University of Cincinnati Law Review

Volume 82 | Issue 1 Article 10

September 2014

The Computer Fraud and Abuse Act or the Modern Criminal at Work: The Dangers of Facebook from Your Cubicle

Justin Precht

THE COMPUTER FRAUD AND ABUSE ACT OR THE MODERN CRIMINAL AT WORK: THE DANGERS OF FACEBOOK FROM YOUR CUBICLE

Justin Precht

I. INTRODUCTION

In 1986, the United States House of Representatives stated, "Computers are rapidly becoming as much a part of American Life as the telephone, automobile, typewriter or our everyday transaction at, for instance, the supermarket."[1] Accordingly, legislation was needed to address the "vast potential for significant criminal activity . . . because the criminal justice system [was] ill-equipped to deal with th[e] changing technology."[2] Congress responded by enacting the Computer Fraud and Abuse Act (CFAA) of 1986 in order to address security concerns arising in conjunction with the rapid growth of computer use.

Section 1030(a)(2)(C) of the CFAA criminalizes "exceeding authorized access" in order "to obtain information from any protected computer."[3] Currently, the circuit courts are split on what it means for an individual to "exceed authorized access" in disputes between employers and former employees arising under employee access provisions of the CFAA.[4]

This Comment focuses on the circuit courts' disagreement on what it means to "exceed authorized access" in employer–employee disputes. Part II examines the legislative history and purpose of the CFAA. Part III examines circuit court decisions that have employed a broad interpretation of the CFAA and the "exceeds authorized access" language, and those decisions employing a narrow interpretation. Part IV will provide an analysis of the varying interpretations and address why the narrow interpretation should be adopted. Part V concludes this Comment and suggests that the rule of lenity requires the narrow interpretation, which more accurately reflects the legislative intent in enacting the CFAA and adheres to principles of statutory interpretation and Constitutional Due Process. The conclusion further argues that the Legislature should amend the CFAA in order to promote certainty and uniformity in the law.

1. H.R. REP. NO. 99-612, at 4 (1986).
2. *Id.* at 5.
3. 18 U.S.C. § 1030 (2012).
4. *See* discussion *infra* Part III.

II. BACKGROUND

Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act as part of the Comprehensive Crime Control Act (CCCA) of 1984.[5] The CCCA made it a crime for a person to "knowingly access a computer without authorization or having accessed a computer with authorization, use[] the opportunity such access provides for purposes to which such authorization does not extend" in order to knowingly use, modify, destroy, or disclose information in, or prevent authorized use of, the computer.[6] However, the CCCA limited this offense to instances where the computer was under the control of the federal government.[7] Additionally, the CCCA stated that it was not an offense to access a computer with authorization and to use "the opportunity such access provides for purposes to which such access does not extend, if the us[e] of such opportunity consists only of the use of the computer."[8]

Section 1030 of Title 18 of the United States Code was amended in 1986 to create the CFAA. Congress specifically cited that one of the purposes for the amendment was to address a new breed of criminal born out of recent technological advancements: "the technologically sophisticated criminal who breaks into computerized data files."[9] The amendment also addressed the lack of legislation regarding theft or damage to computers, as federal enforcement previously relied on prior legislation "designed for other offenses such as mail fraud (18 U.S.C. 1341) or wire fraud (18 U.S.C. 1343)."[10] The 1986 amendment remained limited to acts affecting federal government computers, but it expanded the CFAA to make it a criminal offense to "knowingly access a computer without authorization or to exceed authorized access."[11]

The CFAA remained limited until Congress passed the Economic Espionage Act of 1996 (EEA). The EEA was created, in part, because "[t]he United States produce[d] the vast majority of the intellectual property in the world" and "[t]he value of the information [was] almost entirely dependent on its being a closely held secret."[12]

---

5. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2101, 98 Stat. 1837, 2190-92 (1984).

6. *Id.* at 2190.

7. *Id*. at 2191. Section (a)(3) made it a crime where the computer "is operated for or on behalf of the Government of the United States and such conduct affects such operation."

8. *Id*.

9. H.R. REP. NO. 99-612, *supra* note 1, at 3.

10. *Id.* at 4.

11. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986) (current version at 18 U.S.C. § 1030 (2012)).

12. S. REP. NO. 104-359, at 6 (1996).

> This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft. The information is pilfered by a variety of people and organizations for a variety of reasons. A great deal of the theft is committed by disgruntled individuals or employees who hope to harm their former company or line their own pockets. In other instances, outsiders target a company and systematically infiltrate the company then steal its vital information. More disturbingly, there is considerable evidence that foreign governments are using their espionage capabilities against American companies.[13]

At that time, federal law was insufficient to protect a company's valuable information and Congress acknowledged concerns with both employee and outsider espionage. The reach of the CFAA was expanded substantially by criminalizing the procurement of "information from any protected computer if the conduct involved an interstate or foreign communication."[14] Thus, by 1996 the CFAA protected a company's proprietary information and could be used in actions by private employers against their employees. In short, the 1986 amendment was responsible for broadening the language of the statute to cover instances where a person "exceeds authorized access," and the 1996 amendment substantially broadened the scope beyond mere misuse of government owned computers.[15]

The current CFAA, as amended in 2008, makes it a crime under Section 1030(a)(2)(C) when an individual "intentionally accesses a computer without authorization or exceeds authorized access" to obtain "information from any protected computer."[16] Similarly, Section 1030(a)(4) states that it is a crime when someone "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."[17] The CFAA defines "exceeds authorized access" in Section 1030(e)(6) as accessing "a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[18] Section 1030(g) allows an individual "who suffers damage or loss" as a result of a violation to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other

13. *Id.*

14. 18 U.S.C. § 1030 (2012).

15. The CFAA was further amended in 2001 and 2002; however, these amendments did not substantially alter the scope as to the provisions discussed in this Comment.

16. 18 U.S.C. § 1030 (2012).

17. *Id*.

18. *Id*.

equitable relief."[19]

III. THE CIRCUIT SPLIT

The circuits are split on how to interpret the "exceeds authorized access" language of the CFAA. The Seventh, Fifth, First, and Eleventh Circuits have utilized a broad interpretation. The Seventh Circuit employs an agency approach, while the Fifth, First, and Eleventh Circuits limit authorized access to access authorized by the employer, so an employee may have physical access to a computer, but is limited in the ways he can use the information on that computer. The Ninth and Fourth Circuits, utilizing the narrow interpretation, have limited "exceeds authorized access" to activities synonymous with hacking.

A. Broad Interpretation of "Exceeds Authorized Access"

The Seventh Circuit addressed the CFAA's "exceeds authorized access" language in *International Airport Centers, L.L.C. v. Citrin.* The defendant was a former employee of International Airport Centers (IAC) who, prior to quitting to start his own business, deleted all of the data on the laptop that IAC had provided him, which included not only information he had been collecting during the course of his employment but also evidence of his improper conduct.[20] The Seventh Circuit applied agency principles and held the defendant breached his duty of loyalty when he acted on interests that were adverse to those of his employer, namely breaching his employment contract to pursue his own business.[21] The breach of the duty of loyalty "terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship."[22] Thus, the defendant "exceeded authorized access" when, no longer an agent of IAC, he accessed the laptop in his possession and "used such access to obtain or alter information in the computer" that he was "not entitled so to obtain or alter."[23]

The Seventh Circuit's agency approach to "exceeding authorized access" made little effort to determine the legislative intent behind the CFAA or to provide a solid definition of "exceeds authorized access." Rather, the Seventh Circuit glossed over the "exceeds authorized access" issue and transposed common law agency principles onto the

19. *Id.*
20. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).
21. *Id.* at 420–21.
22. *Id.*
23. 18 U.S.C. § 1030(e)(6) (2012).

criminal statute to determine that an individual "exceeds authorized access" whenever acting on an interest adverse to that of her employer.

The Fifth Circuit similarly advocated for a broad interpretation of "exceeds authorized access." However, counter to the Seventh Circuit's agency rationale, the Fifth Circuit held that "exceeding authorized access" includes exceeding the purposes for which the employer authorizes access.[24] In *United States v. John*, the defendant was an account manager at Citigroup who accessed seventy-six corporate customer accounts and provided the information to her half-brother.[25] Her half-brother and his accomplices then incurred fraudulent charges on some of the accounts.[26] The court stated that an employee could "exceed authorized access" where the employee exceeds "the purposes for which access has been given."[27] The court reasoned that John's access to Citigroup's data was confined because "[s]he was not authorized to access that information for any and all purposes but for limited purposes."[28] The government had shown that "Citigroup's official policy, which was reiterated in training programs that John attended, prohibited misuse of the company's internal computer systems and confidential customer information," so John's authorized access did not extend to using the information to perpetuate fraud.[29] Thus, under the broad interpretation an employee violates the CFAA and exceeds his authorized access on a protected computer through activities outside of the scope of employer designated access.

The Fifth Circuit held that finding the CFAA to include authorized data the employee did not have access to or information used in carrying out a criminally fraudulent scheme would not in any way be surprising to the defendant.[30] This broad interpretation of the CFAA sets the level of authorization only so far as the bounds authorized by an employer and notes it is especially applicable where an employee is clearly part of a fraudulent scheme.[31] The rationale was that John knew she was aiding in the commission of a crime and knew that she was "exceeding authorized access" such that it would be fair to punish her under the statute.

The First Circuit also held in *EF Cultural Travel BV v. Explorica, Inc.* that access in the "exceeds authorized access" language was to be

24. United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).
25. *Id.* at 269.
26. *Id.*
27. *Id.* at 272.
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.* at 271–73.

determined by the employer. Explorica was a competitor of EF Cultural Travel BV (EF) in providing high school tours, and Explorica's vice president, Gormley, was a prior employee of EF.[32] Explorica designed and used a "scraper" program that focused solely on EF's website and would transfer its pricing information for tours back to Explorica.[33] The court held that Gormley exceeded authorized access where he entered into a broad confidentiality agreement which "prohibit[ed the] disclosure of any information 'which might reasonably be construed to be contrary to the interests of EF.'"[34] In providing Explorica proprietary information about the structure of EF's website and its tour coding system, Gormley exceeded his authorized access as defined by the confidentiality agreement.[35] Thus, the First Circuit held for the broad interpretation and limited authorized access to authorization the employer expressly allowed.

The Eleventh Circuit held that an employee had exceeded authorized access when he accessed the personal records of seventeen individuals for personal reasons in violation of company policy in *United States v. Rodriguez*.[36] Rodriguez worked as a TeleService representative for the Social Security Administration (SSA) where he had access to social security numbers, annual income, and other personal information.[37] While employed, Rodriguez would look up women he had met or knew.[38] The court stated that, since the policy of the SSA only authorized the use of the databases for business reasons, Rodriguez "exceeded authorized access" when he began looking up women for personal reasons.[39] Therefore, the *Rodriguez* decision also linked authorized access to that allowed under express company policy.

B. Narrow Interpretation of "Exceeds Authorized Access"

Other courts, led by the Ninth Circuit, have rejected the broad interpretation and adhere to a narrow interpretation of the CFAA that refuses to criminalize violations of employer computer use policies. In

32. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).

33. *Id.* The Court noted that "[l]ike a robot, the scraper sought information through the Internet. Unlike other robots, however, the scraper focused solely on EF's website, using information that other robots would not have. Specifically, [Explorica] utilized tour codes whose significance was not readily understandable to the public. With the tour codes, the scraper accessed EF's website repeatedly and easily obtained pricing information for those specific tours."

34. *Id.* at 583.

35. *Id.*

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

37. *Id.* at 1260.

38. *Id.* at 1261–62.

39. *Id.* at 1263.

LVRC Holdings L.L.C. v. Brekka, an employee at an addiction treatment center accessed and emailed company records from his employee email to his personal email.[40] The Ninth Circuit began its analysis stating "[t]he act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives.'"[41] The court then rejected the Seventh Circuit's reliance on agency principles in *Citrin*, determining that the agency approach would mean that an employee "exceeds authorized access" once his mental state changes from loyal employee to disloyal competitor."[42] More importantly, the court reasoned that since section 1030(a) of the CFAA is primarily a criminal statute, "any ambiguity should be resolved in the favor of lenity."[43]

The rule of lenity "vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed."[44] Thus, where an "employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA."[45] The court held that a person "exceeds authorized access" when the person uses a computer either without permission to use the computer for any purpose, like a hacker, or when the employer rescinds permission to access the computer.[46] In so holding, the court adopted the narrow interpretation of the "exceeds authorized access" language in the CFAA.

A later Ninth Circuit case, *United States v. Nosal*, furthered the narrow interpretation of the "exceeds authorized access" language in the CFAA. The case wavered between the broad and narrow interpretations as it wound its way through the system before the Ninth Circuit, sitting en banc, concluded the narrow interpretation was correct. Nosal was an employee at Korn/Ferry International (KFI), which provided executive recruitment services.[47] Nosal left to start a rival company, signed a separation agreement, and agreed to serve as an independent contractor

40. LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127, 1129–30 (9th Cir. 2009).

41. *Id.* at 1130 (quoting H.R. Rep. No. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)).

42. *Id.* at 1134.

43. *Id.* (quoting United States v. Carr, 513 F.3d 1164, 1168 (9th Cir.2008)).

44. *Id.* at 1134–35 (citing United States v. Santos, 553 U.S. 507, 514 (2008)).

45. *Id.* at 1135.

46. *Id.*

47. United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *1 (N.D. Cal. April 13, 2009).

to KFI for approximately one year.[48] In the separation agreement Nosal agreed not to compete with KFI in exchange for $25,000 per month as well as two lump-sum payments.[49] However, during this period Nosal, along with two coworkers, obtained "source lists and other custom reports of names and contact information from the KFI 'Searcher' database, a highly confidential and proprietary database of executives and companies."[50]

In 2009, the District Court for the Northern District of California acknowledged both the broad and narrow interpretations of "exceeds authorized access" before holding in favor of the broad interpretation.[51] The district court noted that Congress had expanded the scope of the CFAA since its enactment and that the rule of lenity was inapplicable because the statute was not ambiguous.[52] The court relied on the Seventh Circuit's use of agency principles in *Citrin* in holding that Nosal had "exceeded authorized access" in accessing KFI's database.[53]

However, driven by the Ninth Circuit's holding in *Brekka*, decided after the first *Nosal* decision, the district court granted reconsideration of *United States v. Nosal* in 2010. In its reconsideration, the district court followed *Brekka* and found that the broad interpretation was unworkable where "the defendant would have no reason to know that making personal use of the company computer against the employer's interest would constitute a criminal violation of the CFAA."[54] The district court noted that the "Ninth Circuit held that authorization hinges on the employer's conduct—has the employer granted the employee permission to access the computer?—not the employee's state of mind when accessing information or documents on the employer's computer."[55] The district court dismissed the CFAA charges and remarked that there was "simply no way" to read the definition of "exceeds authorized access" to include corporate computer-use policies.[56]

On appeal, the Ninth Circuit first focused on the text of the CFAA. It noted that the statute defines "exceeds authorized access" to mean "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

48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.* at *4–7.
52. *Id.* at *6–7.
53. *Id.*
54. *Id.* at *5 (quoting LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009)).
55. *Id.* (quoting *Brekka*, 581 F.3d at 1133).
56. *Id.* at *7.

obtain or alter."[57] The government argued, and the court accepted, that the narrow interpretation of "exceeds authorized access" made "so" superfluous in its definition.[58] The court held that the proper interpretation should be, "when the employee uses that authorized access 'to obtain or alter information in the computer that the accesser is not entitled [in that manner] to obtain or alter.'"[59] The Ninth Circuit emphasized that "[w]e decline to render meaningless a word duly enacted by Congress."[60] After justifying the broad interpretation on the statute's plain language, the Ninth Circuit distinguished *Brekka* on its absence of access restrictions. However, the court stated that "[o]ur decision today that an employer's use restrictions define whether an employee 'exceeds authorized access' is simply an application of *Brekka*'s reasoning."[61] The Ninth Circuit also looked to the decisions of the Fifth Circuit in *John*, the Eleventh Circuit in *Rodriguez*, and the First Circuit in *Explorica* for support of its new position.[62]

This decision could have ended the circuit split on the "exceeds authorized access" language and designated *Brekka* as applying only when there was no employee policy in place. However, the Ninth Circuit was not finished with this case and granted a rehearing en banc in 2012. The court made clear that they were deciding between two very different approaches to the CFAA:

> This language can be read either of two ways: [f]irst, as Nosal suggests and the district court held, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data: [h]e would "exceed [ ] authorized access" if he looks at the customer lists. Second, as the government proposes, the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. For example, an employee may be authorized to access customer lists in order to do his job but not to send them to a competitor.[63]

The court then acknowledged, but rejected, the government's statutory

57. United States v. Nosal, 642 F.3d 781, 785 (9th Cir. 2011).

58. *Id.* at 785.

59. *Id.* at 786–87.

60. *Id.* at 786 (citing *Corley v. United States*, 556 U.S. 303, 314 (2009) ("[O]ne of the most basic interpretive canons [is] that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." (internal quotation marks and alteration omitted)).

61. *Id.* at 787.

62. *Id.* at 788.

63. United States v. Nosal, 676 F.3d 854, 856–57 (9th Cir. 2012) (en banc).

argument that "entitled" should be interpreted in line with the dictionary definition of "to furnish with a right."[64] The court said the better interpretation is to simply treat "entitled" as a synonym for "authorized."[65] The Ninth Circuit then rejected the government's "so" argument because of concerns that adopting such a definition would transform the CFAA from an anti-hacking statute to an expansive misappropriation statute all because of a "two-letter word that is essentially a conjunction."[66] The Circuit court stated that "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose."[67] A major concern justifying the court's decision was the expansive scope of the broad interpretation.

The court acknowledged that Congress passed the initial version of the CFAA in 1984 for the express purpose of combating hackers.[68] The government contended that because "without access" applies to hackers, the "exceeds authorized access" provision must apply to people who have authorized access but exceed it.[69] The court stated that both provisions could apply to hackers, "without access" for external hackers and "exceeds authorized access" for internal hackers.[70] The Ninth Circuit expressed further concern in making criminals of people who would have no idea they are committing a federal crime.[71] The court stated that "while ignorance of the law is no excuse, we 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."[72]

Finally, the Ninth Circuit rejected the government's interpretation because of its breadth in regards to subsection 1030(a)(2)(C), "which [would] make[] it a crime to exceed authorized access of a computer connected to the internet *without* any culpable intent."[73] Under "the government's proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct."[74] Instead, the Ninth Circuit invoked common sense:

64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.* at 858.
69. *Id.*
70. *Id.*
71. *Id.* at 859.
72. *Id.*
73. *Id.*
74. *Id.*

> Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes. While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you *could* be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement.[75]

Therefore, in *Nosal*, the Ninth Circuit affirmed *Brekka*'s core holding and kept the circuit split alive by adopting the narrow interpretation of the CFAA. The Ninth Circuit was clearly uncomfortable in expanding the statute, originally designed to punish hacking, into one that could potentially cover any employee conduct outside the scope of an employer policy.

The Fourth Circuit's recent decision in *WEC Carolina Energy Solutions L.L.C. v. Miller* followed the Ninth Circuit's en banc decision in *Nosal*. In *Miller*, an employee left WEC Carolina Energy Solutions, Inc. (WEC) for its competitor Arc Energy Services, Inc. (Arc).[76] Before leaving, the employee downloaded and used WEC's proprietary information to make presentations to potential customers. The court acknowledged that the "crux of the issue is the scope of . . . 'exceeds authorized access.'"[77] The court followed *Brekka* and *Nosal* and held that it must interpret the ambiguous statute using the rule of lenity. "[I]n the interest of providing fair warning 'of what the law intends to do if a certain line is passed' we will construe this criminal statute strictly and avoid interpretations not 'clearly warranted by the text.'"[78] The court also used the dictionary definition of access which meant "[t]o obtain, acquire," or "[t]o gain admission to."[79] The Fourth Circuit committed to the narrow interpretation and clearly held: "we reject 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."[80]

Other courts are also following the Ninth Circuit's lead in adopting

75. *Id.* at 860.

76. WEC Carolina Energy Solutions L.L.C. v. Miller, 687 F.3d 199, 200 (4th Cir. 2012).

77. *Id.* at 203.

78. *Id.* at 204 (citations omitted).

79. *Id*.

80. *Id.* at 207.

the narrow interpretation of the CFAA. For example, the District Court for the Western District of Michigan decided *Dana Ltd. v. American Axle & Manufacture Holdings, Inc.* in June 2012. The court noted that "[t]he Sixth Circuit has not squarely addressed the meaning of 'without authorization' or 'exceeds authorized access' in the context of departing employees."[81] Yet, the court, reasoned that a prior Sixth Circuit decision, which relied on the Ninth Circuit's decision in *Brekka*, suggested that the Sixth Circuit would likewise adopt the narrow view.[82] The court acknowledged *Nosal* and other decisions of district courts within the Sixth Circuit and concluded the "[c]ourt agrees with the rationale of the district courts in this circuit, and joins these courts in concluding that the terms 'without authorization' and 'exceeds authorized access' in the CFAA must be given a narrow meaning."[83]

IV. DISCUSSION

The narrow interpretation of the "exceeds authorized access" language should be adopted for a number of reasons. First, the legislative history of the CFAA indicates that Congress intended "exceeds authorized access" to combat hacking. Second, the rule of lenity requires any ambiguity to be resolved in favor of the party accused of violating the law where the CFAA could potentially attach criminal liability. Third, constitutional due process concerns support a narrow interpretation of the statute. Finally, practicality and efficiency dictate limiting the use of the criminal statute in employer–employee disputes.

A. Congressional Intent

The House of Representatives Committee Report on the 1986 version of the CFAA stated in a section titled "Need for Legislation:"

> One somewhat unique aspect of computer crime is the expanding group of electronic trespassers—the so called 'hackers' who have been frequently glamorized by the media, perhaps because this image of the hacker is that of a bright, intellectually curious, and rebellious youth—a modern day Huck Finn. The fact is, these young thrill seekers are trespassers, just as much as if they broke a window and crawled into a home while the occupants were away. The Committee believes we should attempt to deter and educate these youths in order to prevent our

81. Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc., No. 1:10-CV-450, 2012 WL 2524008, at *4 (W.D. Mich. June 29, 2012).

82. *Id.*

83. *Id.* at *5.

hacker of today from becoming our white-collar criminal of the future.[84]

The legislative intent for the initial version of the CFAA was to combat the rise of hackers. In fact, the Committee Report's "Need for Legislation" focused primarily on two themes with almost equal recognition: the rapid growth of computer technology in everyday life and hackers.[85]

The Senate Committee Report addressed the same concerns:

> Th[e] technological explosion has made the computer a mainstay of our communications system, and it has brought a great many benefits to the government, to American businesses, and to all of our lives. But it has also created a new type of criminal—one who uses computers to steal, to defraud, and to abuse the property of others. The proliferation of computers and computer data has spread before the nation's criminals a vast array of property that, in many cases, is wholly unprotected against crime.[86]

The Senate Report then noted a group of hackers known as the "414 Gang," who had hacked the radiation treatment records of cancer patients.[87] The report stated, "the potentially life-threatening nature of such mischief is a source of serious concern to the Committee."[88] The Senate Report then acknowledged "pirate bulletin boards," also mentioned extensively in the House Report, which were a community system of computers accessed via phone that had computer passwords and other vital information.[89] These concerns suggest that the legislative intent behind the 1986 CFAA was to prevent harm caused by the sophisticated hacker.

Furthermore, the 1996 EEA opened the CFAA beyond only those offenses against United States government owned computers. This version of the CFAA protected "information from any protected computer if the conduct involved an interstate or foreign communication."[90] The Senate Committee Report stated:

> Only by adopting a national scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge and thus safeguard our national security. Foremost, we believe that the greatest benefit of the Federal statute will be as a powerful deterrent. In addition, a Federal criminal law is needed because of the international and interstate nature of this activity, because of the sophisticated

84. H.R. REP. NO. 99-612, *supra* note 1, at 5–6.
85. *Id.* at 4–6.
86. S. REP. NO. 99-432, at 2 (1986).
87. *Id.* at 2–3.
88. *Id.* at 3.
89. *Id.*
90. 18 U.S.C. § 1030 (2012).

> techniques used to steal proprietary economic information, and because of the national implications of the theft.[91]

The Report in its section titled "Increasing Incidents of Theft of Proprietary Economic Information" noted that "computer intrusions . . . account for the largest portion of economic and industrial information lost by U.S. corporations. Most American companies are poorly prepared to deal with these sophisticated and coordinated efforts to obtain their proprietary economic information."[92] Thus, the 1996 Senate Report also focused clearly on international hackers' access to vulnerable information.

Furthermore, the 1996 Committee Report addressed the rise of internal theft. One example the Report addressed was "an engineer for an automobile air bag manufacturer who asked the company's competition for more than half a million dollars" for a "laundry list" of "manufacturing designs, strategies, and plans."[93] Another was a "former employee of two major computer companies" who stole "vital information on the manufacture of microchips" and sold it "to China, Cuba, and Iran."[94]

All of the above Committee Reports addressed actions are covered by the narrow interpretation of the CFAA's "exceeds authorized access" language. Clearly hacking and foreign and internal espionage represent something more serious than actions that are merely beyond an express employer computer use policy. The legislative history acknowledges the threat of hacking and advanced espionage, but is lacking on actions like deleting the information on a work laptop seen in *Citrin* or using a work database to look at information for personal reasons in *Rodriguez*.[95]

The legislative intent argument is not addressed in the circuit court opinions adhering to the broad interpretation. However, legislative intent is raised by the Fourth Circuit in *WEC Carolina Energy Solutions*:

> Our conclusion here likely will disappoint employers hoping for a means to rein in rogue employees. But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or

91. S. REP. NO. 104-359, *supra* note 12, at 11–12.

92. *Id.* at 8.

93. *Id.*

94. *Id.* at 8–9.

95. *See id.* at 7–9; Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) (an employee who upon terminating his employment wiped his work laptop); and United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (a Social Security Administration employee who used his work access to spy on female acquaintances).

information in bad faith, or who disregard a use policy.[96]

Likewise, the Ninth Circuit raised the issue in *Nosal* stating that the "narrower interpretation" was "a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere."[97]

The Committee Reports for the multiple amendments to the CFAA support a narrow interpretation limited to hacking as seen in the Ninth and Fourth Circuit cases. The legislative intent argument is compelling because the 1986 Reports specifically mentioned hacking as a major impetus for the legislation.[98] Likewise, the 1996 Report focused on foreign and internal espionage.[99] There is some room for movement in the legislative intent argument, since the Report does not give internal espionage a clearly defined scope.[100] However, the Report does provide sufficiently egregious examples to differentiate the intent of the statute from the broad holdings of the Seventh, Fifth, First, and Eleventh Circuits.[101]

B. Rule of Lenity

Ambiguity concerning the scope of criminal statutes should be resolved in favor of lenity, meaning any doubts about an ambiguous statute should be resolved in favor of the defendant.[102] In *United States v. Bass* the Supreme Court stated that the "choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite."[103]

There are two principles behind the rule of lenity:

First, 'a fair warning should be given to the world in language that the

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

97. United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

98. *See* H.R. REP. NO. 99-612, *supra* note 1, at 5–6; S. REP. NO. 99-432, *supra* note 86.

99. *See generally* S. REP. NO. 104-359, *supra* note 12.

100. *Id.*

101. *Id.* The Report notes an engineer who stole manufacturing designs and plans who sold the information to company competition for half a million dollars; an employee for two major computer companies who sold information to China, Cuba and Iran; and an employee who worked at a computer firm that supplied software technology to various government projects like NASA who transmitted the source code to another person.

102. *See* United States v. Bass, 404 U.S. 336 (1971); United States v. Santos, 553 U.S. 507 (2008).

103. *Bass*, 404 U.S. at 347 (quoting United States v. Universal C.I.T. Credit Corp., 344 U.S. 218, 221–22 (1952)).

> common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so fair as possible the line should be clear.' Second, because of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity.[104]

The rule of lenity is a strong argument for the narrow interpretation of the CFAA statute for "exceeds authorized access."[105] The CFAA attaches a criminal penalty where a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[106] The Fourth and Ninth Circuits first found the statute ambiguous by relying on legislative intent and the plain meaning interpretation, and then applied the rule of lenity as support for adopting the narrow interpretation of the statute.

The Ninth Circuit reasoned:

> The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we 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.[107]

Additionally, the Ninth Circuit stated that section 1030(a)(2)(C), the section that primarily comes up in employee–employer disputes, is the broadest subsection and "makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent. Were we to adopt the government's proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct."[108]

The Ninth Circuit further reasoned that "employer–employee and company–consumer relationships are traditionally governed by tort and contract law," and "the government's proposed interpretation of the

104. *Id.* at 348 (citations omitted).

105. *But see* 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, 449 (2012) (citing Note, *The New Rule of Lenity*, 119 HARV. L. REV. 2420, 2423–24 (2006) (collecting cases)) (noting that "[t]he Supreme Court has increasingly watered down its formulation of the lenity rule, applying it only in the face of 'grievous ambiguity,' or only if 'after seizing everything from which aid can be derived,' the Court can make 'no more than a guess as to what Congress intended'").

106. 18 U.S.C. § 1030(a)(2)(C).

107. United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc).

108. *Id.*

CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law."[109] Furthermore, "[b]asing 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."[110]

The Fourth Circuit also applied the rule of lenity in adopting the narrow interpretation of "exceeds authorized access:"

> Thus, faced with the option of two interpretations, we yield to the rule of lenity and choose the more obliging route . . . . Here, Congress has not clearly criminalized obtaining or altering information "in a manner" that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter.[111]

The two circuits that adopted the narrow interpretation applied the rule of lenity because the statute was ambiguous. One reason criminal liability need not attach to the ambiguous statute, per the Fourth Circuit, was because "nine other state-law causes of action potentially provide relief, including conversion, tortious interference with contractual relations, civil conspiracy, and misappropriation of trade secrets."[112] The rule of lenity is especially applicable where the potential criminal liability subsumes so much seemingly innocuous daily activity.

C. Constitutional Due Process Concerns

A law may fail to meet the requirements of the Due Process Clause "if it is so vague and standardless that it leaves the public uncertain as to the conduct it prohibits or leaves judges and jurors free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case."[113] Thus, "[v]agueness may invalidate a criminal law for either of two independent reasons. First, it may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement."[114]

The broad interpretation of the CFAA's "exceed authorized access" language might violate both elements of the void-for-vagueness

109. *Id.* at 860.

110. *Id.*

111. WEC Carolina Energy Solutions L.L.C. v. Miller, 687 F.3d 199, 206 (4th Cir. 2012).

112. *Id.* at 207 n.4.

113. Giaccio v. Pennsylvania, 382 U.S. 399, 402–03 (1966).

114. City of Chicago v. Morales, 527 U.S. 41, 56 (1999).

doctrine.[115] It is highly unlikely that employees in the workforce are aware they are potentially violating federal law when they spend a small portion of their time at the office casually browsing the internet. Whether or not such access would be considered a federal criminal infraction would depend on the state and the employer's acceptable use policy. The CFAA, a criminal law, fails to provide adequate notice of liability to otherwise reasonable, law-abiding citizens. "Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read."[116] A criminal statute that includes seemingly harmless, everyday activity is vague in that it surprises ordinary people.

In addition, the interpretation that relies on computer-use policy is also likely overbroad, in that arbitrary enforcement necessarily follows a statute that potentially criminalizes daily activity.[117] The Ninth Circuit in *Nosal* discussed *United States v. Kozminski*, in which the Supreme Court refused to adopt the broad interpretation of a statute because it would "criminalize a broad range of day-to-day activity."[118] In *Kozminski*, the Court applied the rule of lenity and cautioned that the broader statutory interpretation would "delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes," subjecting individuals to discriminatory and arbitrary enforcement.[119] The broad interpretation of the CFAA is no different. The government argued in *Nosal* that it would not prosecute minor crimes under the broad interpretation of the CFAA.[120] However, such a concession acknowledges that the law would be so broad as to cover activity which need not be considered criminal. A law, on the books, which is enforced against some, but not others, at the discretion of government actors is arbitrary.

115. See Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562 (2010), stating "[t]he void-for-vagueness doctrine requires courts to adopt narrow and clear interpretations of unauthorized access to save the constitutionality of the statute. The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access will render it unconstitutional."

116. *See* United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc).

117. *See* Cheryl Conner, *Employees Really Do Waste Time at Work*, FORBES.COM (July 17, 2012, 4:24 PM), http://www.forbes.com/sites/cherylsnappconner/2012/07/17/employees-really-do-waste-time-at-work (discussing a recent survey which estimated 64% of employees visited non-work related websites at work).

118. United States v. Kozminski, 487 U.S. 931, 949 (1988).

119. *Id.*

120. *Nosal*, 676 F.3d at 862.

D. Practicality, Common Sense, and Court Resources

There are real world implications where employees could potentially be held criminally liable for seemingly minor transgressions that occur at work within the confines of one's cubicle. It is only natural for an employee in a nine-to-five career to take a break from his work. Prior to the computer take-over of the office environment, employees may have wasted time in extended meetings, making small talk with coworkers, getting coffee, or talking on the phone. Now, with a computer at every desk, while an employee may be using the Internet to check his bank account or personal email, or pay his bills, or e-mail a friend, it is more likely that he will be checking Facebook, Reddit, Tumblr, Twitter, Pinterest, LinkedIn, Amazon, or any other number of social media sites.[121] Many employees are not transfixed solely on work for eight straight hours, interrupted by a lunch at noon, when the wealth of content on the internet is available by a click of the mouse. The Internet may be the greatest source of distraction and it is ever so close. Some studies show that breaks from work might even be productive, and criminalization of productive activity should be discouraged.[122]

The Ninth Circuit addressed this argument in *Nosal*. Minds wonder, and people procrastinate.[123] We are not always perfect workers. However, many computer use policies prohibit such temporary excursions to one's favorite website or activity that are unrelated to work. Under the broad interpretation of the CFAA, attaching authorized access only as far as the employer allows in its computer use policies, these miniscule misdeeds would be classified as federal crimes. Also, linking authorized access to employee computer use policies is problematic because it will always be arbitrary. While it is not likely that such a crime would be enforced, it is possible. The CFAA interpretation that casts such a wide net to include common conduct in

121. Conner, *supra* note 117.

122. There are a number of studies on the subject and the conclusions differ, but some suggest that breaks are a good thing. *See Brief Diversions Vastly Improve Focus, Researchers Find*, SCIENCEDAILY (Feb. 8, 2011), http://www.sciencedaily.com/releases/2011/02/110208131529.htm (noting that a new study "overturns a decades-old theory about the nature of attention and demonstrates that even brief diversions from a task can dramatically improve one's ability to focus on that task for prolonged periods"). *But see* Adam Gorlick, *Need a Study Break to Refresh? Maybe Not, Say Stanford Researchers*, STANFORD REPORT (Oct. 14, 2010), http://news.stanford.edu/news/2010/october/willpower-resource-study-101410.html (discussing a paper published in *Psychological Science* by Stanford psychologists that found "a person's mindset and personal beliefs about willpower determine how long and how well they'll be able to work on a tough mental exercise"). *See also* Charlotte Fritz, *Coffee Breaks Don't Boost Productivity After All*, HARVARD BUSINESS REVIEW (May 30, 2012), http://hbr.org/2012/05/coffee-breaks-dont-boost-productivity-after-all/ar/1.

123. *See Nosal*, 676 F.3d at 860.

the workplace is unworkable.[124]

Furthermore, the broad interpretation of the CFAA should also be avoided because there are other causes of action for employer–employee disputes. "The CFAA should not create liability in the employment context that overlaps or preempts traditional causes of action applying to employees. These tools include, among others, noncompete provisions, trade secret protections, conspiracy, contract law, and the duty of loyalty."[125] Employer–employee relationships are traditionally governed by tort and contract law, and the government's broad interpretation of "exceeds authorized access" would allow employers to manipulate their acceptable-use policies to turn the relationship into ones policed by the criminal law.[126] Moreover, the Supreme Court has held that federal laws should only be read to interfere with the balance of power between state and federal government only when the congressional intent is unmistakably clear.[127] The narrow interpretation of the CFAA avoids unnecessary federal usurpation of causes of action available to employers under state law.

A broad interpretation of the CFAA also has the potential to create absurd results. Imposing criminal liability on computer use policy means that "innocuous behavior" can be turned into a federal crime "simply because a computer is involved."[128] For example, an employee who brings a Sudoku book into work and solves puzzles during downtime would be safe, but another employee who access www.websudoku.com, in violation of an employer computer use policy, is breaking federal criminal law.[129] Likewise, reading a hard copy of ESPN: The Magazine or The New York Times is safe, but visiting www.espn.com or www.nyt.com is criminal.

Finally, the broad interpretation of the CFAA could waste scarce

---

124. *Id.* at 862 (discussing *Kozminski*, 487 U.S. at 949, in which the Supreme Court refused to adopt the broad interpretation of a statute because it would "criminalize a broad range of day-to-day activity," and warned that the broader statutory interpretation would "delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes" and "subject individuals to the risk of arbitrary or discriminatory prosecution and conviction").

125. Garret D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1390 (2011).

126. *See Nosal*, 676 F.3d at 860.

127. Urban, *supra* note 125, at 1390–91 (citing Gregory v. Ashcroft, 501 U.S. 452, 460–61 (1991)).

128. *See Nosal*, 676 F.3d at 860.

129. *Id.* stating, "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 [S]udoku 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 [S]udoku skills behind bars."

federal judicial resources. The broad interpretation relies on computer use policies, and any violation could be a potential federal crime. If all of these crimes were pursued, the federal court system would be inundated with causes of action under the CFAA.

V. CONCLUSION

The current circuit split concerning the CFAA's "exceeds authorized access" leads to confusion for lower courts. Furthermore, the differing circuit court interpretations of the CFAA's authorized access language inhibit multistate employers' ability to create and implement company-wide comprehensive CFAA policies.[130] The Seventh, Fifth, First, and Eleventh Circuits have held that the plain language of the CFAA supports a broad interpretation of the statute covering the "misuse or misappropriation" of protected information.[131] The Ninth and Fourth Circuits have recently held that the CFAA is ambiguous as to what employee conduct "exceeds authorized access" and that the rule of lenity should be applied to limit the definition to conduct on par with hacking, which coincides with the legislative intent.[132] The narrow interpretation of the CFAA's statute is the correct one for employer–employee disputes because the CFAA is a criminal statute and other areas of law already cover the activity to which it ascribes criminal liability. The broad interpretation of the statute casts the net much wider than it need or should be.

In *United States v. Nosal*, the Ninth Circuit noted that "[t]he government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations."[133] However, leaving an unduly broad statute on the books is not the correct approach. The solution to the ambiguity should come from either a legislative fix or for the Supreme Court of the United States to grant certiorari on a relevant case to resolve the dispute. A statutory fix, however, would be the superior option because Congress is capable of amending and clarifying an ambiguous statute. Senate Judiciary Committee Chairman Patrick Leahy had filed amendments to The Cybersecurity Act of 2012.[134]

130. Obie Okuh, Comment, *When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access*, 21 ALB. L.J. SCI. & TECH. 637, 641 (2011).

131. *See* Int'l Airport Ctrs, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

132. *See Nosal*, 676 F.3d at 862; WEC Carolina Energy Solutions L.L.C. v. Miller, 687 F.3d 199, 200 (4th Cir. 2012).

133. *Nosal*, 676 F.3d at 862.

134. Josh Smith, *Cybersecurity Bill Hinges on Amendments*, NATIONAL JOURNAL (July 30, 2012), http://www.nationaljournal.com/tech/cybersecurity-bill-hinges-on-amendments-20120730.

These amendment would have satisfied the Department of Justice by "enhancing the CFAA's penalties, adding an asset forfeiture provision, and creating a new extra-punitive 18 U.S.C. 1030A."[135] In exchange, "Leahy's Amendment would [have applied a] statutory fix to the definition of 'exceeds authorized access' that essentially adopts the narrow view of the circuit split on the scope of the CFAA."[136] However, the Cybersecurity Act of 2012 was defeated in the Senate.[137] If Congress is not able to amend the statute, the Supreme Court should grant certiorari in order to provide clarity and guidance to the lower courts.

135. Orin Kerr, *Recent Developments–Both in the Court and in Congress–on the Scope of the Computer Fraud and Abuse Act*, THE 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/#.ULw_fg1MgPw.email.

136. *Id.*

137. Tony Romm, *Senate Cybersecurity Bid Sputters*, POLITICO (Aug. 2, 2012, 12:54 PM), http://www.politico.com/news/stories/0812/79322.html.