View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Georgia State University College of Law: Reading Room

Georgia State University Law Review

Volume 27
Issue 2 *Winter 2011*

Article 14

1-1-2011

Lenity on Me: LVRC Holdings LLC v. Brekka Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act

Warren Thomas

Follow this and additional works at: https://readingroom.law.gsu.edu/gsulr

Part of the Law Commons

Recommended Citation

Warren Thomas, *Lenity on Me: LVRC Holdings LLC v. Brekka Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act*, 27 Ga. St. U. L. Rev. (2011).
Available at: https://readingroom.law.gsu.edu/gsulr/vol27/iss2/14

This Article is brought to you for free and open access by the Publications at Reading Room. It has been accepted for inclusion in Georgia State University Law Review by an authorized editor of Reading Room. For more information, please contact mbutler@gsu.edu.

LENITY ON ME: *LVRC HOLDINGS LLC V. BREKKA* POINTS THE WAY TOWARD DEFINING AUTHORIZATION AND SOLVING THE SPLIT OVER THE COMPUTER FRAUD AND ABUSE ACT

Warren Thomas*

INTRODUCTION

According to one recent survey, almost 60% of employees who leave their jobs take company data with them.[1] Indeed, technological advances have made it easier than ever for employees to walk out the door with confidential information:[2] "The digital world is no friend to trade secrets."[3] Companies' data loss prevention programs have struggled to keep up with such advances during the current economic downturn.[4] In recent years, employers have increasingly filed lawsuits using the Computer Fraud and Abuse Act (CFAA)[5] to

---

* J.D. Candidate, 2011, Georgia State University College of Law. Thanks to Professor Mark Budnitz and Aaron Danzig for their time and input, and thanks to my wife Lindsay for her love and encouragement.

1. PONEMON INSTITUTE LLC, DATA LOSS RISKS DURING DOWNSIZING 3 (2009), http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Data%20Loss%20Risks%20During%20Downsizing%20FINAL%201.pdf; Brian Krebs, *Data Theft Common by Departing Employees*, WASH. POST, Feb. 26, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html (summarizing the report's findings).

2. Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359, 361 (2009) (comparing the traditional thief who might steal company information by "back[ing] up a tractor-trailer truck to the office in the dead of night and load[ing] up several boxes" and the "new ways . . . to perform the same task . . . [because] [t]oday's thief could simply walk out with the information on his digital music player [or] . . . e-mail the information to its intended destination").

3. *Id.*

4. *See* PRICEWATERHOUSECOOPERS, TRIAL BY FIRE: WHAT GLOBAL EXECUTIVES EXPECT OF INFORMATION SECURITY—IN THE MIDDLE OF THE WORLD'S WORST ECONOMIC DOWNTURN IN THIRTY YEARS 14–15 (2009), http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf (finding over forty percent of survey respondents believe security incidents are more likely "due to employee layoffs and risks associated with business partners and suppliers weakened by the downturn"); *accord* PONEMON INSTITUTE, *supra* note 1, at 2 (discussing increased data loss risks during the recession).

5. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (2006)). "Technically speaking, . . . [the] acronym CFAA refer[s] only to the 1986 amendments. In practice, however, courts and commentators use both labels to refer to the entire federal unauthorized access statute . . . ." Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1598 n.11 (2003)

punish employees who absconded with company data and to deter further abuses.[6]

The CFAA defines several violations that include access "without authorization" as a necessary element for the plaintiff to allege and prove. For example, the statute creates liability for "[w]hoever . . . intentionally accesses a protected computer without authorization, and as a result of such conduct causes damage and loss."[7] Many cases ultimately turn on whether the former employees accessed their computers *without authorization* or *in excess of authorization*.[8] However, the statute does not define *authorization*[9] and "[c]ourts have struggled over how to interpret the provisions of the CFAA" in the context of employer litigation over employees' misappropriation of data.[10] The landscape of conflicting opinions is so treacherous that one court recently suggested it was relieved that it "need not parse through the complex issues" to interpret the statute.[11]

A widening split among circuit and district courts over the meanings of *without authorization* and *exceeds authorized access* in the CFAA continues to cause confusion among litigants and threatens to improperly expose defendants to greater criminal liability if expansive interpretations remain unchecked.[12] In 2003, Professor

---

[hereinafter Kerr, *Cybercrime's Scope*]. 18 U.S.C. § 1030(g) (2006) provides the basis for a civil action in the otherwise criminal statute.

6. *See generally*, *e.g.*, Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL'Y J. 11 (2008); Graham M. Liccardi, Note, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155 (2008); Nick Akerman, *When Workers Steal Data to Use at New Jobs: Despite Some Negative Case Law, The Computer Fraud and Abuse Act is an Effective Tool for Employers*, NAT'L L. J., July 6, 2009, at 18.

7. 18 U.S.C.A. § 1030(a)(5)(C) (West Supp. 2010).

8. *See* discussion *infra* Parts II–III.

9. *See generally* § 1030. *Cf.* 18 U.S.C. § 1030(e)(6) (2006) (defining *exceeds authorized access* in terms of the undefined *authorization*).

10. ES & H, Inc. v. Allied Safety Consultants, Inc., No. 3:08-CV-323, 2009 WL 2996340, at *2 (E.D. Tenn. Sept. 16, 2009).

11. *Id.* at *3–4 (finding the plaintiff's inadequate allegation of "loss" dispositive and dismissing the CFAA claims).

12. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1598–99 (discussing the "uncertain scope" of unauthorized access statutes as it applies to contracts between computer owners and users granted authorized access).

Orin Kerr[13] worried about the implications of an increasingly broad scope of conduct found to violate the CFAA: "These precedents have arisen in the civil context, and have not yet been applied to criminal cases. . . . [B]road judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web."[14]

In 2008, federal prosecutors confirmed Kerr's fear when they brought criminal charges against Lori Drew in the wake of the tragic suicide of Megan Meier.[15] The government alleged Ms. Drew accessed MySpace servers "without authorization and in excess of authorized access" when she violated the MySpace terms of the service agreement.[16] Although the court ultimately dismissed the case,[17] some commentators suggested the prosecutor's "novel and extreme" interpretation of the CFAA set an alarming precedent.[18] Indeed, a district court adopted the broad view of authorization—previously only applied in civil cases and the subject of vigorous

13. Kerr is a faculty member of the George Washington University Law School. GW Law Faculty Directory, http://www.law.gwu.edu/Faculty/profile.aspx?id=3568 (last visited Oct. 12, 2010).

14. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1599.

15. For a detailed profile of Megan Meier and the story of her death, see Lauren Collins, *Friend Game: Behind the Online Hoax That Led to a Teen's Suicide*, THE NEW YORKER, Jan. 21, 2008, at 34, *available at* http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_collins. Essentially, Lori Drew and her daughter created a fictitious MySpace profile in violation of the site's terms of service. Posing as "Josh," they befriended and then later harassed Megan. She ultimately hung herself in her bedroom.

16. Indictment at 9, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (CR08-00582), 2008 WL 2078622.

17. *See generally Drew*, 259 F.R.D. 449 (granting defendant's post-verdict motion for judgment of acquittal on the misdemeanor CFAA violation because it contravenes the "void-for-vagueness" doctrine); Kim Zetter, *Cyber Bullying Case Officially Dismissed for Vagueness*, WIRED, Aug. 31, 2009, http://www.wired.com/threatlevel/2009/08/lori-drew-ruling. The U.S. Attorney's Office filed a notice of appeal in September 2009, although it subsequently dropped the appeal. Orin Kerr, *Government Files Notice of Appeal in Lori Drew Case*, THE VOLOKH CONSPIRACY (Sept. 25, 2009, 7:52 PM), http://volokh.com/2009/09/25/government-files-notice-of-appeal-in-lori-drew-case (referencing Professor Kerr's own work on the case: he represents the defendant); Orin Kerr, *Justice Department to Drop Lori Drew Appeal*, THE VOLOKH CONSPIRACY (Nov. 19, 2009, 7:51 PM), http://volokh.com/2009/11/19/justice-department-to-drop-lori-drew-appeal.

18. Kim Zetter, *Experts Say MySpace Suicide Indictment Sets 'Scary' Legal Precedent*, WIRED, May 15, 2008, http://www.wired.com/threatlevel/2008/05/myspace-indictm. Others have praised the prosecution, however. Kim Zetter, *Congresswoman Praises Lori Drew Prosecutors*, WIRED, July 1, 2009, http://www.wired.com/threatlevel/2009/07/congresswoman-praises-lori-drew-prosecutors (quoting Rep. Sanchez's statement that she "applaud[s] the work of the U.S. attorneys who have worked hard to bring Ms. Drew to justice" and highlighting her sponsorship of a "cyberbullying" prevention bill).

debate[19]—and allowed the first criminal prosecution against a former employee charged with unauthorized access of his company's data in the twenty-five year history of the CFAA.[20] These cases illustrate the importance of resolving the question of when access is unauthorized.

This Note examines the debate over the nature of unauthorized access in the context of the maturing circuit split. Part I provides an overview of the CFAA and introduces the cause for disagreement. Part II discusses the development of the split of authority interpreting *without authorization* under the CFAA and focuses on the milestone cases in the debate. Part III analyzes the recent Ninth Circuit case, *LVRC Holdings LLC v. Brekka*,[21] and its disparagement of *International Airport Centers, L.L.C. v. Citrin*,[22] the Seventh Circuit's prior influential interpretation. Part IV evaluates several of the interpretive methods courts have used to reach their conclusions and finds them unsatisfactory to resolve the question. Finally, Part V proposes that courts should interpret the CFAA in light of the rule of lenity to arrive at a narrow construction and definition of *unauthorized access*.

I. BACKGROUND AND OVERVIEW OF THE CFAA

The CFAA is "by far the most important and influential computer misuse statute in the United States"[23] and serves "as the centerpiece of federal enforcement efforts related to computer-based crimes."[24] As computer use increased in the 1970s and 1980s, so did computer *misuse*.[25] Law enforcement agencies needed new criminal laws that

19. *Compare* Kerr, *Cybercrime's Scope*, *supra* note 5 (arguing for a narrow interpretation of authorization), *with* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395 (2006–2007) (arguing for a broader "reasonable person" test of authorization).

20. United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *4–7 (N.D. Cal. Apr. 13, 2009) (denying defendant's motion to dismiss and stating the court was "[un]persuaded by Nosal's arguments or by the narrower view of 'authorization'").

21. LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

22. International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

23. Winn, *supra* note 19, at 1402.

24. A. HUGH SCOTT & KATHLEEN BURDETTE SHIELDS, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 4-3 (Cumulative Supp. 2006).

25. *See* Kerr, *Cybercrime's Scope*, *supra* note 5, at 1602.

were better suited to fight the emerging computer crimes,[26] and Congress responded by passing the initial version of the CFAA in 1984, which applied only to federal government computers.[27]

Congress amended the CFAA several times since its initial passage.[28] Subsection (a) defines seven substantive criminal offenses, and these offenses have been modified over the years.[29] In 1994, Congress added subsection (g)[30] to give a civil cause of action for "victims who suffer specific types of loss or damage as a result of a violation[] of the Act," thus creating compensatory damages and injunctive or other equitable relief.[31] Amendments in 1996 and 2001 broadened the statute to protect essentially all computers used in interstate communication.[32]

Many of the CFAA offenses require a prosecutor or plaintiff to show that a defendant "accesses a protected computer without authorization, or exceeds authorized access" to create liability for such conduct.[33] Congress defined *exceeds authorized access* as

---

26. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 1 (2007), *available at* http://www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf [hereinafter COMPUTER CRIMES].

27. SCOTT & SHIELDS, *supra* note 24, at 4-8 to 4-9. Between 1978 and 1999, every state enacted its own computer crime statute as well. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1615.

28. The most recent update re-designated several subsection identifiers within § 1030. Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, tit. II, § 204, 122 Stat. 3560, 3561–63. The provisions that are the focus of this Note are "substantially similar, albeit now codified [as] different provisions." ES & H, Inc. v. Allied Safety Consultants, Inc., No. 3:08-CV-323, 2009 WL 2996340, at *2 n.2 (E.D. Tenn. Sept. 16, 2009). Thus, to aid future readers, CFAA citations within this Note refer to the current version as codified in U.S.C.A. and its supplement. Further, CFAA references in cases have been altered (as indicated) to refer to the corresponding, current subsection.

29. 18 U.S.C.A. § 1030(a)(1)–(7) (West 2000 & Supp. 2010). These are: "Obtaining National Security Information," "Compromising the Confidentiality of a Computer," "Trespassing in a Government Computer," "Accessing a Computer to Defraud & Obtain Value," "Causing Damage to a Protected Computer," "Trafficking in Passwords," and "Extortion Involving Threats to Damage a Protected Computer." COMPUTER CRIMES, *supra* note 26, at 2; *see also* SCOTT & SHIELDS, *supra* note 24, at 4-4.

30. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX, § 290001, 108 Stat. 2097.

31. COMPUTER CRIMES, *supra* note 26, at 3; SCOTT & SHIELDS, *supra* note 24, at 4-11.

32. SCOTT & SHIELDS, *supra* note 24, at 4-3 (citing the definition of *protected computer* as it existed in 2006). Today the CFAA includes computers "used in or affecting interstate or foreign commerce or communication." 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 2010).

33. COMPUTER CRIMES, *supra* note 26, at 4–5 (illustrating authorization requirements in tabular format). Only the crimes dealing with unauthorized damage, trafficking in passwords, and extortion lack an element of authorized access. *See* 18 U.S.C.A. § 1030(a)(5)(A), (a)(6), (a)(7). Additionally, Professor Kerr notes that "most statutes start with the basic building block of 'unauthorized access' to computers,

follows: "to *access* a computer *with authorization* and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[34] However, definitions of *access* and *authorization* are notably absent.[35] While the meanings of both terms are open for debate,[36] this Note deals only with the interpretation of *authorization*.[37]

II. REVIEW OF PAST CASE LAW INTERPRETING AUTHORIZATION

From the leading case of *United States v. Morris*[38]—"one of the first prosecutions under the CFAA"[39]—to the full-blown circuit split present today,[40] judicial interpretation of *authorization* has changed dramatically. In *Morris*, the Second Circuit held that the defendant gained unauthorized access to computer systems when he used a program for something other than the program's "intended

---

and then add additional elements to the offense to deal with specific types of computer misuse." Kerr, *Cybercrime's Scope*, *supra* note 5, at 1616 (discussing both state and federal statutes).

34. 18 U.S.C.A. § 1030(e)(6) (West 2000) (emphasis added).

35. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1623–24. Professor Kerr calls this a "mystery." *Id.* at 1597. He also points out that only one state, Michigan, attempted to define *without authorization*, and he criticizes its statute as potentially unconstitutional. *Id.* at 1624 n.110.

36. *See generally* Kerr, *Cybercrime's Scope*, *supra* note 5 (discussing the development of unauthorized access statutes and various interpretations of both *access* and *without authorization*).

37. Other authors and courts discuss the meaning and construction of *access* under the CFAA and other unauthorized access statutes. *See, e.g.*, Role Models Am., Inc. v. Jones, 305 F. Supp. 2d 564, 567 (D. Md. 2004) ("'[A]ccess' in this context, is an active verb: it means 'to gain access to,' or 'to exercise the freedom or ability to make use of something.'" (quoting Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1272 (N.D. Iowa 2000))), *quoted in* SCOTT & SHIELDS, *supra* note 24, at 4-16; State v. Allen, 917 P.2d 848, 852–53 (Kan. 1996) (construing Kansas statute's definition of *access* narrowly); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2232–34, 2253–58 (2004) (arguing that "the narrower reading of 'access' is . . . the more natural one," where *access* refers to "conduct by which one is in a position to obtain privileges or information not available to the general public"); Kerr, *Cybercrime's Scope*, *supra* note 5, at 1619–21, 1624–28, 1646–48 (analyzing various interpretations, including those in *Allen* and *America Online*, and proposing a broad construction of *access*); Susan Brenner, *"Access,"* CYB3RCRIM3 (Feb. 12, 2006, 2:28 PM), http://cyb3rcrim3.blogspot.com/2006/02/access.html (noting it is "surprising . . . that there [is] relatively little case law" defining *access* and citing *State v. Allen* as a leading case).

38. United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

39. Winn, *supra* note 19, at 1406.

40. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (declining to adopt the Seventh Circuit's interpretation of *without authorization*).

function."[41] Today, two primary lines of diverging case law compete to either expand or narrow the meaning of authorization.[42]

Despite the criminal background of the CFAA, the amendments adding a civil cause of action and expanding the definition of "protected computer" quickly led to many more civil cases than criminal prosecutions.[43] Perhaps for this reason—"the context of civil disputes rather than criminal prosecutions"[44]—courts expanded the interpretation of *authorization* to cover more conduct than before: "It is one thing to say that a defendant must pay a plaintiff for the harm his action caused; it is quite another to say that a defendant must go to jail for it."[45] Thus, the problem lies in the fact that judicial interpretations that broadened civil liability under the CFAA have also broadened *criminal* liability.

The most common fact pattern deals with employee data theft: an employee decides he will leave his employer to join a competitor and uses the employer's computer systems to take data useful to his new pursuit.[46] The former employer discovers the data leak and files suit under the CFAA, alleging the employee used the company's computers "without authorization."[47] It is within this context that

41. SCOTT & SHIELDS, *supra* note 24, at 4-17 (citing United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991)). Professors Kerr and Winn both theorize that "the intended function test appears to derive largely from a sense of social norms in the community of computer users." Kerr, *Cybercrime's Scope*, *supra* note 5, at 1632; *accord* Winn, *supra* note 19, at 1406 (noting that the "system of unwritten norms . . . established between the users of the network" conscribed Morris's authorization).

42. United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *5 (listing cases and summarizing the positions); Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *4 nn.3–4 (D. Minn. Dec. 15, 2008) (same).

43. Winn, *supra* note 19, at 1408; *see also* Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 n.11 (M.D. Fla. Aug. 1, 2006) ("[T]he CFAA has largely been addressed in the civil context . . . .").

44. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1641.

45. *Id.* at 1641–42 ("Courts are more likely to hold a defendant liable under an ambiguous statute when the stakes involve a business dispute between two competitors than when the government seeks to punish an individual with jail time.").

46. Orin Kerr, *Lori Drew, Take 2?: The Government's Computer Fraud and Abuse Act Prosecution in* United States v. Nosal, THE VOLOKH CONSPIRACY (Feb. 25, 2009, 2:03 AM), http://volokh.com/2009/02/25/lori-drew-take-2-the-governments-computer-fraud-and-abuse-act-prosecution-in-united-states-v-nosal [hereinafter Kerr, *Take 2*].

47. *Id.*

courts took the first step to the "remarkable" expansion of the meaning of access.[48]

A. Expanding the Scope of Without Authorization: Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.[49]

In *Shurgard*, the plaintiff and defendant were direct competitors in the self-storage facilities business.[50] The defendant offered a job to Eric Leland, a manager for Shurgard, and before leaving Shurgard's employment, Mr. Leland "sent e-mails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff."[51] Shurgard sued under various provisions of the CFAA, including §1030(a)(2)(C), which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer."[52] The defendant moved to dismiss the claim because the plaintiff did not allege that Leland accessed the information without authorization.[53]

The district court adopted the plaintiff's theory, holding "the authorization for [Shurgard's] . . . employees ended when the employees began acting as agents for the defendant."[54] This is the so-

---

48. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1632.

49. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000). We begin with *Shurgard* because, according to Professor Winn, "[a]lthough a district court opinion, the analysis in [the case] has been very influential. Its broad reading of the CFAA has been followed by the majority of other courts in the United States." Winn, *supra* note 19, at 1409. However, Kerr, in early 2009, wrote the following:

> [T]here have been about 20 district court decisions on this, about 10 of which were handed down in the last year alone, and the cases are divided almost 50/50 . . . between decisions accepting the [*Shurgard*] theory and decisions rejecting it. Also, there is a clear trend in the caselaw: The earlier decisions generally accepted this theory, and the more recent cases tend to reject it.

Kerr, *Take 2*, *supra* note 46; *see also infra* notes 70–107 and accompanying text.

50. *Shurgard*, 119 F. Supp. 2d at 1123.

51. *Id.*

52. 18 U.S.C.A. § 1030 (a)(2)(C) (West Supp. 2010).

53. *Shurgard*, 119 F. Supp. 2d at 1124. The defendant's contention was based on the fact that Shurgard alleged "Mr. Leland had full access" to the information and thus could not have been "without authorization." *Id.* at 1123–24.

54. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1633 (omission in original) (quoting *Shurgard*, 119 F. Supp. 2d at 1124).

called "agency theory of authorization."[55] The court applied the rule from the Restatement (Second) of Agency section 112 stating, "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or he is otherwise guilty of a serious breach of loyalty to the principal."[56] Therefore, according to the plaintiff, Mr. Leland "lost" his authorization and was thus without authorization (according to the CFAA) when he accepted the defendant's job offer and chose to email the proprietary information to Safeguard.[57]

B. Cementing Shurgard*:* International Airport Centers, L.L.C. v. Citrin[58]

In the ensuing years, several district courts in various jurisdictions adopted the agency theory in *Shurgard*.[59] When Judge Posner adopted the argument for the Seventh Circuit in *Citrin* and reversed the district court's grant of summary judgment for the defendant, its weight increased significantly.

In *Citrin*, the defendant was an employee of International Airport Centers (IAC) and used a company-provided laptop to perform the duties assigned him.[60] According to IAC's complaint, Citrin had engaged in "improper conduct" before deciding to quit and form his own, competing business.[61] He installed a "secure-erasure" program on the laptop and deleted all the files—data belonging to IAC—in such a manner as to make them unrecoverable.[62] The Seventh Circuit held that the IAC could state a claim under the "intentionally causes

55. *Id.*; *accord* Warner, *supra* note 6, at 18; Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employers' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 823 (2009).

56. RESTATEMENT (SECOND) OF AGENCY § 112 (1958), *quoted in Shurgard*, 119 F. Supp. 2d at 1125.

57. *Shurgard*, 119 F. Supp. 2d at 1125.

58. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

59. *See, e.g.*, Warner, *supra* note 6, at 19 n.36 (noting the "widespread endorsement" of *Shurgard* and citing cases).

60. *Citrin*, 440 F.3d at 419.

61. *Id.*

62. *Id.*

damage without authorization" provision.[63] The court went on to say that Citrin violated the CFAA provision barring access without authorization[64] as well: "[H]is authorization to access the laptop terminated" when he engaged in the improper conduct, decided to quit, and chose to delete the files, thus violating his "duty of loyalty that agency law imposes" on employees.[65] As in *Shurgard*, the "breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop."[66]

Arguably, this part of Judge Posner's conclusion—that Citrin's *access* was unauthorized—is mere dicta. The plaintiff alleged a violation of the CFAA provision that prohibits *causing damage* without authorization.[67] Because the court only needed to reach a holding on the elements that comprise subsection (a)(5)(A), it was unnecessary to conclude Citrin terminated his agency relationship and authorized access by acquiring an adverse interest.[68] Nonetheless, many courts have approvingly adopted the reasoning and authority of the Seventh Circuit opinion.[69]

---

63. *See* 18 U.S.C.A. § 1030(a)(5)(A) (West Supp. 2010) (creating liability for whoever "knowingly causes the transmission of a program . . . or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" without requiring a showing of *access* without authorization).

64. *See id.* § 1030(a)(5)(B).

65. *Citrin*, 440 F.3d at 420.

66. *Id.* at 420–21.

67. 18 U.S.C.A. § 1030(a)(5)(A); Third Amended Complaint at 12–13, *Citrin*, 440 F.3d 418 (No. 03 C 8104), 2006 WL 3038522.

68. US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 n.3 (D. Kan. 2009) ("[T]he *Citrin* court's reasoning might even be considered dicta, as it reached the issue in concluding that, although the plaintiff asserted a violation of paragraph (a)(5)(A)[] of the CFAA (which contains no authorization language), the alleged conduct would also violate paragraph (a)(5)[(B)]; thus, it is not clear that the authorization issue was fully presented to that court.").

69. *See, e.g.*, Motorola, Inc. v. Lemko Corp., 609 F. Supp. 2d 760, 767 n.2 (N.D. Ill. 2009) (finding the defendant's use of contrary authority "misplaced. Those courts expressly disagreed with the Seventh Circuit's holding in *Citrin* and adopted narrower definitions with respect to the authorization element . . . . This Court is bound by the Seventh Circuit's decision in *Citrin*.").

C. Stemming the Tide, Narrowing the Scope: Lockheed Martin Corp. v. Speed[70]

However, not all courts followed *Citrin*. In a case in the Middle District of Florida with facts very similar to *Shurgard*, plaintiff Lockheed Martin Corporation alleged that a rival defense contractor conspired to gain an unfair advantage on bids for an Air Force contract.[71] Lockheed alleged that three employees abused their "complete access" to proprietary information[72] and copied data to compact discs and personal digital assistants before departing for their new employer.[73] Lockheed argued that, as in *Citrin* and *Shurgard*, the employees terminated their agency authority and accessed the data without authorization when they formed the intent to steal the information and give it to Lockheed's competitor.[74]

However, the court was "not persuaded by the analysis in either *Citrin* or *Shurgard*."[75] Rather, it relied on the "plain language" of the CFAA to resolve the issue without resorting to "extrinsic materials."[76] Applying a dictionary definition of *authorization*, the court held the employees were authorized to access their computers and did not exceed authorization because Lockheed permitted their access to the "precise information at issue."[77] Thus, the court drew a distinction between the employees' improper *access*—which would be actionable under the CFAA—and the employees' improper *actions*.[78]

The court provided four reasons it disagreed with the Seventh Circuit: (1) the agency approach improperly expanded the meaning of

---

70. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006).

71. *Id.* at *1.

72. Specifically, defendant Speed had "complete access," defendant Fleming had "unrestricted access," and defendant St. Romain had "access" to the files. *Id.*

73. *Id.*

74. *Id.* at *4.

75. *Id.*

76. *Speed*, 2006 WL 2683058, at *4 (slyly noting that "[i]n the Eleventh Circuit, there is a presumption that, in drafting a statute, 'Congress said what it meant and meant what it said.'").

77. *Id.* at *5.

78. *Id.* ("As much as Lockheed might wish it to be so, § 1030(a)(4) does not reach the actions alleged in the Complaint.").

without authorization by encroaching on the distinct meaning of *exceeds authorized access*;[79] (2) the interpretation encompassed a larger "spectrum of wrongful access" than Congress intended;[80] (3) the agency approach "broaden[ed] the doorway to federal court" for employers when such intent is unclear in the statute;[81] (4) the statutory construction did not comport with the rule of lenity, which would be appropriate because of the criminal nature of the CFAA.[82]

The reasoning in *Speed* has significantly influenced subsequent courts. Although *Shurgard* and *Citrin* were the prevailing authority for a time, "more recent decisions of district courts in the federal system reflect an evolving analysis favoring the narrow view of the CFAA."[83] Many of the decisions in this trend cite *Speed* as persuasive.[84] However, other persuasive authority might soon threaten to eclipse it.

---

79. *Id.* at *6 ("[T]he term becomes equipped with a breadth that effectively shaves 'exceeds authorized access' down to a mere sliver of what its plain meaning suggests. . . . [I]t appears that *Citrin* relegates the work performed by 'exceeds authorized access' . . . .").

80. *Id.* ("*Citrin* slays all three heads of wrongful access when Congress only aimed at two heads. . . . Congress singled out those accessing 'without authorization' . . . and those 'exceeding authorization' . . . while purposefully leaving those in the middle untouched (those accessing *with* authorization), regardless of their subjective intent.").

81. *Id.* at *7 ("[T]he 'adverse interest' inquiry affixes remarkable reach to the statute—a reach that is not apparent by the statute's plain language.").

82. *Speed*, 2006 WL 2683058, at *7 ("[T]he CFAA is a *criminal* statute with a civil cause of action. To the extent . . . [there are] ambiguous terms, the rule of lenity, a rule of statutory construction for criminal statutes, requires a restrained, narrow interpretation." (citing Pasquantino v. United States, 544 U.S. 349, 383 (2005))). The court also acknowledged Professor Kerr's comment, see *supra* note 45 and accompanying text, regarding the expansive interpretations made easier in civil litigation. *Id.* at *7 n.11.

83. NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 n.7 (S.D. Iowa 2009) (declining, however, to adopt this evolving analysis); *accord* Kerr, *Take 2*, *supra* note 46 ("[T]here is a clear trend in the caselaw [sic]: The earlier decisions generally accepted [the *Citrin*] theory, and the more recent cases tend to reject it."); Amy E. Bivins, *Employers Should Revisit Data Misuse Policy In Light of Ninth Circuit* Brekka *CFAA Ruling*, 8 Privacy & Sec. L. Rep. (BNA) 1441, 1441 (Oct. 5, 2009) ("[The] trend of courts almost uniformly becoming less receptive to the CFAA as a cause of action in trade secret cases.").

84. *See, e.g.*, Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *4 (D. Minn. Dec. 15, 2008) ("[T]he *Lockheed* line of cases reflects a more correct interpretation."); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (concluding that *Speed* supports "the more reasoned view"). *But see NCMIC Fin. Corp.*, 638 F. Supp. 2d at 1058 (noting two circuit courts adopted the broad view, but no circuit court had yet adopted the narrow view).

III. THE CIRCUIT SPLIT RIPENS: THE NINTH CIRCUIT REJECTS *CITRIN* IN *LVRC HOLDINGS LLC V. BREKKA*

In September of 2009, the Ninth Circuit explicitly rejected the Seventh Circuit's holding in *Citrin* and opened wide the split in authority. As discussed above, most of the decisions interpreting the CFAA occurred in the district courts.[85] However, until 2009, *Citrin* remained the only court of appeals holding on the matter. At least twenty-six district courts handed down decisions between the beginning of 2008 and the middle of 2009; these decisions split approximately even over the proper interpretation of *without authorization*.[86] Moreover, district courts within the same circuit occasionally reached different conclusions.[87]

The Ninth Circuit experienced such an intra-circuit split. Before 2008, the Ninth Circuit was a leader in district courts broadly construing the CFAA: *Shurgard* birthed the agency theory of authorization,[88] and several other decisions within the circuit followed *Shurgard*, *Citrin*, or both.[89] In 2008, one court within the Ninth Circuit broke ranks and strongly argued for the narrow interpretation—relying heavily on *Speed*—in its "widely cited"

85. *See supra* Part II.

86. Robert D. Brownstone, *Privacy Litigation*, *in* DATA SECURITY AND PRIVACY LAW: COMBATING CYBERTHREATS § 9:13.50 (West Supp. 2010) (noting, however, that six of the thirteen district court opinions favoring the broad interpretation originated in the Seventh Circuit, where *Citrin* is mandatory authority).

87. In one suit, a Tennessee district court narrowly interpreted the CFAA but then certified an interlocutory appeal so that the Sixth Circuit could resolve the intra-circuit division. Black & Decker, Inc. v. Smith, No. 07-1201, 2008 WL 3850825, at *3–4 (W.D. Tenn. Aug. 13, 2008) (finding no Sixth Circuit opinion interpreting the CFAA, a difference of opinion among the district courts within the circuit, and a split of authority outside the circuit and holding "this difference in opinion that causes the [c]ourt to certify this case for immediate appeal"); *accord* Brownstone, *supra* note 86, at n.5. The Sixth Circuit denied the plaintiff's petition for leave to appeal. *In re* Black & Decker (U.S.), No. 08-0512, 2009 U.S. App. LEXIS 21199 (6th Cir. Jan. 16, 2009).

88. *See supra* Part II.A.

89. *See, e.g.*, United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *7 (N.D. Cal. Apr. 13, 2009); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1194, 1196 (E.D. Wash. 2003) (granting preliminary injunction and supporting the broad interpretation).

opinion.[90] Finally, in September 2009, the Ninth Circuit resolved the difference *within* the circuit in *LVRC Holdings LLC v. Brekka*[91] and provided additional support for future courts that also wish to reject *Citrin*.[92]

A. Brekka*: The Case and Its Reasoning*

The essential facts in *Brekka* resemble the familiar pattern. Mr. Brekka, while an employee of the plaintiff LVRC, sent several company documents to his personal email account.[93] He subsequently ceased working for LVRC, though he owned and operated a consulting business within the same industry.[94] LVRC alleged that Brekka committed two *without authorization* violations under the CFAA[95] when he accessed the confidential information "to further his own personal interests."[96]

Like in *Speed*, the Ninth Circuit began its analysis by examining the "plain language" of the CFAA. The court looked to the dictionary definition of *authorization* and concluded that authorization in the employment context equates with "permission."[97] It found "[n]o language *in the CFAA*" to suggest that an interest contrary to the employer would end an employee's authorization;[98] thus, because

90. *See generally* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008) (citing *Speed* throughout its reasoning); Bivins, *supra* note 83 (stating that *Shamrock* has been "widely cited outside the circuit" for its rejection of the *Citrin* line of reasoning).

91. LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009); *accord* Bivins, *supra* note 83.

92. Jeff Neuburger, *Citing Plain Language of the Computer Fraud and Abuse Act, Ninth Circuit Rules Employee's Disloyal Act Does Not Terminate Authorization to Access Employer's Computer*, NEW MEDIA & TECH. L. BLOG (Sept. 15, 2009, 1:32 PM), http://newmedialaw.proskauer.com/2009/09/articles/computer-fraud-and-abuse-act/citing-plain-language-of-the-computer-fraud-and-abuse-act-ninth-circuit-rules-employees-disloyal-act-does-not-terminate-authorization-to-access-employers-computer ("The Ninth Circuit has now weighed in on the issue . . . and has taken a position diametrically opposed to that of an influential Seventh Circuit opinion . . . .").

93. *Brekka*, 581 F.3d at 1129–30.

94. *Id.*

95. *Id.* at 1131; *see also* 18 U.S.C.A. § 1030(a)(2), (a)(4) (West 2000 & Supp. 2010).

96. *Brekka*, 581 F.3d at 1132.

97. *Id.* at 1132–33 (relying on the "fundamental canon of statutory construction" that words should be interpreted according to their "ordinary, contemporary, common meaning" (quoting Perrin v. United States, 444 U.S. 37, 42 (1979))).

98. *Id.* at 1133 (emphasis added). *Cf.* Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *4 (M.D. Fla. Aug. 1, 2006) ("Because the plain language of the statute is sufficient to interpret the disputed terms, this Court need not resort to extrinsic materials.").

Brekka had permission to use his computer, his use was authorized.[99] The court further explained that the result was a "sensible interpretation of §§ 1030(a)(2) and (4), which *gives effect to both* the phrase 'without authorization' and the phrase 'exceeds authorized access'"—*without authorization* means without any permission, and *exceeds authorized access* means permission to access the computer but not to the information at issue.[100]

The Ninth Circuit was "unpersuaded" by *Citrin*'s interpretation of the CFAA.[101] However, unlike some of the cases in the *Speed* line,[102] the court said that the criminal nature of the statute was "most important" to justify its reasoning.[103] First, it noted that its interpretation in this civil case would be "equally applicable" to a criminal context.[104] The rule of lenity "requires courts to limit the reach of criminal statutes . . . and construe any ambiguity against the government."[105] The rule ensures that defendants have notice of what conduct may subject them to criminal liability.[106] Thus, because of "the care with which [the court] must interpret criminal statutes," it declined to adopt the interpretation and agency theory of *Citrin*.[107]

---

99. *Brekka*, 581 F.3d at 1133.

100. *Id.* (emphasis added). *Cf. Speed*, 2006 WL 2683058, at *6 ("[T]he plain meaning brings clarity to the picture and illuminates the straightforward intention of Congress, [that is,] 'without authorization' means no access authorization and 'exceeds authorized access' means to go beyond the access permitted.").

101. *Brekka*, 581 F.3d at 1134.

102. *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966–67 (D. Ariz. 2008) (turning "[f]inally" to the rule of lenity for construing statutes with both criminal and noncriminal applications); *Speed*, 2006 WL 2683058, at *6–7 (discussing criminal nature last among four justifications for adopting the narrow interpretation).

103. *Brekka*, 581 F.3d at 1134.

104. *Id.* (citing Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004)); *see also* discussion *infra* Part V.B.

105. *Brekka*, 581 F.3d at 1135 (quoting United States v. Romm, 455 F.3d 990, 1001 (9th Cir. 2006)); *see also* BLACK'S LAW DICTIONARY 1449 (9th ed. 2009) (defining "rule of lenity" as "[t]he judicial doctrine holding that a court, in construing an ambiguous criminal statute that sets out multiple or inconsistent punishments, should resolve the ambiguity in favor of the more lenient punishment"); discussion *infra* Part V.A.

106. *Brekka*, 581 F.3d at 1134–35.

107. *Id.* at 1135. *But cf.* United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *7 (N.D. Cal. Apr. 13, 2009) (finding the argument concerning the rule of lenity "unavailing" because it is only applied when there exists statutory ambiguity and finding no such ambiguity in the CFAA).

B. Brekka*'s Wake*

Following the release of the opinion, some commentators anticipated that the time could be near for the Supreme Court to resolve the questions surrounding the meaning of *without authorization* in the CFAA.[108] However, no petition for writ of certiorari was ever filed. But at a minimum, *Brekka* was new mandatory authority within the Ninth Circuit and therefore had important implications for two recent criminal cases in the circuit. The Department of Justice withdrew its appeal from the dismissal in *United States v. Drew*.[109] Later, on motion for reconsideration of its earlier order in *United States v. Nosal*,[110] the district court dismissed five counts against the defendants in light of *Brekka* because the alleged activity took place while they were still employees who had permission to access their employer's systems.[111]

In the civil context outside the Ninth Circuit, however, it is too early to say whether the decision will accelerate the "clear trend" to reject the agency theory of authorization and to construe the term *without authorization* more narrowly.[112]

---

108. *See, e.g.*, David Kravets, *Court: Disloyal Computing Is Not Illegal*, WIRED, Sept. 18, 2009, http://www.wired.com/threatlevel/2009/09/disloyalcomputing ("The appellate court's decision Wednesday, meanwhile, sets the stage for possible review by the U.S. Supreme Court."); Neuburger, *supra* note 92 ("No doubt more will be heard on this issue in the Ninth Circuit, and other courts as well. And eventually, perhaps, the U.S. Supreme Court."). Despite this anticipation, no petition for certiorari was filed.

109. Orin Kerr, *Justice Department to Drop Lori Drew Appeal*, THE VOLOKH CONSPIRACY (Nov. 19, 2009, 7:51 PM) http://volokh.com/2009/11/19/justice-department-to-drop-lori-drew-appeal. A copy of the motion is posted at http://www.steptoe.com/assets/attachments/3943.pdf.

110. *Nosal*, 2009 WL 981336, at *4, 7 (noting that, at the time, the Ninth Circuit had not yet ruled whether an employee who was permitted to access computer information could be liable if the employee subsequently acquired an improper purpose, and then holding that one could).

111. United States v. Nosal, No. CR 08-0237 MHP, 2010 WL 934257, at *6–8 (N.D. Cal. Jan. 6, 2010) ("Quite clearly, *Brekka* implicates the reasoning employed by this court in initially denying Nosal's motion to dismiss the CFAA charges levied against him.").

112. *See supra* note 83 and accompanying text. *But see* Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., & Consulting, LLC, No. 4:08CV01683 JCH, 2009 WL 3523986, at *4 (E.D. Mo. Oct. 26, 2009) (holding that "[u]nder the statute, the Restatement, and the reasoning of *Citron* [sic] and other courts"—but without any reference to *Brekka*—defendants acted without authorization when they breached their fiduciary duty to their employer); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 46 (D. Mass. 2009) (citing *Brekka* as an example of the narrow interpretation of "authorization" but viewing mandatory First Circuit authority as favoring the broad interpretation).

IV. THE VARIOUS APPROACHES AND THEIR EFFECTIVENESS

Courts have used several different techniques of statutory construction to interpret the CFAA. However, almost every interpretive method used to reach one result has also been used to reach the opposite. This section examines several of the common approaches and evaluates how well they resolve the ultimate question of when access is *without authorization*.

A. Plain Meaning or "Strained" Meaning?

Several cases begin their analyses by looking to the "plain meaning" of *unauthorized access* in the CFAA but come to different conclusions as to what, if any, meaning they can ascertain. For example, in *Shurgard*, the court said, "[T]he *unambiguous meaning* of a statute should be the *first and final* inquiry unless it would lead to an absurd result."[113] It then proceeded to hold that the former employees accessed the computers *without authorization* because their authority ended when they became agents of the defendant,[114] apparently believing this construction was such an "unambiguous meaning." In contrast, the *Brekka* court found that an interpretation of "authorization" based on *Citrin* "does not comport with the plain language of the CFAA."[115] These diametrically opposed viewpoints provide little help to decide the proper meaning of *without authorization*.

---

113. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000) (emphasis added); *see also Nosal*, 2009 WL 981336, at *6 ("The court finds no ambiguity in the statute here.").

114. *Shurgard*, 119 F. Supp. 2d at 1124–25 (agreeing with plaintiff's reliance on *United States v. Galindo*, 871 F.2d 99 (9th Cir. 1989), for the rule that acquisition of an adverse interest terminates the agency relationship and authority, notwithstanding that the case post-dated Congress's initial passage of the CFAA).

115. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009); *see also* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) ("[T]he plain language supports a narrow reading of the CFAA. . . . The definition of [*exceeds authorized access*] obviates any need to revert to outside sources . . . ."); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *4 (M.D. Fla. Aug. 1, 2006) ("[T]he plain language of the statute is sufficient to interpret the disputed terms," and the court "need not resort to extrinsic materials.").

B. What Did Congress Intend?

Many cases interpreting the CFAA look to legislative history for clues as to Congress's intended meaning of "unauthorized access." *Shurgard* examined the history of the CFAA en route to rejecting the notion that the statute applied to only "outsiders" and not at all to "insider" employees.[116] The court also found "dispositive" language in the Senate Report accompanying the 1996 amendment:

> The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain information.
> . . . .
> . . . [I]ndividuals who intentionally break into, or abuse their authority to use, a computer . . . would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for purposes of commercial advantage or . . . any criminal or tortious act . . . .[117]

Therefore, the *Shurgard* court found, the Senate Report's emphasis on the purpose of the CFAA to prevent individuals from abusing their right to use a computer "demonstrates the broad meaning and intended scope" of *without authorization*.[118]

Predictably, courts adopting the narrow interpretation marshal legislative history to support their conclusion as well. In 1986, Congress replaced the phrase "or having accessed a computer with authorization, uses the opportunity . . . for purposes to which such authorization does not extend" with the phrase "exceeds authorized access."[119] By doing so, its intent was to "remov[e] from the sweep of the statute one of the murkier grounds of liability, under which a

---

116. *Shurgard*, 119 F. Supp. 2d at 1127–29.

117. *Id.* at 1128–29 (quoting S. REP. NO. 104-357, at 7–8 (1996)) (emphasis omitted).

118. *Id.* at 1129; *see also* NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) ("The legislative history of § 1030(e)(6) supports the broad view."); Field, *supra* note 55, at 830 n.71 (noting that courts adopting the broad interpretation "use legislative history to find that the CFAA's scope has been broadened over time such that it reaches and can be invoked by employers").

119. Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (quoting S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486).

[person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization."[120] One court interpreted this history to find that "a violation does not depend upon the defendant's unauthorized use of *information*, but rather upon the defendant's unauthorized use of *access*."[121]

The conflicting statements in the legislative history provide little help to interpret the proper meaning of *without authorization*. One author, after thoroughly examining much of the legislative history, determined that it "does not support a legislative preference" for any approach and thus "provides little authority value to the current debate."[122]

C. Providing Access to Federal Courts Versus Shutting the Door

Courts illustrate another inherent tension that results from the different interpretations of *without authorization*. The choice either provides a forum to resolve these employer-former employee disputes in federal court or potentially relegates them to state court. At one point, there was a clear trend to increase access to the federal courts for injured employers. First, the broad, agency-based approach of *Shurgard* and *Citrin* necessarily increased the opportunities for aggrieved plaintiffs to sue under the CFAA.[123] Additionally, the Third Circuit in 2005 expanded the scope of violations for which

---

120. *Id.* (quoting S. REP. NO. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494–95) (second alteration in *Werner-Masuda* retained but emphasis omitted).

121. Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); *see also* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008) ("Thus, the legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."); Field, *supra* note 55, at 830 n.71 (noting that courts adopting the narrow interpretation often argue that legislative history supports them).

122. Field, *supra* note 55, at 830–31. *But see* Winn, *supra* note 19, at 1416 ("Based on the language of the CFAA *and its legislative history* . . . the breadth of the holdings in the unauthorized access cases . . . appears to be consistent with Congressional intent." (emphasis added)).

123. *See* Linda K. Stevens & Jesi J. Carlson, *The CFAA: New Remedies for Employee Computer Abuse*, 96 ILL. B.J. 144, 144, 161 (2008) (noting the expanded universe of potential litigants and "powerful federal cause of action" the CFAA offers); Warner, *supra* note 6, at 12–13 (noting the "recent expansion of liability under the CFAA" and that the CFAA "puts another arrow in the employer's quiver, and the new arrow is proving increasingly popular").

plaintiffs could bring a civil action under the CFAA.[124] The court rejected the argument that the reference to the conduct factors in subsection (a)(5)(B)[125] precluded relief for violations of the other sections.[126] By clarifying that plaintiffs could allege other violations and obtain relief, the Third Circuit added to employers' opportunities to allege CFAA violations in federal court.[127]

On the other hand, courts favoring the narrow interpretation of *without authorization* hesitate to expand federal jurisdiction. In *Shamrock*, the court feared that conferring a federal cause of action whenever an employee "accesses the company computer with adverse interests" would "open the doorway to federal court [too] expansively when this reach is not apparent from the plain language of the CFAA."[128] Under this view, it is unlikely Congress intended to criminalize breach of contract claims,[129] and jurisdiction is further limited by requiring "integral" use of a computer in the perpetuation of the wrong.[130]

These common analytical approaches yield conflicting interpretations of the CFAA and prove ineffective to guide future litigants.[131] One court may conclude the plain meaning of *without*

---

124. 18 U.S.C.A. § 1030(g) (West Supp. 2010); P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 512 (3d Cir. 2005).

125. At the time, § 1030(a)(5)(A) encompassed the three violations of what is now subsection (a)(5); the conduct factors in § 1030(a)(5)(B) are now codified in § 1030(c)(4)(A)(i)(I)–(V).

126. *P.C. Yonkers*, 428 F.3d at 512 (concluding that the plaintiffs' claims fit "squarely within the class of claims" eligible for relief).

127. *See also* Liccardi, *supra* note 6, at 182–89 (noting that any of the six causes of action in the CFAA can be used to litigate trade secret disputes in federal courts and arguing that the CFAA is an apt vehicle to provide federal question jurisdiction to employers).

128. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008) (internal quotations omitted).

129. Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007).

130. *Id.* (noting that under the broad interpretation, "turning over information to a competitor would be a violation of the CFAA if obtained from a computer but not, for example, from a wastebasket, even though the defendant was permitted to access the information in the computer").

131. Indeed, the broad interpretations of the CFAA and employers' use of it resemble the "results-oriented" use of traditional trespass and burglary laws to prosecute computer misuse before the passage of the CFAA. Kerr, *Cybercrime's Scope*, *supra* note 5, at 1605. As Kerr points out, this resulted in "little ex ante guidance . . . and liability depended on ex post assessments of whether the computer misuse caused enough of a harm to be considered theft." *Id.* at 1613.

authorization encompasses access after a serious breach of loyalty,[132] while another may conclude the plain meaning only refers to initial permission to access.[133] Courts may find persuasive legislative history to support either the broad interpretation[134] or the narrow.[135] Some courts favor permitting more claimants access to federal courts,[136] while others refuse access without more explicit congressional direction.[137] Given these conflicts, the question remains—Is there a way to interpret the statute to resolve the dispute?

V. PROPOSAL: APPLYING THE RULE OF LENITY TO BREAK THE TIE

With apologies to Chief Justice Marshall, we must never forget that it is a *criminal statute* we are expounding.[138] Because the CFAA creates both civil and criminal liability for violators,[139] courts should apply principles of strict construction of criminal laws to interpret the statute. As this Note has discussed, several courts interpreting the CFAA have already referred to the rule of lenity to justify their conclusions.[140] In the absence of any congressional resolution of the problem,[141] this Note proposes that courts, and potentially the

---

132. *See, e.g.*, Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000).

133. *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132–33 (9th Cir. 2009).

134. *See, e.g.*, *Shurgard*, 119 F. Supp. 2d at 1128–29.

135. *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965–66 (D. Ariz. 2008).

136. *See, e.g.*, P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 512 (3d Cir. 2005); *accord* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006) (reversing district court dismissal and reinstating suit under the broad interpretation).

137. *See, e.g.*, *Shamrock*, 535 F. Supp. 2d at 967.

138. *Cf.* M'Culloch v. Maryland, 17 U.S. (4 Wheat.) 316, 407 (1819) ("[W]e must never forget that it is a *constitution* we are expounding.").

139. In fact, many courts recite that it is "primarily" criminal. *E.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) ("[M]ost important, [the CFAA] is primarily a criminal statute . . . ."); A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 n.8 (1st Cir. 2001); Lewis-Burke Assocs., LLC v. Widder, 2010 WL 2926161, at *5 (D.D.C. July 28, 2010) (noting that a court must interpret both criminal and civil applications consistently); *Shamrock*, 535 F. Supp. 2d at 966 ("[T]he CFAA is a criminal statute focused on criminal conduct. The civil component is an afterthought.").

140. *See supra* notes 102–07 and accompanying text.

141. Congress could add a definition of *without authorization* to clarify its intent. *See* Stacy Nowicki, Ph.D., *No Free Lunch (or Wi-fi): Michigan's Unconstitutional Computer Crime Statute*, 13 UCLA J.L. & TECH. 1, 33–41 (2009) (providing draft definitions of *authorization* and *exceeding authorized access* that would likely make disloyal employee conduct unauthorized), http://www.lawtechjournal.com/

Supreme Court, should apply the rule of lenity to serve as a "tiebreaker"[142] to resolve the circuit split. This section provides a brief overview of the lenity doctrine and explains why and how it applies to interpret the phrase *without authorization* in the CFAA.

A. Strict Construction of Criminal Statutes[143]

"What does a court do . . . if, after careful analysis, the meaning of a statute remains uncertain?"[144] According to the traditional canons of construction of criminal laws, the answer is to narrowly construe them to favor the defendant.[145] The doctrine of strict interpretation of criminal laws, or the rule of lenity, is a court-evolved doctrine[146] that dates at least to eighteenth century England,[147] and it was applied in the United States as far back as 1820.[148]

One author expressed the rule of lenity as follows: "[T]he language you have used in this criminal statute does not convey a clear intention to cover the case before us. Therefore this man, who may well have done something that all of us would like to treat as criminal, must go free."[149] Another author suggested that the rule is "a principle, not for *reading* statutes, but for *limiting or prescribing* the court's *creative functions* in cases where the quest for true

---

articles/2009/01_091026_nowicki.pdf. However, one commentator suggests Congress's inaction may demonstrate its "intent to grant judicial discretion" to courts to interpret *authorization* in the CFAA. Field, *supra* note 55, at 838–41.

142. JOSHUA DRESSLER, UNDERSTANDING CRIMINAL LAW 48 (5th ed. 2009) (noting that the lenity doctrine is merely a "tie breaker").

143. WAYNE R. LAFAVE, CRIMINAL LAW 88 (4th ed. 2003).

144. DRESSLER, *supra* note 142, at 48 (introducing the rule of lenity).

145. WILLIAM D. POPKIN, A DICTIONARY OF STATUTORY INTERPRETATION 191 (2007); *accord* United States v. Santos, 553 U.S. 507, 514 (2008) (Scalia, J., plurality opinion) ("The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them.").

146. HERBERT L. PACKER, THE LIMITS OF THE CRIMINAL SANCTION 95 (1968); *id.* at 93 ("[T]he canon of strict construction has a lengthy common law history.").

147. POPKIN, *supra* note 145, at 191; *accord* LAFAVE, *supra* note 143, at 88 (stating the rule developed at a time when many minor crimes were punishable by death).

148. Note, *The New Rule Of Lenity*, 119 HARV. L. REV. 2420, 2420 (2006) ("Chief Justice Marshall described it as 'perhaps not much less old than construction itself.'" (quoting United States v. Wiltberger, 18 U.S. (5 Wheat.) 76, 95 (1820))).

149. PACKER, *supra* note 146, at 95.

meaning has met an impasse."[150] Similarly, the Supreme Court said that when there are "two rational readings of a criminal statute, one harsher than the other, we are to choose the harsher only when Congress has spoken in *clear and definite* language."[151] Thus, lenity weighs in favor of a narrow interpretation.[152]

One author uses *McBoyle v. United States*[153] to illustrate the principle.[154] In *McBoyle*, the defendant was convicted for transporting a stolen airplane under a statute that barred transport of a stolen "motor vehicle."[155] The defendant surely knew he was committing some sort of "wrong"—the airplane was in fact stolen—but the question was whether this was a wrong proscribed by the statute. In an "affirmation of the values inherent in the principle of legality,"[156] the Court declined to extend the statute to cover aircraft "upon the speculation that if the legislature had thought of it, very likely broader words would have been used."[157] Such construction of statutes may have the added benefit of encouraging the legislature to use "sufficiently precise" language.[158]

However, the rule of lenity is a limited rule.[159] First, it is usually only applied as a last resort to interpret a statute.[160] The Supreme Court also said that "[t]he rule of lenity applies only if, after seizing

150. REED DICKERSON, THE INTERPRETATION AND APPLICATION OF STATUTES 210 (1975) (emphasis added). Compare this "limiting" principle to the *Shurgard* and *Citrin* courts' importation of agency principles into the context of the CFAA. *See supra* Parts II.A–B.

151. Pasquantino v. United States, 544 U.S. 349, 383 (2005) (Ginsburg, J., dissenting) (emphasis added); *see also* DRESSLER, *supra* note 142, at 48.

152. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008).

153. McBoyle v. United States, 283 U.S. 25 (1931).

154. PACKER, *supra* note 146, at 95.

155. *McBoyle*, 283 U.S. at 25–26.

156. PACKER, *supra* note 146, at 95. The doctrine of strict construction of criminal statutes is one of the two "devices . . . [that] keep the principle of legality in good repair." *Id.* at 93.

157. *McBoyle*, 283 U.S. at 27.

158. PACKER, *supra* note 146, at 95; *see also* United States v. Santos, 553 U.S. 507, 514 (2008) (Scalia, J., plurality opinion) ("This venerable rule [of lenity] . . . places the weight of inertia upon the party that can best induce Congress to speak more clearly and keeps courts from making criminal law in Congress's stead.").

159. DRESSLER, *supra* note 142, at 48 (observing that some courts "strictly construe *the lenity doctrine itself*.").

160. *Id.* (qualifying when the rule comes into play as "only" if there "*truly* is a 'tie'"); *see also The Supreme Court, 2007 Term—Leading Cases*, 122 HARV. L. REV. 475, 475 (2008) ("[W]hen a statute is irreconcilably ambiguous, the tie goes to the defendant.").

everything from which aid can be derived, we can make no more than a guess as to what Congress intended. To invoke the rule, we must conclude that there is a grievous ambiguity or uncertainty."[161] Thus, the doctrine does not apply to an unambiguous statute.[162] Further, the rule should not be "carried to extremes" by using it to give a statute the "narrowest meaning" or an "overstrict [sic] construction."[163] Finally, some commentators suggest the rule's influence has waned in recent years.[164]

B. Strict Construction in Civil Contexts?

The rule of lenity is not limited to purely criminal statutes or criminal prosecutions.[165] In *United States v. Thompson/Center Arms Co.*, the Supreme Court applied the rule to interpret civil tax provisions in the National Firearms Act because failure to comply with the act could subject a defendant to criminal liability.[166]

---

161. Muscarello v. United States, 524 U.S. 125, 138–39 (1998) (internal quotations, omissions, and citations omitted); *see also* United States v. Shabani, 513 U.S. 10, 17 (1994) ("The rule of lenity, however, applies only when, after consulting traditional canons of statutory construction, we are left with an ambiguous statute."). Of course, the "traditional canons" that "aid" a court in determining Congress's intent include looking to the plain meaning of the words in the statute, divining the intent of the legislature through legislative histories, and using all "appropriate means and *indicia*, such as the purposes appearing from the statute taken as a whole, the phraseology, the words ordinary or technical, the law as it prevailed before the statute, the mischief to be remedied, . . . statutes *in pari materia*, the preamble, the title, and other like means." DRESSLER, *supra* note 142, at 47–48 (quoting *In re* Banks, 244 S.E.2d 386, 389 (N.C. 1978)) (internal quotations omitted). These are some of the same guideposts courts have used to interpret the CFAA. *See supra* Part IV.

162. For example, in *Nosal* the court refused the defendant's request to apply the rule of lenity when interpreting the CFAA because it found "no ambiguity in the statute here." United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *7 (N.D. Cal. Apr. 13, 2009).

163. LAFAVE, *supra* note 143, at 89 (citations omitted).

164. *E.g.*, JOSHUA DRESSLER, CASES AND MATERIALS ON CRIMINAL LAW 110 (5th ed. 2007) ("Today, the lenity doctrine often is not applied."); POPKIN, *supra* note 145, at 192 (2007) ("As the [twentieth] century wore on . . . the lenity canon lost considerable force . . . . But judicial or statutory rejection of the rule of lenity might only mean rejecting a strong presumption . . ., leaving a somewhat weaker presumption in tact."). *See generally* Note, *The New Rule Of Lenity*, *supra* note 148 (arguing throughout that, while "not defunct," the Supreme Court has adopted a "narrower rule of lenity de facto" requiring strict construction "only when a broad interpretation would penalize 'innocent' conduct"). *But see The Supreme Court, 2007 Term*, *supra* note 160, at 475–76 (suggesting that the Supreme Court "began reversing the contraction of lenity and revitalizing a crucial protection for defendants" in *United States v. Santos*, 553 U.S. 507 (2008)).

165. LINDA D. JELLUM & DAVID CHARLES HRICIK, MODERN STATUTORY INTERPRETATION 386 (1st ed. 2006).

166. United States v. Thompson/Center Arms Co., 504 U.S. 505, 507, 517–18 (1992) (Souter, J., plurality opinion). Although the opinion garnered only three votes, a full majority of five justices

Moreover, in *Leocal v. Ashcroft*, the Supreme Court narrowly interpreted the term *crime of violence* in the Immigration and Nationalization Act.[167] Although the case arose in a civil deportation case, the Court explained that "[b]ecause we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."[168] This is correct because it would be an absurd result for a single statutory provision to have two separate meanings depending on the context of the court proceeding.[169]

C. Strict Construction of Without Authorization in the CFAA

Courts should apply the rule of lenity to narrowly interpret the term *without authorization* in the CFAA. First, the CFAA meets the "threshold requirement"[170]—it is primarily a criminal statute.[171] Next, there exists the requisite amount of ambiguity that cannot be resolved by traditional canons of construction.[172] Despite some courts' statements otherwise, there is no plain meaning of *without authorization*.[173] The legislative history proves inconclusive to aid interpretation because, within it, there are multiple instances supporting either construction.[174] Nothing else in the text of the CFAA or outside of it provides significant help to understand what Congress actually intended by the term.[175] Therefore, the arguments

---

applied the rule of lenity to resolve the ambiguity. *Id.* at 519 (Scalia, J., concurring in the judgment) (agreeing that application of the statute was "sufficiently ambiguous to trigger the rule of lenity" but "disagree[ing] with the plurality, however, over where the ambiguity lies").

167. Leocal v. Ashcroft, 543 U.S. 1, 11–12 (2004).

168. *Id.* at 12 n.8.

169. *See* Clark v. Martinez, 543 U.S. 371, 380 (2005) ("It is not at all unusual to give a statute's ambiguous language a limiting construction called for by one of the statute's applications, even though other of the statute's applications, standing alone, would not support the same limitation. The lowest common denominator, as it were, must govern."); *see also* Kerr, *Cybercrime's Scope*, *supra* note 5, at 1599 (noting the "usual rule that civil precedents apply to criminal cases" (citing United States v. Bigham, 812 F.2d 943, 948 (5th Cir. 1987))).

170. JELLUM & HRICIK, *supra* note 165, at 386.

171. *See supra* note 139.

172. *See* JELLUM & HRICIK, *supra* note 165, at 386.

173. *See supra* Part IV.A.

174. *See supra* Part IV.B.

175. *See supra* note 161.

for either a narrow or a broad interpretation essentially balance each other out—it is a "tie" in need of breaking.[176]

Not all courts agree that this tie exists and the rule of lenity applies to the CFAA. In a criminal case, *United States v. Nosal*, the court refused to apply the rule because it found "no ambiguity in the statute."[177] Thus, the court possessed "ample authority . . . to permit criminal actions to proceed based on violations of [the CFAA] by employees, *as interpreted by civil cases*."[178] Although the court found no ambiguity, this Note has demonstrated that there is in fact sufficient, irreconcilable ambiguity in the text.

The Ninth Circuit provided the better analysis in *Brekka*. In rejecting the broad agency theory and applying the rule of lenity, the court considered the notice afforded the defendant and the criminal nature of the statute:

> If the employer has not rescinded the defendant's right to use the computer, the defendant would have *no reason to know* that . . . breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner. . . .
>
> [G]iven *the care with which we must interpret criminal statutes* to ensure that defendants are on notice as to which acts are criminal, we decline to adopt the interpretation of "without authorization" suggested by *Citrin*.[179]

Like in the example case of *McBoyle*,[180] the "wrong" in *Brekka* was not clearly proscribed by the statute such that the defendant

176. *See* United States v. Santos, 553 U.S. 507, 514 (2008) (reasoning that when there is "no more reason to think" one interpretation is better than another, "the tie must go to the defendant").

177. United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *7 (N.D. Cal. Apr. 13, 2009).

178. *Id.* (emphasis added).

179. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (emphasis added).

180. *See supra* text accompanying notes 153–58.

would know his conduct could be *criminal*.[181] It makes no difference that *Brekka* involved a civil suit; the same allegation brought by the federal government would subject the defendant to criminal liability. Thus, the principles embodied in the rule of lenity give the benefit to the defendant and require a narrow interpretation.

Other courts also point to this same concern and use the rule of lenity as a tool to reach a narrow interpretation. In *Speed*, the court noted that "[t]o the extent 'without authorization' . . . can be considered [an] ambiguous term[], the rule of lenity . . . requires a restrained, narrow interpretation."[182] Similarly, in *Shamrock*, the rule of lenity "guide[d] the Court's interpretation" to weigh in favor of the narrow approach and reject any broad interpretation based on agency principles.[183] Moreover, in the criminal prosecution of Lori Drew, the court favorably noted that the rule of lenity "ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct *clearly* covered" before holding that the government's CFAA charge was unconstitutional under the void-for-vagueness doctrine.[184]

Finally, applying the rule of lenity to interpret the CFAA does not violate any of the other common limits to the doctrine. The rule is hardly "carried to extremes" or "overstrict" by its application here to limit the use of the federal courts as a forum for trade secret

---

181. However, the Fifth Circuit distinguished *Brekka* in a case where the defendant was more clearly engaged in a crime. In *United States v. John*, 597 F.3d 263 (5th Cir. 2010), an account manager at Citigroup used her system access to take customer account data, intending to use the data to incur fraudulent charges on the accounts. *Id.* at 269. The Fifth Circuit thought it neither improper nor unexpected to interpret *exceeds authorized access* to encompass a limit on use:

> An authorized computer user "has reason to know" that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme. Moreover, [*Brekka*'s] reasoning at least implies that when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be "proper" to conclude that such conduct "exceeds authorized access" within the meaning of § 1030(a)(2).

Id. at 273.

182. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. Aug. 1, 2006); *see also* US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1194 nn.3, 5 (D. Kan. 2009).

183. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966–67 (D. Ariz. 2008).

184. United States v. Drew, 259 F.R.D. 449, 463–64 (C.D. Cal. 2009) (quoting United States v. Lanier, 520 U.S. 259, 266 (1997)) (emphasis added).

litigation.[185] While it is fair to say that the defendants in many of these cases have wronged their former employers,[186] this does not automatically grant plaintiffs entry into federal court. Rather, even if denied a CFAA claim, plaintiffs have many legal options in state courts to recover against former employees who misuse information: breaches of contract or non-disclosure agreements, misappropriation of trade secrets, conversion, and violations of intellectual property rights.[187] Indeed, many plaintiffs *prefer* to sue in federal court under the CFAA because they believe it lowers the burdens of pleading and proof compared to state employee non-compete and trade secret laws.[188] Thus, no equitable principles are offended by a narrow construction that bars plaintiffs from taking advantage of an "effective tool"[189] that Congress never explicitly created.

CONCLUSION

Congress initially enacted the CFAA to provide federal prosecutors with a tool to combat the growing threat of computer hackers.[190] Since the addition of a civil cause of action, however, businesses have used the statute as another "arrow in the . . . quiver"[191] of their data loss prevention programs. The increased litigation led some courts to expand the statute's reach by broadly interpreting access

185. *See supra* note 163 and accompanying text.

186. Moreover, courts *assume* the truth of the plaintiffs' claims because most decisions are decided at pleading or summary judgment phase. *E.g.*, *Shamrock*, 535 F. Supp. 2d at 962.

187. Bivins, *supra* note 83; *accord* Warner, *supra* note 6, at 12–13 (stating that employers may sue for trade secret misappropriation or breach of contract).

188. Elizabeth A. Cordello, *Commentary: Split over Unauthorized Use Remains*, DAILY REC. (Rochester, N.Y.), Nov. 16, 2009, *available at* 2009 WLNR 23220555 ("Aside from obtaining federal jurisdiction, the CFAA also is an attractive means to pursue former employees in non-compete or trade secret litigation because employers do not have to show the existence of an employment agreement, or that the disputed information is confidential."). *See generally* Liccardi, *supra* note 6 (discussing barriers plaintiffs face litigating complex trade secret cases in state courts and how a broad interpretation of the CFAA overcomes some of those barriers).

189. *See generally* Akerman, *supra* note 6 (arguing that the CFAA remains an "effective tool" against employees who misuse their employers' data).

190. Bellia, *supra* note 37, at 2256 (citing H.R. REP. NO. 98-894, at 8–12 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694–97) ("Congress clearly sought to target hacking activities. The House Report accompanying the statute stressed both governments' and businesses' growing reliance on computers and the threat that increased networking would make society more vulnerable to hacking incidents.").

191. Warner, *supra* note 6, at 13.

without authorization to include an employee's breach of a duty of loyalty to his employer. A split among the circuits ultimately developed over whether this is a proper interpretation of the statute.

The split of authority over the interpretation of the CFAA presents a close question. Unfortunately, none of the traditional tools of statutory construction resolve the inherent ambiguity. Therefore, this Note proposes that courts should apply the rule of lenity to break the "tie" and narrowly interpret the statute. One court noted that the broad, agency-based interpretation "has its allure—it gets all of the wrongful accessers."[192] However, courts should recognize that "the criminal law's reach is limited to . . . identifiable, discrete events."[193] When a person acquires an "adverse interest"[194] is not discrete enough an event to make a person subject to criminal prosecution.[195] Arguably, each of the defendants in these cases knew they were committing some sort of "wrong," but this should not suffice to subject them to criminal prosecution where Congress has not made its intent sufficiently clear to impose it.[196]

As Justice Scalia recently affirmed, "[T]he tie must go to the defendant. The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them."[197] The term *without authorization* in the CFAA is one such ambiguity subjecting individuals to criminal liability. The agency-based interpretation favors plaintiffs and the government rather than defendants. Therefore, future courts should follow the Ninth Circuit's lead in *Brekka*, reject this agency-based interpretation, and instead apply the rule of lenity. The narrow interpretation of *without authorization* limits the overuse of the CFAA in criminal prosecutions and

---

192. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *6 (M.D. Fla. Aug. 1, 2006).

193. PACKER, *supra* note 146, at 97.

194. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

195. *See* Jennifer Granick, *Ninth Circuit Holds Disloyal Computer Use Is Not A Crime*, DEEPLINKS BLOG (Sept. 17, 2009), http://www.eff.org/deeplinks/2009/09/ninth-circuit-holds-disloyal-computer-use-not-crim (characterizing this as "a 'thought crime' interpretation of the CFAA where the employee's mental state determines whether she was authorized or not").

196. *See supra* note 151 and accompanying text.

197. United States v. Santos, 553 U.S. 507, 514 (2008) (Scalia, J., plurality opinion).

inappropriate use of the federal courts as a preferred forum for trade secret litigation.