deeply familiar with the intricacies of the fashion industry, and she has decided to quit her job at GWEN, Inc. and pursue her life-long dream of becoming a fashion designer.

Karen hopes to start her own fashion line and develop it into a brand. While she can handle the artistic side of creating a new company, she does not know anything about the financial planning that comes with it. She remembers that one of her friends, Emily, who also works at GWEN, Inc., works in the finance department of the company. Karen tells Emily about her plans, and Karen offers Emily a position at her new company as its Chief Financial Officer, a position much higher, both in salary and in prestige, than the job Emily currently possesses at GWEN, Inc. Emily jumps at the opportunity to receive a raise and gain more power in her career.

However, to turn this dream into reality, Karen needs GWEN, Inc.'s financial records to see the company's contractual obligations, the monetary value of those contracts, and the company's tax planning information. Karen wants to use this confidential information to help kick-start her new company, but since she left GWEN, Inc., she no longer has access to this type of confidential information and needs Emily's help before she resigns. Emily agrees and sends Karen the sensitive tax information and trade secrets.[72]

---

supra note 61 (arguing that restrictions on computer use policies have become confusing due to society's technological advancement and shifting work style).

72. *See* Ramon A. Klitzke, *The Uniform Trade Secrets Act*, 64 MARQ. L. REV. 277, 278 (1980-1981) (explaining that the Uniform Trade Secrets Act defines a trade secret as "information, including a formula, pattern, compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.").

Now that Karen has GWEN, Inc.'s financial records, she decides to start contacting all of the people that she cultivated professional relationships with over the years while working at GWEN, Inc. However, she created these relationships as a representative of, and on behalf of GWEN, Inc., but now wants these clients to work exclusively with her new company. Even though the clients worked with Karen directly while she was at GWEN, Inc., more senior officials would make the arrangements. The client contracts would be signed with GWEN, Inc. and not Karen, since celebrities and other famous stars do not want many people to know their personal information. Apart from safety issues, celebrities love to shock the public, so before they go on stage or the red carpet, they keep private "who" they will be wearing. Therefore, only a handful of people actually know before the big debut with Karen being one of them.

According to GWEN, Inc.'s employee manual and terms-of-use policy, any and all confidential information is to remain within the confines of the company, GWEN, Inc., and distribution of any of this information is strictly prohibited. Once a person is no longer an employee of GWEN, Inc., whether voluntarily or involuntarily, the agency relationship with GWEN, Inc. and all powers, access, and confidential information about the company cease to exist. When applied to these set of facts, the Seventh Circuit analysis and the Ninth Circuit Analysis can cause vastly distinct results.[73]

A. Under a Seventh Circuit Analysis, Karen Will Most Likely Be Found Guilty of Violating the Computer Fraud and Abuse Act Because the Seventh Circuit Provides Broad Employer Protections in These Situations

If the reviewing court applies the broad Seventh Circuit standard of the CFAA, both Karen and Emily will be held liable because of the Seventh Circuit's employer-friendly reading of the CFAA.[74] In the Seventh Circuit,

---

73. *See supra* note 9.

74. *See* United States v. Teague, 646 F.3d 1119, 1125 (8th Cir. 2011) (convicting an employee for improperly accessing President Obama's student loan records); United States v. Rodriguez, 628 F.3d 1258, 1261, 1264 (11th Cir. 2010) (ruling that an employee exceeded authorized access by reviewing personal records of numerous different individuals for nonbusiness reasons—that he did not use the information to defraud anyone or gain financially is irrelevant); United States v. John, 597 F.3d 263, 270 (5th Cir. 2010) (holding that an employee only had authorized access to certain information for specific reasons, so when she accessed it under other pretenses, she violated the CFAA); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 431 (7th Cir. 2006) (finding a violation of the CFAA when the agency relationship terminated due to the employee's violation of his employment contract); *see also* Augello, *supra* note 2 (analyzing the various competing discrepancies in CFAA interpretations).

any employee that accesses information on a computer to the detriment of his employer has violated a duty of loyalty under agency law, which in effect terminates the agency relationship and gives him no proper authorization.[75] Any rights that the employee had were governed by the agency relationship with the employer, so any employee-authorized access expires once the agency relationship has been violated.[76]

The First Circuit also contributed to this school of thought by holding that an employee exceeds authorized access by violating both use and access restrictions.[77] This suggests that whenever an employee violates his or her employer's company employee manual or terms of use agreement,[78] he or she loses the permitted access once received as an employee, and therefore, any sensitive information used or obtained after this gross violation is a serious breach of the CFAA.[79]

In the proposed hypothetical, and under a Seventh Circuit analysis, any

---

75. *See Int'l Airport Ctrs., LLC*, 440 F.3d at 419 (finding that an employee is without authorization once he violates his fiduciary duty of loyalty to his employer); *see also Teague*, 646 F.3d at 1121(stating that employees violate the CFAA when they abuse their privileged access to confidential information); *Rodriguez*, 628 F.3d at 1261 (clarifying that the CFAA states that merely accessing information by exceeding authorized access constitutes criminal conduct under the CFAA); *John*, 597 F.3d at 268 (rejecting the argument that the CFAA prohibits using authorized access to obtain or alter prohibited information but allows unlawful use of material that was gained through authorized access); Field, *supra* note 2 (explaining that an employee's adverse interests are enough to terminate an agency relationship in employment cases).

76. *See Int'l Airport Ctrs., LLC*, 440 F.3d at 419 (analyzing the role of agency relationships in CFAA interpretation); *see also Teague*, 646 F.3d at 1121 (stating that an employee prohibited from accessing information without proper authorization will be held liable under the CFAA); *Rodriguez*, 628 F.3d at 1261 (holding that accessing confidential information without permission is a violation of the CFAA); *John*, 597 F.3d at 268 (claiming that the employee violated the CFAA once she committed the acts adverse to her employer's interest).

77. *See generally* EF Cultural Travel v. Explorica, 274 F.3d 577, 577 (1st Cir. 2001); Field, *supra* note 2 (arguing that clear contracts are the best mechanisms for employers to protect themselves from employees who want to steal their confidential business information).

78. *See* Field, *supra* note 2, at 828 ("Language within employment contracts and documents can vary greatly, with some having only vague reference to employees maintaining confidentiality and not exposing trade secrets, and others explicitly stating that employees are not authorized to access or distribute certain confidential company information.").

79. *See EF Cultural Travel*, 274 F.3d at 583 (arguing that employee manuals and policies are good tools for employers to protect themselves, but they are not enough in certain jurisdictions); *see also id.* (explaining that most courts require the contracts or terms to explicitly state the limits of employees' authorization); Orzechowski, *supra* note 18 (explaining that the Fifth Circuit considers "exceeding authorized access" to include accessing information for purposes other than those permitted by one's employer).

access Karen had to confidential information was terminated the moment that she quit her job at GWEN, Inc. Whether or not Karen herself logged onto a GWEN, Inc. computer is unimportant for the purposes of this analysis, as she still used and obtained the information once her agency relationship with GWEN, Inc. ceased.

Another critical point is that Karen plans to use this confidential information to the detriment of GWEN, Inc. She intends to steal GWEN, Inc.'s celebrity clients as well as any potential future contracts it may have with others in the industry, such as magazine editors, photographers, and other high-end fashion designers to further the future success of her own business. Much like the employee in *International Airport Centers, LLC*, Karen had decided to quit her job in violation of her employment agreement to start a competing business.[80] Karen also resembles the employee who exceeded authorized access when he obtained President Obama's student loan records in *Teague*. The personal information concerning magazine editors, photographers, clients, and other powerful figures in the fashion industry was just as confidential to GWEN, Inc. as President Obama's student loan records are to the President himself.[81]

Karen also wants to know how GWEN, Inc. pays its taxes and any of its other financial planning information. This information could provide Karen with the opportunity to copy the company's contractual plans and trade schemes, and it would also allow her to expose and blackmail GWEN, Inc. if she were to become aware of tax evasion, unfair employee-pay practices, or other unjust and deceptive behavior. If Karen were to take advantage of any of these opportunities, such action would certainly be to the detriment of GWEN, Inc. as a leading retailer in the fashion world.

Emily would also be held liable under the Seventh Circuit's interpretation of the CFAA.[82] Even though she is still an employee of GWEN, Inc. and she has the authority to access the company's financial records, it is well outside the scope of her authority to share this confidential and sensitive information with Karen given that she is no longer an employee of GWEN, Inc.[83] Under a similar First Circuit

80. *See Int'l Airport Ctrs., LLC*, 440 F.3d at 428 (finding a violation of the CFAA when, after the employee had quit his job—thereby losing access authorization as he breached his fiduciary duty—he continued to access confidential information).

81. *See Teague*, 646 F.3d at 1123 (focusing on the employee's detrimental decision to take advantage of her privileged position of power).

82. *See Int'l Airport Ctrs., LLC*, 440 F.3d at 425 (noting that accessing and disclosing trade secrets can be a violation of unauthorized access); *see also* Field, *supra* note 2 (arguing that Congress may have kept the statute broad so that it could cover all situations of computer misuse and not just computer hacking).

83. *See EF Cultural Travel*, 274 F.3d at 583-84 (holding that, despite the fact that

analysis, Emily would be exceeding the bounds of her confidentiality agreement with her employer.[84]

Moreover, Emily has clearly violated her duty of loyalty to GWEN, Inc. under the theory of agency law.[85] Emily has breached GWEN, Inc.'s terms of use policy as well as the requirements set forth in GWEN, Inc.'s employee manual. However, if Emily is somehow able to show that the language in either or both of the agreements was ambiguous, that she had no knowledge of the restrictions, or that she did not have proper understanding of the terms of both policies, then she may have a reasonable defense.[86] Emily is like the employee in *Rodriguez* who exceeded his authorized access when he used the Social Security Administration's database to gather information on potential romantic partners because Emily is accessing GWEN, Inc.'s information for her own personal advancement with the goal of landing a better job at Karen's new company in mind.[87] Emily undoubtedly intended to cause harm to her employer by accessing the confidential information, which was only furthered by her subsequent detrimental action of sending the information to Karen. The actions of accessing and sending the proprietary information to Karen terminated the agency relationship that Emily had with GWEN, Inc., and she no longer has proper authorization to proceed with authorized access into the company's computer, its secret files, or its data.[88]

---

he was authorized to use the company's website as it was open to the public, the employee exceeded his authorization by using confidential information to obtain better access than other members of the public).

84. *See id.* at 583 (explaining that not only authority, but also the scope of an employee's authority, is an important factor to consider when determining CFAA liability).

85. *See* Orzechowski, *supra* note 18 (discussing the Seventh Circuit's broadest interpretation of the CFAA); *see also* ALLEN, *supra* note 8 (explaining the theories of agency law in terms of fiduciary duties).

86. *Contra* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (finding that the employer's official policy, which was reiterated in training programs that the employee attended, prohibited misuse of the company's internal computer systems and confidential customer information. Despite being aware of these policies, "the employee accessed account information for individuals whose accounts she did not manage, removed this highly sensitive and confidential information from [the employer's] premises, and ultimately used this information to perpetrate fraud").

87. *See* United States v. Rodriguez, 628 F.3d 1258, 1260-61 (11th Cir. 2010) (explaining that accessing information for an employee's personal reasons exceeds the scope of authorization); *see also* United States v. Teague, 646 F.3d 1119, 1122 (8th Cir. 2011) (clarifying that the employee exceeded authorized access when she did so to further personal interests).

88. *See Teague*, 646 F.3d at 1119, 1126 (8th Cir. 2011) (ruling that the employee's use of the information is irrelevant, if it is obtained without authorization); *Rodriguez*, 628 F.3d at 1263 (holding that an employee exceeds authorized access when his

There are important similarities between Emily in the proposed hypothetical and the employee in *John*.[89] Emily, who legally accessed GWEN Inc.'s confidential financial files and gave them to Karen, is like the employee in *John*, who in similar circumstances legally accessed customer account information and provided her half-brother with this sensitive information, so that they could incur fraudulent charges.[90] Emily, like the employee in *John*, should have known, or reasonably should have known, that she was not authorized to access a computer in furtherance of an action that violates the terms of use, company policy, or, in the case of *John*, the law.[91] Emily exceeded the purpose for which her access was given. She most likely knew that she was violating GWEN, Inc.'s company policy, and she should have known that she was outside the scope of her access when she wanted to share GWEN, Inc.'s confidential trade secrets.[92]

B. Under a Ninth Circuit Analysis, Karen Will Most Likely Be Found Not Guilty of Violating the Computer Fraud and Abuse Act Because the Ninth Circuit Provides Narrow Employee Protections in These Situations

If the reviewing court applies a Ninth Circuit analysis of the CFAA, both Karen and Emily will most likely be found innocent because the Ninth Circuit affords employees more protection.[93] In *Nosal*, the Ninth Circuit

---

interest in acquiring the confidential information is in conflict with his employer's interest); *John*, 597 F.3d at 271 (emphasizing that going beyond the limits of authorization may constitute a CFAA violation); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d at 421 (7th Cir. 2006) (explaining that adverse employer-employee interests in terms of agency law may produce a violation of the CFAA).

89. *See John*, 597 F.3d at 269 (noting that the employee exceeded her authorized access when she intended on using her employer's confidential information for purposes other than those for which she was given permission by her employer).

90. *See id.*

91. *Id.* at 271 (explaining that an employee would exceed authorized access if he or she used that access to obtain or steal information to the detriment of his or her employer as part of a criminal scheme).

92. *See id.*

93. *See* United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (cautioning that a broad interpretation would create precedent for employers to threaten to report minor violations); *see also LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009) ("[F]or purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations."); *see also* Dial, *supra* note 5 (discussing the importance of the Ninth Circuit's reasoning in *Nosal* as it pertains to practical societal implications); *see also* Orzechowski, *supra* note 18

limited application of the term "exceeds authorized access" to situations relating to improper access of a computer and its information, but it does not include the use of information that has been derived.[94] Therefore, an individual "exceeds authorized access" by violating a restriction on access to a work computer but not a restriction on use of a work computer and its contents.[95]

In the proposed hypothetical, Karen never improperly accessed a computer or its information; she only used information that was derived by Emily. Much like the employee in *WEC Carolina Energy Solutions, LLC*, who used his former employer's confidential business information to develop a competing business, Karen is unlikely to be held liable under the CFAA because she did not access the files illegally.[96] Additionally, like the employee in *Nosal* who convinced his former colleagues to download and send him confidential information from their firm to him, Karen convinced Emily, a former GWEN, Inc. colleague of hers, to download GWEN, Inc.'s confidential financial information and send it to her.[97] Therefore, Karen never exceeded authorized access by violating any access restrictions because she never utilized GWEN, Inc.'s computers improperly; she did not even touch the computer.[98]

(advising employers to be careful in managing employee access to proprietary information and emphasizing the importance of technical and security measures to protect employers because in jurisdictions with a narrower interpretation, the CFAA does not easily apply).

94. *See Nosal*, 676 F.3d at 863 (noting that the CFAA was intended to combat hacking, not unauthorized use of information); *see also* Abramowitz, *supra* note 36 (noting that the opinions in the Fourth and Ninth Circuits find that the CFAA only addresses an employee's improper access, not improper use of confidential information).

95. *See Nosal*, 676 F.3d at 863 (finding that "exceeds authorized access," refers to data or files on a computer that one was not authorized to access by one's employer); *see also LVRC Holdings, LLC*, 581 F.3d at 1134 (ruling that it is the employer's actions rather than the employee's state of mind that determines an employee's authorized access).

96. *See* WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012).

97. *See Nosal*, 676 F.3d at 856; *see also LVRC Holdings, LLC*, 581 F.3d at 1134 (holding that the employee did not exceed his authorized access when he e-mailed documents from his work computer to his personal computer because he had permission to use his employer's computer).

98. *See Nosal*, 676 F.3d at 862 (adopting a broad CFAA interpretation); *see also Abramowitz*, *supra* note 36 (noting that the Fourth and Ninth Circuits find that the CFAA only addresses an employee's improper access, as opposed to improper use which is not taken into account); Orzechowski, *supra* note 18 (explaining that employee access to information should be expanded only if and when necessary under a Ninth Circuit analysis).

Emily would also not be held liable under a Ninth Circuit analysis because even though she accessed a work computer to gain the confidential information, her access was legal.[99] She may have handed it over to Karen, who breached a duty of loyalty, but under the Ninth Circuit's reading of the CFAA, the statute does not apply to individuals that have authority to access a computer but later misuse the information.[100] Therefore, Emily's actions would be found to be lawful.

IV. THE NINTH CIRCUIT'S INTERPRETATION IS THE PROPER ANALYSIS OF THE CFAA

Today, the employment landscape is fraught with different jurisdictional interpretations of the CFAA. Thus, employers must be mindful of the split in authority to properly protect their computer systems, trade secrets, and confidential information. For example, in those jurisdictions where the CFAA is interpreted broadly, employers ought to clearly define all terms in their employee manuals and specify what it means to misuse confidential information.[101] Having these detailed documents, in addition to a training program, may be sufficient to prove that an employee was aware of and understood the rules by which he or she was governed.[102] Conversely, in jurisdictions where the Ninth Circuit's narrow approach is taken, employers ought to put in safeguards to limit any access of confidential information by its employees in an effort to expose them only to the information that they need to know.[103] This continued split requires either a legislative or judicial fix.

Given that courts are split as to how to apply the CFAA,[104] especially as it pertains to the interpretation and understanding of the term and phrase

---

99. *See Nosal*, 676 F.3d at 859 (discussing that those courts who have adopted a broad reading of the CFAA have "failed to consider the effect on millions of ordinary citizens" caused by the statute's ambiguous language); *see also LVRC Holdings, LLC*, 581 F.3d at 1131 (noting that the CFAA prohibits a number of different computer crimes).

100. *See Nosal*, 676 F.3d at 856 (applying the plain language of the CFAA to an analogous situation).

101. *See* Orzechowski, *supra* note 18 (discussing the importance and responsibility that employers have in setting the stage of a possible CFAA claim through their contracts and employee manuals).

102. *Id.*

103. *See id.* (emphasizing that employers can be left extremely vulnerable in jurisdictions that adopt Ninth Circuit interpretations if they don't take proper precautions).

104. *See* 18 U.S.C. § 1030 (2010); *see also* Orzechowski, *supra* note 18 (indicating that Court confusion in regards to CFAA interpretation will continue until Congress or the Supreme Court steps in).

"authorization" and "exceeds authorized access,"[105] Congress should adopt the Ninth Circuit's narrow reading[106] as the appropriate interpretation. Originally enacted as an anti-hacking statute, Congress was unable to predict how the CFAA would apply to modern cases due to vast technological advancement.[107] However, as the Ninth Circuit acknowledged, the rule of lenity[108] provides some guidance in its requirement that penal laws be construed strictly to give fair notice.[109] Absent fair notice, there exists the ability to "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime," an outcome unlikely intended by Congress.[110]

As mentioned, interpretation under a broader regime could result in several unintended outcomes impacting corporate culture. First, if a broad interpretation of the CFAA is adopted, then there is a grave risk that people will be held criminally liable for actions that they believed to be legal.[111] This is particularly true as it pertains to terms of use and terms of service. In an age where policies and their legally binding terms can change with the click of a mouse and with no requirement to notify the public at large, everyday computer users run the risk of violating provisions of the CFAA.[112]

Second, a broad reading of the CFAA would result in extreme

---

105. *See* Augello, *supra* note 2 (noting that definitions of key terms in the CFAA still remain unsettled).

106. *See* United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (interpreting the CFAA as targeting "the unauthorized procurement or alteration of information, not its misuse or misappropriation").

107. *See* Justin Precht, Comment, *The Computer Fraud and Abuse Act or the Modern Criminal at Work: The Dangers of Facebook from Your Cubicle*, 82 U. CIN. L. REV. 359, 365 (2013) (explaining that the CFAA was originally enacted as legislation to deal with technological advancement at the time that it was passed); *see also* Orzechowski, *supra* note 18 (stating that district courts in the Second, Fourth, Sixth, Eighth, and Tenth Circuits have also adopted narrow interpretations of the CFAA).

108. *See supra* notes 64-66 and accompanying text.

109. *See* Orzechowski, *supra* note 18 (stating that the Ninth Circuit focused on the rule of lenity when deciding *Nosal*).

110. *Nosal*, 676 F.3d at 859 ("While ignorance of the law is no excuse, [the Ninth Circuit] can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer.").

111. *See* Orzechowski, *supra* note 18 (listing the Fifth, Seventh, and Eleventh Circuits as also adopting broader interpretations of the words, "authorization" and "exceeds authorized access" so that they include violating terms of use policies and breaches of the duty of loyalty under the theory of agency law).

112. *Nosal*, 676 F.3d at 862 (explaining that given the ease with which these terms can change, "behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.").

punishments for very minimal acts both in and out of the workplace. For example, as the Ninth Circuit explained in *Nosal*, "minor dalliances," like checking Facebook or Instagram on a work computer, would become criminally punishable by federal law.[113] Even outside of the employment context, many websites accessed by everyday users prohibit the posting of misleading information or access to minors.[114] While there may be menial punishments for such errors in judgment, they ought not amount to a prison sentence.

Recent congressional action on the part of Senator Patrick Leahy (D-VT) proposes that the CFAA should be amended to adopt the narrow view of the Ninth Circuit.[115] Senator Leahy has introduced the amendment to say that a "Computer Fraud and Abuse Act action may not be brought where the sole basis for determining unauthorized access to a computer is an alleged violation of an acceptable use policy or terms of service agreement with an Internet service provider, Internet website, or non-government employer."[116] Congress should adopt this new language, so that employers, employees, and courts can have a better understanding of when the CFAA does and does not apply.

The United States Supreme Court should also seek certiorari on this circuit split to ameliorate the confusion associated with the Act's interpretation. If the Supreme Court were to decide the scope of the CFAA's interpretation, the lower courts would be able to apply it in a uniform fashion. However, in 2012 the United States government declared that it would not seek Supreme Court review of the Ninth Circuit's decision in *Nosal*.[117] Therefore, the Circuit split will continue to reign over CFAA case law for the near future unless a legislative fix is successfully adopted.

---

113. *See supra* note 46; *see e.g., Nosal*, 676 F.3d at 861 ("Adopting the government's interpretation would turn vast numbers of teens and pre-teens into juvenile delinquents—and their parents and teachers into delinquency contributors.").

114. *Nosal*, 676 F.3d at 861-62 (providing examples from eHarmony to eBay of the multitude of ways that the average computer users could violate the CFAA under a broad interpretation).

115. *See* Abramowitz, *supra* note 36 (assessing the past and present Congressional action in regards to CFAA amendments).

116. *See id.* (addressing the present and possibly future political and judicial action in regards to the CFAA).

117. *See* Grant McCool, *U.S. Will Not Challenge Computer Fraud Case to High Court*, REUTERS (Aug. 9, 2012), http://www.reuters.com/article/2012/08/08/net-us-computerfraud-law-idUSBRE8771BK20120808 (interpreting the repercussions of not seeking certiorari of the *Nosal* case); *see also* Dial, *supra* note 5 (arguing that the CFAA issue will be prolonged since the *Nosal* case will not be up before the Supreme Court).

CONCLUSION

The circuit split has a significant impact not only on employer-employee relationships in a business setting, but also on the judges throughout the country who struggle with how to interpret and apply the CFAA. Congress intended for the CFAA to combat hacking, but as society continues to develop and utilize advanced technologies, employers have to grapple with new issues concerning computers and confidential information. With two different standards of application, courts are lacking adequate guidance on where they should fall on the spectrum.

There are only two available and complicated redresses to solve this conflict. One is for Congress to amend the current CFAA and to reflect one of the two schools of thought. Another possibility is for the Supreme Court to directly address the ambiguities created by the Seventh and Ninth Circuits.