Vanderbilt Journal of Entertainment & Technology Law

Volume 13
Issue 3 *Issue 3 - Spring 2011*

Article 3

2011

# Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act

Thomas E. Booms

# Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act


## ABSTRACT

*Few would disagree that computers play an important role in modern United States society. However, many would be surprised to discover the modest amount of legislation governing computer use. Congress began addressing computer crime in 1984 by enacting the Computer Fraud and Abuse Act (CFAA). The CFAA represented the first piece of federal legislation governing computer crimes and has undergone eight amendments to date, making it one of the most expansive criminal laws in the United States. In 1994, Congress added a civil provision opening the door for application of the statute in novel situations. Initially enacted to target crimes committed by "hackers," the most common type of CFAA case in recent years involves claims brought against disloyal employees. The typical fact-pattern involves an employee who uses his work computer to misappropriate confidential or proprietary business information from his current employer to start a new business venture or join a competitor. Applying the CFAA to this common situation has resulted in a split of authority regarding the interpretation of "authorization," an undefined predicate for liability under the statute. Some courts have construed the term narrowly, holding that an employee's misuse or misappropriation of an employer's business information is not "without authorization" so long as the employer has given the employee permission to access such information. Others have construed the term broadly, holding that an employer has a cause of action when an employee obtains business information with disloyal intent for the employee's own benefit or that of a competitor, regardless of whether the employer granted permission to access the information.*

*This Note examines the CFAA's history and analyzes the benefits of seeking relief under the CFAA compared to alternative claims. It also discusses the judicial color given to the term "authorization," looking at the rationales behind each approach and focusing on emerging trends in the employer-employee context.*

*Additionally, it examines past Supreme Court cases in an effort to predict how the Supreme Court will ultimately resolve this issue. The Note concludes by proposing that the Supreme Court adopt a narrow interpretation of "authorization," and hold that an employee does not violate the statute by acquiring interests adverse to those of his employer when the employee accesses information with his employer's permission.*

## TABLE OF CONTENTS



In the 1970s few people appreciated the potential of computers to transform the way we do business, communicate, or even commit crimes.[1] Computer use has increased since the mid-1980s, both in the

1. *See Computer Use and Ownership*, U.S. CENSUS BUREAU, http://www.census.gov/population/www/socdemo/computer.html (last visited Feb. 6, 2010) (only 8.2% of households had personal computers in 1984).

home and in the workplace.[2] For many employees, the use of computers has been one of the most innovative workplace transformations.[3] One can scarcely imagine a world without computers—to contact friends and family, receive news, as well as store and easily access data. Given the importance of these machines and their prominence in the United States, the modest amount of legislation relating to computer use is surprising.[4]

Computers confer substantial benefits to employers by measurably increasing worker efficiency and allowing for greater connectivity between enterprises and individuals.[5] However, these benefits often come at a price and pose new challenges for employers.[6] While companies use passwords, firewalls, and encryption to protect network data, they cannot safeguard confidential and proprietary information in every instance.[7] It is difficult, if not impossible, for employers to prevent those employees with access to confidential business information from disseminating that information to an outside party.[8] Typically, if the employee does not use the information to start his or her own business, the outside party is a competitor.[9] Employers have looked to the Computer Fraud and Abuse Act (CFAA) to prevent insiders from misappropriating confidential information and to recover losses resulting from a disloyal employee's misappropriation.[10]

In response to increasing computer use in the United States, Congress enacted the CFAA in 1984—the first piece of federal legislation addressing computer crime.[11] Initially, the Act was narrow, dealing only with criminal activity; however, Congress has amended the Act eight times to accommodate the evolving role of

---

2. *Id.*

3. Adam M. Zaretsky, *Have Computers Made Us More Productive? A Puzzle*, THE REGIONAL ECONOMIST (Oct. 1998), http://www.stlouisfed.org/publications/re/articles/?id=1769.

4. *See generally Computer Crime Legal Resources*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/cybercrime/cclaws.html (last visited Feb. 6, 2010).

5. Erik Brynjolfsson & Marshall Van Alstyne, *Information Worker Productivity: Evidence from Worker Output, Compensation and Email Traffic Data*, CENTER FOR EBUSINESS (Jan. 2005), *available at* http://ebusiness.mit.edu/research/Briefs/VanAlstyne_Info_Productivity_Final_VI.pdf; *see also* Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 820 (2009).

6. *See infra* Part I.

7. Field, *supra* note 5, at 820.

8. Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J. L. & PUB. POL'Y 661, 661 (2009).

9. Field, *supra* note 5, at 820.

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

11. H.R. REP. NO. 98-894, at 3691 (1984).

computers in U.S. society.[12] Each amendment indicates a clear trend toward expanding the Act's scope.[13] Congress added a civil provision in 1994, allowing parties harmed by statutorily covered criminal activity to recover compensatory damages or obtain injunctive relief.[14] Employers have taken advantage of this provision to recover damages from disloyal employees.[15]

While the CFAA is an expansive statute covering a wide range of activity, this Note addresses CFAA claims against employees or former employees for misusing or stealing proprietary or confidential information accessed using an employer's computer.[16] Whereas employees once had to remove physical materials to smuggle confidential information from an employer, the proliferation of computers and the increased ease of information transfer have facilitated misappropriation.[17] "With increasing numbers of employees using computers at work, employers have turned to the CFAA in situations where disloyal employees have pilfered company information from the employer's computer system."[18]

The most common form of employee misconduct involves the misappropriation of "[c]lient lists, marketing secrets, price indexes, and other company specific information in order to start a new company [or] to compete unfairly with a former employer."[19] A brief hypothetical illustrates this common scenario.

An employer, Spotless House Company ("Spotless"), is in the home-cleaning business. It has invested considerable time, effort, and money to develop its client list and business methods to serve clients efficiently. Employees Andy and Brian are cleaning coordinators, responsible for maintaining client lists, cleaning schedules, and market pricing. Andy and Brian have been with Spotless for several years and have access to Spotless's business records. They have

---

12. Boyer, *supra* note 8, at 665.

13. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010) (discussing five substantial modifications of the statute from its inception in 1984 through the 2008 amendment as part of the Identity Theft Enforcement and Restitution Act of 2008).

14. 18 U.S.C. § 1030(g) (2008).

15. *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008) (addressing the question of whether a claim is properly brought under the CFAA when an employee emailed himself the employer's proprietary business information shortly before leaving to work for a competitor).

16. *See, e.g.*, NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042 (S.D. Iowa 2009) (discussing claims brought by employer against a former employee for accessing the employer's computer in order to obtain business information for his own personal benefit and to the detriment of his employer).

17. Boyer, *supra* note 8, at 661.

18. Field, *supra* note 5, at 819.

19. Boyer, *supra* note 8, at 662.

determined they could make more money by starting a competing cleaning business, rather than working for Spotless. Before resigning, Andy emails Spotless's client list, employee names, price schedules, and market intelligence reports to his personal email account. Andy and Brian then resign and shortly thereafter open Crystal Clear Cleaning ("Crystal"), which will directly compete with Spotless. Spotless experiences many client losses to Crystal, as well as decreased revenues, and decreased growth in client development. Spotless learns that Andy stole its proprietary business information in order to start Crystal. In addition to various state law claims, Spotless brings a CFAA claim against Andy to recover losses incurred as a result of his "unauthorized access" to its computer system.[20]

By examining court decisions interpreting "authorization," an undefined predicate for liability under the CFAA, this Note analyzes whether an employer like Spotless has a CFAA claim against an employee like Andy for accessing its computers "without authorization."[21] Part I examines the Act and its history, including statutory amendments. Additionally, it addresses the benefits of seeking relief under the CFAA rather than other available remedies. Part II presents a detailed discussion of the judicial color given to "authorization." Specifically, it analyzes the rationales behind each approach, focusing on emerging trends in the employer-employee context. It also examines past Supreme Court decisions for clues as to how the Court will ultimately resolve this issue. Part III proposes that the Court adopt a narrow interpretation of "authorization," and exclude from liability an employee who acquires interests adverse to those of his employer when the employee accesses information with his employer's permission.

## I. CFAA AND THE SCOPE OF EMPLOYEE "AUTHORIZATION"

### *A. Importance of the Computer Fraud and Abuse Act*

Recognizing that computer use would become an important part of everyday life,[22] Congress enacted the CFAA at a time when the personal computer was still in its infancy and computer use was

20. See *Gast*, 535 F. Supp. 2d at 962, for another common situation resulting in employer action under the CFAA.

21. 18 U.S.C. § 1030 (2008).

22. *See* H.R. REP. NO. 98-894, at 3694 ("Over the past quarter of a century our society has witnessed an amazing technological transformation. The computer has become an integral part of our everyday lives, critical to our national defense, financial transactions, and information transmissions.").

limited primarily to educational institutions and the government.[23] Personal computers did not become commonplace in the United States until the 1990s.[24] In 1984, the year Congress enacted the CFAA, only 8.2 percent of U.S. households had personal computers.[25] That number continued to grow steadily, and by 2003, 61.8 percent of households had a computer and 54.7 percent had Internet access.[26]

Congress enacted the CFAA to aid the government in prosecuting computer crimes,[27] targeting hackers "who accessed computers to steal information or to disrupt or destroy computer functionality."[28] The Act was the first piece of federal legislation addressing computer crimes.[29] Today, it remains primarily a criminal statute, prohibiting unauthorized access to computers,[30] and is one of the most expansive criminal laws in the United States.[31]

The numerous amendments since 1984 indicate a clear trend toward expanding the Act's scope.[32] First, in 1986, Congress added three new provisions, the most significant of which subjects a person to criminal liability if the individual accesses a computer without authorization and causes $1,000 or more in damage.[33] In 1994, Congress added civil liability to the CFAA, allowing victims to sue for compensatory damages or injunctive relief.[34] Congress added this civil remedy to "[o]ffset the monetary damage caused by criminal violations."[35] A second 1994 amendment expanded the statute to apply to computer damage resulting from negligence.[36]

---

23. *See infra* Part I.

24. *Computer Use and Ownership, supra* note 1.

25. *Id.*

26. *Id.*

27. H.R. REP. NO. 98-894, at 3694 ("[W]hile our society has been readily afforded access to computer technology so as to improve the standard of living of law-abiding citizens, so too have criminal elements gained access to computers in order to perpetuate crimes.").

28. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009).

29. Kerr, *supra* note 13; H.R. REP. NO. 98-894, at 3691.

30. 18 U.S.C. § 1030 (2008).

31. Kerr, *supra* note 13.

32. *See id.* (discussing five substantial modifications of the statute from its inception in 1984 through the 2008 amendment as part of the Identity Theft Enforcement and Restitution Act of 2008).

33. *Id.* at 1565. There were other means to fall within the statute, but for the purpose of this Note, the most significant is accessing a computer without authorization and causing the statutory amount of damages. It is this provision that expanded the CFAA's scope into the employer-employee domain, and led to the ambiguity in interpreting "without authorization" pertaining to an employee's actions. *Id.*

34. *Id.*; 18 U.S.C. § 1030(g).

35. Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155, 160 (2008).

36. Kerr, *supra* note 13, at 1566.

In 1996, Congress further expanded the Act by removing restrictions on the type of information covered by the Act and adding a new category of "protected computers."[37] Any computer used in interstate commerce—for example, any computer connected to the Internet—is considered a "protected computer."[38] Recently, Congress further revised the CFAA in 2008,[39] removing the requirement of an interstate communication from § 1030.[40] Significantly, the statute now extends liability to "[a]ny unauthorized access to any protected computer that retrieves any information of any kind, interstate or intrastate,"[41] protecting "[a]ll networked business computers and the information stored on them."[42]

Section 1030(g) allows for a civil remedy in certain circumstances:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).[43]

The aggravating factors set forth in § 1030(c)(4)(A)(i) include: modification or impairment of medical treatment for an individual; physical injury; a threat to public health or safety; damage to a computer owned by the U.S. government; or causing loss to one or more persons in a one year period aggregating to at least $5,000.[44]

In the employer-employee scenario this Note addresses, a plaintiff bringing a civil claim under the CFAA must show that the defendant's access to a "protected computer" was either "without authorization" or "exceeded authorized access."[45] The CFAA defines both "exceeds authorized access" and "protected computer," but not "authorization."[46] Because "authorization" is undefined, courts have

---

37. *Id.* at 1567.

38. The 1996 amendments replaced the category of "federal interest" computers with "protected computers." *Id.*

39. There was also an amendment in 2001 as part of the Patriot Act; however, those changes are not relevant in the situation posed in this Note. *See* Kerr, *supra* note 13, at 1568.

40. *Id.* at 1569.

41. *Id.*

42. Liccardi, *supra* note 35, at 160.

43. 18 U.S.C. § 1030(g) (2008).

44. 18 U.S.C. § 1030(c)(4)(A)(i) (factors I–V).

45. 18 U.S.C. § 1030(a). Employer claims against employees are typically brought under 18 U.S.C. § 1030(a)(2) or (a)(4). *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009); ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010).

46. *See* 18 U.S.C. § 1030(e) (The term "exceeds authorized access" is defined as "access to 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." The term "protected computer"

inconsistently applied the statute in cases where an employer has sued an employee for improperly using confidential or proprietary business information.[47]

### *B. The Benefits of Asserting a CFAA Claim*

Employers derive significant benefits from the availability of a civil action against disloyal employees under the CFAA.[48] First, the cause of action offers litigants a doorway into federal court that would otherwise be unavailable.[49] Without the CFAA, in the hypothetical situation introduced above, Spotless could sue Andy only in state court for breach of contract,[50] breach of fiduciary duty, or trade secret misappropriation.[51] In contrast, under some courts' interpretation of "authorization," employers are able to pursue claims under the CFAA in federal court and file one or more state claims through federal court supplemental jurisdiction.[52]

Second, plaintiffs face a lower burden of proof when they bring claims under the CFAA rather than a claim for trade secret misappropriation under state law.[53] To make out a state trade secret claim, plaintiffs typically must show that (1) the information qualifies as a trade secret; (2) the plaintiff took reasonable measures to prevent the information's disclosure; and (3) the defendant acquired the trade secret through wrongful means.[54] In contrast, under the CFAA, plaintiffs need not prove that the misappropriated information or computer data was a trade secret under state law.[55] Rather, they need

---

means a computer "(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government, or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States").

47. Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 933 (W.D. Tenn. 2008).

48. 18 U.S.C. § 1030(g).

49. Liccardi, *supra* note 35, at 187.

50. This assumes that the employer has had employees sign documents prohibiting the alleged conduct that gave rise to the case.

51. *See* Boyer, *supra* note 8, at 662.

52. 28 U.S.C. § 1367 (1990).

53. Liccardi, *supra* note 35, at 187.

54. *See id.* at 158–60, for a more thorough discussion on what is required to make out a trade secret misappropriation claim.

55. *Id.* at 157.

only show that the information was accessed from a "protected computer."[56]

## II. ANALYZING THE COURT SPLIT

In recent years, suits against disloyal employees—primarily civil—have become the most common type of action brought under the CFAA and have sharply divided lower courts.[57] While courts should apply the provisions of the CFAA uniformly, they have inconsistently interpreted the terms "without authorization" and "exceeds authorized access."[58] Diverse results from courts facing fact patterns similar to the hypothetical posed above demonstrate the need to adopt a uniform approach in applying CFAA provisions.[59] The various interpretations of "authorization" can generally be characterized as reflecting either a "broad view" or a "narrow view" of the term.[60]

The narrow view of authorization reasons that an employee who is authorized to access an employer's computer retains authorization even if the employee misappropriates or misuses the employer's confidential data thereafter.[61] Proponents of the broad view argue that when an employee misuses or steals company data, he acts contrary to his employer's interests and therefore loses his authorization even though his initial access was authorized.[62] Most circuit courts facing CFAA claims arising out of employee misconduct have broadly construed "authorization."[63] Only the Ninth Circuit has adopted the narrow view, in *LVRC Holdings v. Brekka*.[64]

While this Note focuses primarily on the narrow and broad views, courts interpreting "authorization" have also adopted various other definitions of the term.[65] The "agency-based" interpretation is essentially the same as the "broad view."[66] The "code-based"

---

56. 18 U.S.C. § 1030 (2008). Under the CFAA, it is irrelevant what information was accessed so long as it was accessed from a "protected computer" and "without authorization" or "exceeding authorized access." *Id.*

57. Kerr, *supra* note 13, at 1583.

58. *Compare* LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), *with* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

59. *Compare Brekka*, 581 F.3d at 1127, *with Citrin*, 440 F.3d at 418.

60. Lewis-Burke Assocs. LLC v. Widder, 725 F. Supp. 2d 187, 192–194 (D.D.C. 2010).

61. Guest-Tek Interactive Entm't Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009).

62. *Id.*

63. *Compare Brekka*, 581 F.3d at 1127 (construing "authorization" narrowly), *with* United States. v. John, 597 F.3d 263 (5th Cir. 2010), *and Citrin*, 440 F.3d at 418 *and* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (construing "authorization" broadly).

64. *Brekka*, 581 F.3d at 1127.

65. Field, *supra* note 5, at 819–30.

66. *Id.* at 823–25.

interpretation is grounded in the operation of computers and implies that access becomes unauthorized when a person "bypasses code-based protections designed to limit use of the computer system."[67] It limits liability to scenarios in which users intentionally manipulate a computer to gain greater access.[68] The "contract-based" interpretation requires a breach of contract to find an employee's computer use to be unauthorized.[69] Though not widely recognized, these additional interpretations of "authorization" may influence the Supreme Court if it confronts this issue. This Note will focus primarily on the more widely-used narrow and broad views.

### *A. The "Narrow View"—Authorized Access Cannot Be Terminated*

Courts adopting the narrow interpretation hold that an employee, once granted permission to access an employer's computers, does not run afoul of the CFAA regardless of how he subsequently uses the information.[70] An employee's misuse or misappropriation of an employer's proprietary business information is not "without authorization" if the employee has been given permission to access such information.[71] In the hypothetical posed above, Andy would not be liable for accessing Spotless's computer "without authorization" even though he acquired interests adverse to his employer and used Spotless's proprietary business information for his own benefit. Although numerous district court cases have construed "authorization" narrowly, every circuit court addressing a situation similar to the above hypothetical embraced the broad view until *Brekka* in 2009.[72] The *Brekka* court—like others interpreting "authorization" narrowly—articulated several rationales for doing so: (1) the plain meaning of the statute compels a court to interpret "authorization" narrowly;[73] (2) the rule of lenity and canon of avoiding absurd results favor a narrow construction;[74] (3) the legislative history

67. *Id.* at 825.

68. *Id.*

69. *Id.* at 827.

70. Shamrock Foods v. Gast, 535 F. Supp. 2d 962, 964–65 (D. Ariz. 2008).

71. *Id.*

72. *See* United States. v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Phillips, 477 F.3d 215 (5th Cir. 2007); United States. v. Salum, 257 Fed. Appx. 225 (11th Cir. 2007); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504 (3rd Cir. 2005) (dicta); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

73. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006).

74. *Id.* at *7.

and congressional intent support such a finding;[75] and, (4) efficient judicial administration requires that courts interpret the statute narrowly.[76]

### 1. Plain Meaning

Many courts narrowly construing "authorization" in the CFAA note that the plain language of the Act supports such a reading because the term is undefined and the statute is silent as to misuse.[77] It is a fundamental canon of statutory construction that when a statutory term is undefined it must be given its ordinary meaning.[78] "Authorization" is commonly understood as "the act of conferring authority; permission."[79] Proponents of the narrow view argue that the statute only addresses unauthorized procurement or alteration of information, and "without authorization" or "exceeds authorized access" "cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access."[80] Courts draw a clear distinction between initial authorization to access information and an individual's subsequent use of that information.[81] The statute does not mention "misuse,"[82] and the common understanding of "authorization" obviates the need to seek outside sources, including Agency law principles, to interpret the term.[83]

Further, other parts of the statute, specifically the definitions of "damage" and "loss," are consistent with the plain meaning interpretation and a prohibition on computer hacking.[84] Extending liability whenever individuals misuse computer information to which they have been granted access would be a departure from the plain meaning of the statutory text and would extend liability beyond the

75. ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 613 (M.D. Tenn. 2010).

76. Boyer, *supra* note 8, at 661–63.

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

78. *See* United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (holding that the word "authorization" for purposes of the CFAA is "of common usage, without any technical or ambiguous meaning"); United States v. Aleynikov, No. 10 Cr. 96(DLC), 2010 WL 3489383, at *15 (S.D.N.Y. Sept. 3, 2010).

79. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006) (quoting *The American Heritage Dictionary* 89 (1976)) (brackets omitted).

80. *Aleynikov*, 2010 WL 3489383, at *15.

81. *Id.*

82. *See* 18 U.S.C. § 1030 (2008).

83. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008).

84. Major, Lindsey & Africa, LLC v. Mahn, No. 10 Civ. 4239(CM), 2010 WL 3959609, at *5 (S.D.N.Y. Sep. 7, 2010).

bounds Congress intended.[85] In summary, an employee is authorized to access a company computer "[w]hen the employer gives the employee permission to use it."[86]

2. The Rule of Lenity and Canon of Avoiding Absurd Results

A second argument advanced by courts narrowly construing "authorization" relies on the rule of lenity and the canon of avoiding absurd results.[87] The rule of lenity states that courts should resolve any ambiguity in a criminal statute in favor of the defendant, because defendants should be on notice as to which acts are criminal.[88] Courts apply the rule to the CFAA because the Act is primarily a criminal statute.[89] Narrow view advocates point out that, because nothing in the statute suggests that employee liability turns on a breach of loyalty, it would be improper to hold an employee criminally liable for such a breach:[90]

> If the 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 . . . 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.[91]

The rule of lenity also applies in the civil context because when a statute "has 'both criminal and noncriminal application,' courts must 'interpret the statute consistently.'"[92] The rule of lenity is inherently a back-up to the plain meaning argument:[93] "Authorization" should be given its plain meaning, but in the event that a court finds the term ambiguous, it should resolve that uncertainty in favor of the defendant and construe the statute narrowly.[94] To hold otherwise

85. *Aleynikov*, 2010 WL 3489383, at *15.

86. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).

87. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. Aug. 1, 2006).

88. Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010).

89. The civil provision was an add-on to that statute in 1994–"an afterthought." Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965–66 (D. Ariz. 2008).

90. Lewis-Burke Assocs. v. Widder, 725 F. Supp. 2d 187, 193 (D.D.C. 2010) (quoting *Brekka*, 581 F.3d at 1135).

91. *Id.* (quoting LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009)).

92. *Bell Aerospace Servs., Inc.*, 690 F. Supp. 2d at 1272 (quoting Leocal v. Ashcroft, 543 U.S. 1 (2004)).

93. The reason is that if the statute is not ambiguous and is accorded its plain meaning then courts never look to the rule of lenity. The rule of lenity is only invoked when courts face an ambiguous statute.

94. *Gast*, 535 F. Supp. 2d at 966–67.

would "sweep broadly within the criminal statute breaches of contract involving a computer."[95]

Courts have also looked at the potentially absurd results that would result from construing "authorization" broadly and imputing agency law principles to the CFAA.[96] In *Lockheed Martin Corp. v. Speed*, the court noted that by reading agency principles into the statute, "employers suddenly have a federal cause of action whenever employees access the company computer with 'adverse interests' and such access causes a statutorily recognized injury."[97] Employees routinely use "protected computers" throughout their workday for a vast array of functions, including many unrelated to an employer's business.[98] As one commentator stated, "employee use of computers tracks employee attention spans."[99] In addition to carrying out duties in their official capacities, employees invariably check personal email, weather, or news throughout the workday—activities that, if done without permission and inadvertently causing damage, may give rise to CFAA liability under the broad interpretation of "authorization."[100]

### 3. Legislative History and Congressional Intent

A third argument espoused by "narrow view" proponents is that the history and intent behind the statute both favor a narrow construction.[101] Courts note that Congress originally enacted the statute to create a cause of action against computer hackers,[102] according to a 1984 House Report, which emphasized that the CFAA "deals with an 'unauthorized access' concept of computer fraud rather

---

95. *Id.* at 967.

96. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. Aug. 1, 2006).

97. *Id.*

98. *Id.*

99. Kerr, *supra* note 13, at 1585.

100. *Speed*, 2006 WL 2683058, at *7.

101. *See* ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 613 (M.D. Tenn. 2010) ("Congress did not intend the CFAA to extend to situations where the access was technically authorized but the particular use of the information was not."); Jet One Group, Inc. v. Halcyon Jet Holdings, Inc., No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864, at *6 (E.D.N.Y. Aug. 14, 2009) ("[T]he statute, read as a whole, strongly indicates that Congress' intent was to prohibit the act of accessing a computer without authorization – not misusing data that one had a lawful right to access."); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1617 (2003) (arguing that the legislative history supports the conclusion that Congress intended the CFAA to do for computers what trespass and burglary laws did for real property); *see also* Field, *supra* note 5, at 829–41 (2009) (thoroughly discussing the CFAA's legislative history devoid of any factual coloring to determine what, if any, value and insight can be derived from the statute's legislative history).

102. Shamrock Foods v. Gast, 535 F. Supp. 2d 962, 965–66 (D. Ariz. 2008).

than the mere use of a computer."[103] As recognized by the U.S. District Court for the Southern District of New York, "Congress was endeavoring to outlaw computer hacking and electronic trespassing, not providing a new means of addressing the unfaithful employee situation."[104] Furthermore, Congress aimed the 1986 amendment at narrowing the sweep of the statute by removing one of the "murkier grounds of liability," the result of which was a person's access might have been be legitimate in one instance, but criminal in another nearly identical instance.[105] The amendment eliminated any reference to a defendant's purpose for accessing information, and instead focused on access—core language that remains unchanged.[106] Courts embracing the narrow view also cite Senate reports highlighting the difference between "access without authorization" and "exceeding authorized access."[107] The reports suggest that Congress was more concerned with "outsiders," such as hackers or others "without authorization" than "insiders" such as employees, who "exceed authorized access."[108] Congress intended to eliminate electronic trespassing, not to police or monitor an insider's subsequent use of a computer after access is granted.[109] Unsurprisingly, courts favoring the "broad view" also use legislative history to support their interpretation, suggesting that the history is ambiguous, and therefore a less compelling justification of either view.[110]

### 4. Judicial Administration

Finally, narrow-view proponents argue that a broad construction of the statute places an undue administrative burden on

---

103. H.R. REP. NO. 98-894, at 3706 (1984); *see also* Briggs v. State, 704 A.2d 904, 911 (Md. 1998) (quoting Committee Report System, Summary of Committee Report, House Bill 121 (1984)) ("The purpose of the bill is to deter individuals from breaking into computer systems.").

104. Major, Lindsey & Africa, LLC v. Mahn, No. 10 Civ. 4239(CM), 2010 WL 3959609, at *6 (S.D.N.Y. Sep. 7, 2010).

105. *See Gast*, 535 F. Supp. 2d at 966 ("By enacting this amendment, and providing an express definition for 'exceeds authorized access,' the intent was to 'eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,' thereby 'removing from the sweep of the statute one of the murkier grounds of liability, under which a 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.") (quoting Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 n. 12 (D. Md. 2005)) (internal brackets omitted).

106. US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009).

107. *Gast*, 535 F. Supp. 2d at 966.

108. *Id.*

109. *Id.*

110. *See* Field, *supra* note 5, at 829–30 ("[M]any of the courts struggling to interpret authorization have turned to the CFAA's legislative history, often finding support for whichever interpretation they themselves adopt in the end.").

federal courts, because it forces them to resolve disputes brought by employers against employees, suits traditionally within the province of state courts, which implicate state, more so than federal, interests.[111] In addition to the anchor claim, federal courts will also hear the derivative claims "so related" to the CFAA claim that they arise out of the same case or controversy.[112] The increased caseload is both inefficient and expensive for the federal judicial system.[113]

#### 5. Criticisms of the "narrow view"

There are very few criticisms of the narrow view noted in court opinions.[114] However, one court has found the rule of lenity unavailing because no statutory ambiguity exists.[115] Another criticism of the narrow view is that it does not provide the necessary flexibility to combat computer crime as it continues to evolve.[116] Taking a black-and-white view of "authorization" would deprive courts of the flexibility to find liability in the infrequent circumstances that may warrant it.[117]

Moreover, the narrow view would preclude many actions arising from disloyal employees being brought in federal court. While narrow view proponents view this as a benefit in reducing the federal case load, it may also eliminate the benefit of a uniform body of law in this area. Also, in criticizing the absurd results argument, broad view proponents would argue that the absurd results achieved from construing "authorization" broadly does not consider an employee's intent.

### *B. The "Broad View"—Employee Misuse Vitiates Authorization*

All but one circuit court confronting situations similar to the hypothetical posed in this Note have construed "authorization" broadly.[118] The broad interpretation advances the theory that an employer has a cause of action under the CFAA when an employee with disloyal intent obtains business information for his own benefit

---

111. *See* Boyer, *supra* note 8, at 662 ("[T]he issues of 'unauthorized use' or 'damage or loss' . . . should be construed narrowly" in order to keep the claims out of federal court. Otherwise the courts will be overrun with claims by employers against former employees.").

112. *Id.*

113. *Id.* at 663.

114. *See, e.g.*, NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042 (S.D. Iowa 2009).

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

116. *See infra* Part II.

117. *Id.*

118. *See supra* Part II.

or that of a competitor.[119] Under this view, an employee may be initially "authorized" but loses that authorization once the employee acts with adverse interests to his or her employer "against the duty of loyalty imposed on an employee in an agency relationship."[120] The primary difference between the narrow and broad interpretation is that under the broad interpretation, an employee can lack authorization in two ways: Either the employee "(1) was never granted permission to use the computer" (comports with the narrow view); or "(2) has been granted access as the access-grantor's agent but loses authorization to access the computer when the agent breaches his duty of loyalty."[121] Implicit in this view is the integration and merger of agency law principles into the CFAA.[122]

The broad view focuses on "an employee's initial access of the employer's computer with the intent to either obtain information or defraud the employer."[123] In *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit became the first federal appellate court to squarely address the meaning of "authorization" in the context of a civil CFAA claim brought by an employer.[124] The *Explorica* court and other circuit courts, as well as numerous district courts,[125] provide several rationales for construing "authorization" broadly, including: (1) the agency relationship, between an employee and his employer, and the duty of loyalty implicit in it;[126] (2) the presence of employer agreements with its employees;[127] and (3) legislative history and congressional intent.[128] Interestingly, courts that interpret the statute

---

119. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 964 (D. Ariz. 2008).

120. *Nosal*, 2009 WL 981336, at *5.

121. NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1057 (S.D. Iowa 2009).

122. *Nosal*, 2009 WL 981336, at *5.

123. *Artino*, 638 F. Supp. 2d at 1059.

124. 274 F.3d 577 (1st Cir. 2001). The next Circuit court case decided which dealt with the disloyal employee fact set was Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006). Several other cases predated both *Citrin* and *Explorica*, but they are distinguishable. *See* United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997); United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

125. *See, e.g.*, Guest-Tek Interactive Entm't Inc. v. Pullen, 665 F. Supp. 2d 42 (D. Mass. 2009); *Artino*, 638 F. Supp. 2d at 1042; Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

126. Ervin & Smith Adver. & Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998, at *8 (D. Neb. Feb. 3, 2009) ("[W]hile the Defendants ordinarily may have been authorized to access the information they appropriated from Plaintiff, that authorization was terminated when Defendants destroyed the agency relationship by accessing and appropriating the protected information for their own personal gain and against the interest of their employer.").

127. *Explorica*, 274 F.3d at 581–82; Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05-CV-456, 2007 WL 275476, at *13 (E.D. Tex. 2007).

128. *Pullen*, 665 F. Supp. 2d at 45–6; Pac. Aero. & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003).

broadly are more inclined to rely upon case precedent for doing so.[129] In the hypothetical introduced above, Andy violated the CFAA under the broad view because he breached his duty of loyalty to his employer by accessing Spotless's computers to send client lists and other confidential data and therefore, his access was "unauthorized."[130]

### 1. Agency Law Principles

An argument commonly raised in favor of the broad interpretation of "authorization," based on agency law principles, asserts that a breach of the duty of loyalty owed by employees to employers terminates the agency relationship and renders previously authorized access to computer files unauthorized.[131] One of the more influential and oft-cited cases employing this argument is *Int'l Airport Centers, LLC v. Citrin*.[132] In *Citrin*, an employer sued a former employee who had deleted all data from his laptop, including the results of his work and evidence of previous improper conduct, before returning the computer to his employer.[133] The court found:

> [h]is authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit . . . in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.[134]

Relying on the black-letter agency principle that "[u]nless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or is otherwise guilty of a serious breach of loyalty to the principal,"[135] courts have found that an employee's authorization terminates the moment he acquires interests adverse to his employer.[136] This theory requires judicial inquiry into the employee's state of mind at the time of data access.[137]

---

129. *See, e.g.*, PharMerica, Inc. v. Arledge, No. 8:07-cv-486-T-26MAP, 2007 WL 865510 (M.D. Fla. Mar. 21, 2007). This may be because many of the early decisions construed "authorization" broadly and it was easy for courts to cite to and follow established case precedent.

130. *Artino*, 638 F. Supp. 2d at 1057.

131. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

132. 440 F.3d 418 (7th Cir. 2006).

133. *Id.* at 419.

134. *Id.* at 420.

135. RESTATEMENT (SECOND) OF AGENCY § 112 (1958).

136. *Shurgard Storage*, 119 F. Supp. 2d at 1125.

137. *Id.*

### 2. Employer Policies and Agreements

While not an argument for broad construction in general, courts have construed the CFAA more liberally where a policy of the employer, or agreement with the employee, explicitly proscribes prohibited conduct.[138] However, while the presence of an employment agreement may bolster the employer's case against a rogue employee, it is not dispositive.[139] In *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit held that employer agreements may define the limits of "authorization."[140] The former employees in that case used their knowledge of proprietary codes in breach of their confidentiality agreement with their former employer to create a program that significantly increased the efficiency with which they could collect information from their former employer's website.[141] Even though the website was public, the ex-employees' use of confidential information in accessing it more efficiently made the access "unauthorized."[142] Other courts, while not specifically relying on employer agreements to find employee access "unauthorized," have found the presence of employer agreements noteworthy in defining "authorized access."[143]

### 3. Legislative History and Congressional Intent

In addition to agency principles and employment agreements, broad-view proponents also cite legislative history indicating that Congress intended the CFAA to have an expansive reach.[144] Advocates of the broad-view rely on the consistent Congressional expansion of the CFAA's scope and coverage since its enactment, in particular, the amendment in 1994 providing for a civil remedy.[145] Courts point to these expansions as proof of Congress's intent to

---

138. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–82 (1st Cir. 2001).

139. *Id.*

140. *Id.*

141. *Id.*

142. *Id.*

143. *See* Ervin & Smith Adver. & Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998, at *8 (D. Neb. Feb. 3, 2009) ("The Confidential Agreement in the Ervin & Smith Employee Handbook supports Plaintiff's contention that Defendants were only authorized to access this protected information so long as they abided by the agreed-upon terms found within the Handbook. . . . Consequently, the Court concludes that Defendants never had authorization to access Plaintiff's protected information to further their own business interests. Instead, when Defendants allegedly violated the Confidential Agreement and allegedly appropriated Plaintiff's secret information for their own private benefit, they exceeded their authorized access.").

144. Guest-Tek Interactive Entm't Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009).

145. *Id.*; Pac. Aero. & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003).

extend the Act beyond hacking, and bring a wide array of computer crimes within its reach, including actions such as Andy's toward Spotless.[146] Several specific amendments illustrate this intent. In addition to the civil remedy for the "unauthorized removal of information from a company's computer database" added in 1994,[147] Congress also widened the CFAA's sweep to encompass more computers by replacing "federal interest computer" with "protected computer."[148] Those favoring a broad construction of the statute argue that a narrow reading ignores Congress's statutory amendments consistently broadening the application of the CFAA, which they view as a signal that Congress intended to cast a wide net over crimes perpetrated with computers.[149]

### 4. Criticisms of the "Broad View"

Those who believe "authorization" should be construed narrowly have criticized the reasoning that courts adopting the broad view employ.[150] Criticisms of the broad view include: (1) the statutory amendments to the CFAA, while broadening its scope, did not deal with "authorization;"[151] (2) the absence of any statutory language pertaining to employee misuse of company information;[152] and (3) the void for vagueness doctrine, which supports a narrow view of "authorization."[153]

The first two counterpoints are straightforward and require little explanation. As noted, Congress has amended the CFAA numerous times, and each amendment has expanded the scope of the statute.[154] However, the amendments primarily relate to penalties associated with a CFAA violation and did not alter the "without

146. NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009).

147. *Taylor*, 295 F. Supp. 2d at 1196.

148. *See Artino*, 638 F. Supp. 2d at 1058–59 (quoting S. REP. NO. 104-357, at 7–8 (1996)) ("[T]he proposed § 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer . . . . This [section] would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. . . . The crux of the offense under § 1030(a)(2)(C), however, is the abuse of a computer to obtain the information. . . . For example, individuals who intentionally break into, or abuse their authority to use, a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for the purposes of commercial advantage or private financial gain . . . .").

149. *Id.* at 1058.

150. *See, e.g.*, Kerr, *supra* note 13, at 1585.

151. ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 613 (M.D. Tenn. 2010).

152. United States v. Aleynikov, No. 10 Cr. 96(DLC), 2010 WL 3489383, at *17 (S.D.N.Y. Sept. 3, 2010).

153. Kerr, *supra* note 13, at 1585.

154. Guest-Tek Interactive Entm't Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009).

authorization" requirement to invoke liability. Congress has given no indication as to how courts should construe "authorization."[155] Furthermore, courts that have read the statute broadly "identify no statutory language that supports interpreting the CFAA to reach misuse or misappropriation of information that is lawfully accessed. Instead, they improperly infer that 'authorization' is automatically terminated where an individual 'exceeds the purposes for which access is authorized.'"[156] Indeed, the statutory text does not mention "misuse of information."[157] The CFAA establishes unauthorized access as a predicate for any violation, making it unreasonable that an employee, working on his own computer, could incur CFAA liability.[158] For liability to result from an employee's improper activities on his own computer, broad-view courts must determine his subjective intent when viewing the information.[159] This is typically established by analyzing how the employee used the information.[160] It seems unlikely, however, that Congress intended such a subjective analysis under the CFAA.[161] It contorts the statute to say that an employee does not have authorized access to his work computer because of his subjective intent in doing so.[162] An employee is either "authorized," or not, and it would be quite odd to think that an employee could lose his authorization simply by changing his thoughts.

Scholars have more recently argued that the void for vagueness doctrine also requires courts to reject the broader agency view of authorization.[163] The doctrine instructs that if a statute provides insufficient clarity for the average citizen to understand what it prohibits and to whom it applies, the vagueness renders it void and unenforceable.[164] The broader agency view of authorization leaves many questions unanswered and does not provide sufficient guidance to citizens as to what conduct is prohibited; therefore, the argument goes, courts should reject it as unconstitutionally vague.[165] As one commenter asked:

---

155. *ReMedPar*, 683 F. Supp. 2d at 613.

156. *Aleynikov*, 2010 WL 3489383, at *17.

157. 18 U.S.C. § 1030 (2008).

158. Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. Aug. 1, 2006).

159. *Id.* at *6.

160. *Id.*

161. *Aleynikov*, 2010 WL 3489383, at *17.

162. *Id.*

163. Kerr, *supra* note 13, at 1585.

164. *Id.* at 1573.

165. *Id.* at 1585.

> Is use of an employer's computer for personal reasons always prohibited? Sometimes prohibited? If sometimes, when? And if some amount of personal use is permitted, where is the line? If use of an employer's computer directly contrary to the employer's interest is required, how contrary is directly contrary? Is mere waste of the employee's time enough?[166]

These are some of the many questions that arise from, and remain unanswered by, the broad view of "authorization" based in agency law.[167]

The void for vagueness doctrine is rooted in the Due Process Clause and has two independent tests: (1) does the law provide fair notice as to what it prohibits?; and (2) does the law allow for discriminatory enforcement?[168] The fair notice test asks whether the law is "so vague and standardless that it leaves the public uncertain" as to the prohibited conduct, leaving judges and jurors to decide cases without fixed standards.[169] The discriminatory enforcement component finds that a statute is "unconstitutionally vague if it does not 'establish minimal guidelines to govern law enforcement,'" and therefore encourages arbitrary and discriminatory enforcement.[170] Because the broad view fails to define what employee conduct is prohibited, and because it allows prosecutors, judges, and juries undue discretion to punish some "offenders" but not others, it violates the void for vagueness doctrine.[171] Therefore, courts must either invalidate the CFAA or adopt the narrow interpretation both to provide the fair warning necessary to defendants and to limit government discretion.[172]

### *C. Trends in Court Opinions Addressing the Employee-Employer Context*

When surveying the opinions confronting employer claims against former disloyal employees, some trends emerge that may shed

---

166. *Id.*

167. *Id.* at 1586; *see also* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (holding that conviction under the CFAA based only on defendant's intentional violation of internet website's terms of service would violate the void-for-vagueness doctrine).

168. Kerr, *supra* note 13 at 1573.

169. *Id.*

170. *Id.* at 1574 (quoting Kolender v. Lawson, 461 U.S. 352, 358 (1983)).

171. *Id.* at 1586. The void for vagueness doctrine refers to a "statute defining a crime which is so vague that a reasonable person of at least average intelligence could not determine what elements constitute the crime. Such a vague statute is unconstitutional on the basis that a defendant could not defend against a charge of a crime which he/she could not understand, and thus would be denied 'due process' mandated by the 5th Amendment." *Void for Vagueness*, LAW.COM LEGAL DICTIONARY, http://dictionary.law.com/Default.aspx?selected=2228 (last visited Feb. 08, 2010).

172. Kerr, *supra* note 13, at 1575.

light on how the Supreme Court might ultimately to resolve this issue.[173] As noted above, all but one circuit hearing employer claims arising from a situation similar to the hypothetical posed in this Note have construed the CFAA broadly, finding that "authorization" terminated when the employee acquired adverse interests to the employer.[174] While the broad view faction is dominant in circuit court opinions, a more even split emerges when rulings on this issue by federal district courts are also considered.[175] Looking at these

---

173. *See infra* Part II.

174. *Compare* United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. v. Citrin, 440 F.3d 418 (7th Cir. 2006); *Explorica*, 274 F.3d at 577 (construing the CFAA broadly finding employee liability), *with Brekka*, 581 F.3d at 1127 (construing the CFAA narrowly finding that subsequent misuse is irrelevant so long as initial access was authorized). *See also* P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504 (3rd Cir. 2005) (although not the holding of the case, the opinion seems to favor a broad construction of "authorization").

175. *Compare John*, 597 F.3d at 263; *Citrin*, 440 F.3d at 418; *P.C. Yonkers, Inc.*, 428 F.3d at 504; *Explorica*, 274 F.3d at 577; Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LLM), 2010 WL 2034404 (S.D.N.Y. May 18, 2010); Guest-Tek Interactive Entm't Inc. v. Pullen, 665 F. Supp. 2d 42 (D. Mass. 2009); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042 (S.D. Iowa 2009); Dental Health Prods., Inc. v. Ringo, No. 08-C-1039, 2009 WL 1076883 (E.D. Wis. Apr. 20, 2009); Motorola, Inc. v. Lemko Corp., 609 F. Supp. 2d 760 (N.D. Ill. 2009); United States v. Nosal, No. CR 08-00237, 2009 WL 981336 (N.D. Cal. Apr. 13, 2009); Ervin & Smith Adver. & Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998 (D. Neb Feb. 3, 2009); TEKsystems, Inc. v. Modis, Inc., No. 08 C 5476, 2008 WL 5155720 (N.D. Ill. Dec. 5, 2008); Alliance Int'l, Inc. v. Todd, No. 5:08-CV-214-BR, 2008 WL 285 9095 (E.D.N.C. Jul. 22, 2008); Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122 (E.D. Cal. 2008); Res. Ctr. for Indep. Living, Inc. v. Ability Res., Inc., 534 F. Supp. 2d 1204 (D. Kan. 2008); Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658 (S.D.N.Y. Sept. 5, 2007); Dudick ex rel Susquehana Precision, Inc. v. Vaccarro, No. 3:06-CV-2175, 2007 WL 1847435 (M.D. Pa. Jun. 25, 2007); Pharmerica, Inc. v. Arledge, No. 8:07-cv-486-T-26MAP, 2007 WL 865510 (M.D. Fla. Mar. 21, 2007); Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05-CV-456, 2007 WL 275476 (E.D. Tex. Jan. 25, 2007); Forge Indus. Staffing, Inc. v. De La Fuente, No. 06 C 3848, 2006 WL 2982139 (N.D. Ill. Oct. 16, 2006); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087 (N.D. Cal. 2006); Int'l Sec. Mgt. Group, Inc. v. Sawyer, No. 3:06CV0456, 2006 WL 1638537 (M.D. Tenn. Jun. 6, 2006); Nilfisk-Advance, Inc. v. Mitchell, No. Civ. 05-5179, 2006 WL 827073 (W.D. Ark. Mar. 28, 2006); Hub Grp., Inc. v. Clancy, No. Civ.A. 05-2046, 2006 WL 208684 (E.D. Pa. Jan. 25, 2006); George S. May Int'l Co. v. Hostetler, No. 04 C 1606, 2004 WL 1197395 (N.D. Ill. May 28, 2004); Pacific Aerospace & Elec., Inc. v. Taylor, 295 F. Supp. 2d 1188 (E.D. Wash. 2003); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (construing "authorization" broadly), *with Brekka*, 581 F.3d at 1127; Oce North Am., Inc. v. MCS Serv., Inc., No. WMN-10-CV-984, 2010 WL 3703277 (D. Md. Sept. 16, 2010); Major, Lindsey & Africa, LLC v. Mahn, No. 10 Civ. 4239(CM), 2010 WL 3959609 (S.D.N.Y. Sept. 7, 2010); United States v. Aleynikov, No. 10 Cr. 96(DLC), 2010 WL 3489383 (S.D.N.Y. Sept. 3, 2010); Lewis-Burke Assocs., LLC v. Widder, 725 F. Supp. 2d 187, 192-94 (D.D.C. 2010); Univ. Sports Pub. Co. v. Playmakers Media Co., No. 09 Civ. 8206(RJH), 2010 WL 2802322 (S.D.N.Y. Jul. 14, 2010); Nat'l City Bank, N.A. v. Republic Mortg. Home Loans, LLC, No. C09-1550RSL, 2010 WL 959925 (W.D. Wash. Mar. 12, 2010); Orbit One Commc'n, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010); Consulting Prof'l Res., Inc. v. Concise Tech. LLC, No. 09-1201, 2010 WL 1337723 (W.D. Pa. Mar. 9, 2010); Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d 1267 (M.D. Ala. 2010); Clarity Servs., Inc. v. Barney, No. 8:08-cv-2278-T-23TBM, 2010 WL 1140865 (M.D. Fla. Feb. 26, 2010); ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010); Mortg. Now, Inc. v. Stone, No. 3:09cv80/MCR/MD, 2009 WL 4262877

decisions over time, it appears that, while courts favored the broad view early on, the narrow view has recently gained critical mass.[176]

First, this Note examines decisions involving a situation like the Spotless hypothetical.[177] Looking at the decisions of both circuit and district courts by year, the number of courts construing "authorization" in the CFAA narrowly versus those construing it broadly breaks down as follows: From 2000 to 2006, eleven opinions adopted the broad view while three adopted the narrow.[178] In 2007, four courts interpreted "authorization" broadly and three narrowly.[179] In 2008, there were four broad decisions and three narrow.[180] In 2009 the trend started to shift, with six broad decisions and eleven narrow.[181] As of late 2010, two courts had chosen the broad view and eleven the narrow.[182] These numbers show that courts have shifted from favoring the broad view to an overwhelming preference for the narrow.[183] It is difficult to determine exactly why this switch has occurred, but one influential factor may be *Brekka*,[184] which gave district courts a persuasive precedent, as well as arguments to cite,

---

(N.D. Fla. Nov. 24, 2009); Joe N. Pratt Ins. v. Doane, No. V-07-07, 2009 WL 3157337 (S.D. Tex. Sep. 25, 2009); Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378 (E.D. Pa. 2009); Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc.,No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009); Vurv Tech. LLC v. Kenexa Corp., No. 1:08-cv-3442-WSD, 2009 WL 2171042 (N.D. Ga. Jul. 20, 2009); Salestraq Am., LLC v. Zyskowski, 635 F. Supp. 2d 1178 (D. Nev. 2009); Am. Family Mut. Ins. Co. v. Hollander, No. C08-1039, 2009 WL 535990 (N.D.Iowa Mar. 3, 2009); Bridal Expo, Inc. v. Van Florestein, No. 4:08-cv-03777, 2009 WL 255862 (S.D. Tex. Feb. 3, 2009); Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., & Consulting LLC, 600 F. Supp. 2d 1045 (E.D. Mo. 2009); US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189 (D. Kan. 2009); Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818 (D. Minn. Dec. 15, 2008); Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929 (W.D.Tenn. 2008); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008); Diamond Power Int., Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D.Ga. 2007); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744 (W.D. Pa. 2007); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006); Int'l Assoc. of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005); Secureinfo Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005) (construing "authorization" narrowly).

176. *Widder*, 725 F. Supp. 2d at 194.

177. Some judgment was exercised in sorting through the cases to determine which are close enough to the hypothetical between Spotless and Andy presented in this Note. Included in the cases under consideration for this section are 5 Circuit Court opinions and 53 District Court opinions. *See supra* note 175.

178. *See supra* note 175.

179. *Id.*

180. *Id.*

181. *Id.*

182. *Id.*

183. *See supra* Part II.

184. *See* NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) ("[N]o Courts of Appeals decisions have adopted the narrow view of the CFAA.").

when construing the statute narrowly.[185] Prior to *Brekka*, most courts interpreted authorization broadly, but they provided little explanation for doing so, and summarily cited binding or persuasive precedent. Conversely, courts that did rule narrowly provided more robust explanations for their decisions.[186]

Since several Circuit Courts of Appeal have already ruled on the authorization issue, so that courts in those jurisdictions cannot make an independent decision, the more interesting analysis turns on the district court cases in circuits without binding precedent—the Second, Third, Fourth, Sixth, Eighth, Tenth, Eleventh, and D.C. Circuits. Lower courts within the Second Circuit favor the narrow approach with five narrow decisions and two broad decisions from 2007 to 2010.[187] Significantly, in 2010, only one of five decisions in the Second Circuit interpreted "authorization" broadly.[188] The law in the Third Circuit is interesting because while one appellate opinion hints in dicta that the CFAA should be construed broadly, subsequent district court opinions have declined to adopt the dicta.[189] The circuit is fairly evenly split with three broad and four narrow decisions from 2005 to 2010; however, similar to the overall trend, district courts in the Third Circuit have clearly favored the narrow view recently.[190] The Fourth and Sixth Circuits have also shown a preference for the narrow view by three to one in the Fourth Circuit and two to one in

185. Indeed, reading through 7th Circuit opinions subsequent to *Citrin*, the courts seemingly feel handcuffed as a result of binding precedent construing the statute broadly. *See, e.g.*, Dental Health Prods., Inc. v. Ringo, 2009 WL 1076883, at *6–7 (E.D. Wis. Apr. 20, 2009).

186. *Compare, e.g.*, Hub Grp., Inc. v. Clancy, No. Civ.A. 05-2046, 2006 WL 208684 (E.D. Pa. Jan. 25, 2006), *with* Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006).

187. *Compare* Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LLM), 2010 WL 2034404 (S.D.N.Y. May 18, 2010), *and* Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658 (S.D.N.Y. Sept. 5, 2007) (construing "authorization" broadly), *with* Major, Lindsey & Africa, LLC v. Mahn, No. 10 Civ. 4239(CM), 2010 WL 3959609 (S.D.N.Y. Sept. 7, 2010); United States v. Aleynikov, No. 10 Cr. 96(DLC), 2010 WL 3489383 (S.D.N.Y. Sept. 3, 2010); Univ. Sports Pub. Co. v. Playmakers Media Co., No. 09 Civ. 8206(RJH), 2010 WL 2802322 (S.D.N.Y. Jul. 14, 2010); Orbit One Commc'n, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010); Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc., No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009) (construing "authorization" narrowly).

188. *Id.*

189. P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504 (3rd Cir. 2005).

190. *Id.*; Consulting Prof'l Res., Inc. v. Concise Tech. LLC, No. 09-1201, 2010 WL 1337723 (W.D. Pa. Mar. 9, 2010); Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378 (E.D. Pa. 2009); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007); Dudick ex rel Susquehana Precision, Inc. v. Vaccarro, No. 3:06-CV-2175, 2007 WL 1847435 (M.D. Pa. Jun. 25, 2007); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744 (W.D. Pa. 2007); Hub Grp., Inc. v. Clancy, No. Civ.A. 05-2046, 2006 WL 208684 (E.D. Pa. Jan. 25, 2006).

the Sixth Circuit.[191] A district court in the D.C. Circuit also joined the narrow camp with its recent opinion, *Lewis-Burke Assocs., LLC v. Widder*.[192] The Eighth and Tenth Circuits are evenly split on the issue.[193] The Eleventh Circuit has not been nearly as conflicted on this issue and is dominated by courts construing "authorization" narrowly, by a ratio of six to one.[194] Overall, the district courts in circuits yet to confront this issue have shown a fairly strong preference for the narrow interpretation of "authorization," citing many of the same rationales discussed above.[195]

### *D. The Crystal Ball—Supreme Court Clues*

Given Congress's reluctance to further delimit the CFAA, a uniform definition of "authorization" will need to come from the Supreme Court.[196] Several Supreme Court decisions may shed light on how the Court could frame and resolve the interpretation of "authorization."[197]

As the Court has long recognized, "laws so vague that a person of common understanding cannot know what is forbidden are

---

191. *Compare* Oce North Am., Inc. v. MCS Serv., Inc., No. WMN-10-CV-984, 2010 WL 3703277 (D. Md. Sept. 16, 2010); ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010); Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929 (W.D.Tenn. 2008); Int'l Assoc. of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005); Secureinfo Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005), *with* Alliance Int'l, Inc. v. Todd, No. 5:08-CV-214-BR, 2008 WL 285 9095 (E.D.N.C. Jul. 22, 2008); Int'l Sec. Mgt. Group, Inc. v. Sawyer, No. 3:06CV0456, 2006 WL 1638537 (M.D. Tenn. Jun. 6, 2006).

192. Lewis-Burke Assocs. v. Widder, 725 F. Supp. 2d 187 (D.D.C. 2010).

193. NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042 (S.D. Iowa 2009); Am. Family Mut. Ins. Co. v. Hollander, No. C08-1039, 2009 WL 535990 (N.D. Iowa Mar. 3, 2009); Ervin & Smith Adver. & Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009); US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189 (D. Kan. 2009); Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., & Consulting LLC, 600 F. Supp. 2d 1045 (E.D. Mo. 2009); Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818 (D. Minn. Dec. 15, 2008); Res. Ctr for Indep. Living, Inc. v. Ability Res., Inc., 534 F. Supp. 2d 1204 (D. Kan. 2008); Nilfisk-Advance, Inc. v. Mitchell, No. Civ. 05-5179, 2006 WL 827073 (W.D. Ark. Mar. 28, 2006).

194. Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d 1267 (M.D. Ala. 2010); Clarity Servs., Inc. v. Barney, No. 8:08-cv-2278-T-23TBM, 2010 WL 1140865 (M.D. Fla. Feb. 26, 2010); Mortg. Now, Inc. v. Stone, No. 3:09cv80/MCR/MD, 2009 WL 4262877 (N.D. Fla. Nov. 24, 2009); Vurv Tech. LLC v. Kenexa Corp., No. 1:08-cv-3442-WSD, 2009 WL 2171042 (N.D. Ga. Jul. 20, 2009); Diamond Power Int., Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D.Ga. 2007); Pharmerica, Inc. v. Arledge, No. 8:07-cv-486-T-26MAP, 2007 WL 865510 (M.D. Fla. Mar. 21, 2007); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006).

195. *See supra* Part II.

196. Kerr, *supra* note 13, at 1563.

197. *See supra* Part II.

unconstitutional on their face."[198] At least arguably, because authorization lacks a fixed meaning, the ambiguity renders CFAA vague—a person of common understanding cannot be sure what is forbidden.[199] By way of example, a Supreme Court case discussing the void for vagueness doctrine is *Coates v. City of Cincinnati*.[200] The case dealt with an Ohio statute making it unlawful for persons to gather on sidewalks or street corners and engage in conduct annoying to persons passing by.[201] The Court found the statute vague because the word "annoy" is unclear and cannot readily be given a fixed meaning.[202] Essentially, the Court held that "no standard of conduct [was] specified at all," leaving men of common intelligence to guess as to its meaning.[203] Similarly, the word "authorization" in the CFAA is arguably vague and cannot readily be given a fixed meaning.[204] This suggests that the Supreme Court may construe the term narrowly.

Another Supreme Court case relevant to the issue is *Carpenter v. United States*, which approved the conversion of an ordinary duty of loyalty violation into a federal offense.[205] Relying upon agency principles, the court affirmed mail- and wire-fraud convictions of a Wall Street Journal ("Journal") reporter who provided insider information to his cohorts, who then used the information to engage in profitable stock transactions.[206] The Court noted that "[e]ven in the absence of a written contract, an employee has a fiduciary obligation to protect confidential information obtained during the course of his

198. Coates v. City of Cincinnati, 402 U.S. 611, 616 (1971) (Black, J., concurring in part, dissenting in part) (citing Lanzetta v. New Jersey, 306 U.S. 451 (1939); U.S. v. L. Cohen Grocery Co., 255 U.S. 81 (1921)).

199. *See supra* Part II.

200. *Coates*, 402 U.S. at 614–16. This argument goes that the CFAA, if not construed narrowly, is unconstitutionally vague because it does not provide adequate notice to possible defendants as to what conduct is criminal and does not provide the necessary law enforcement standards.

201. *Id.* at 611.

202. *Id.* at 614 ("We are thus relegated, at best, to the words of the ordinance itself. If three or more people meet on a sidewalk or street corner, they must conduct themselves so as not to annoy any police officer or other person who should happen to pass by. In our opinion this ordinance is unconstitutionally vague because it subjects the exercise of the right of assembly to an unascertainable standard . . . . Conduct that annoys some people does not annoy others. Thus, the ordinance is vague, not in the sense that it requires a person to conform his conduct to an imprecise but comprehensible normative standard, but rather in the sense that no standard of conduct is specified at all.").

203. *Id.*

204. *See supra* Part II.

205. Nick Akerman, *Computer Fraud and Abuse Act Count Dismissed Against Goldman Sachs Computer Programmer Charged with Stealing Source Code*, DORSEY & WHITNEY LLP (Sept. 13, 2010), http://computerfraud.us/recent-updates/computer-fraud-and-abuse-act-count-dismissed-against-goldman-sachs-computer-programmer-charged-with-stealing-source-code.

206. Carpenter v. United States, 484 U.S. 19 (1987).

employment."[207] Intentionally exploiting that information for personal benefit amounted to a scheme intended to defraud the Journal.[208] The Court showed little hesitation imputing this agency notion into mail- and wire-fraud statutes.[209] The Court reasoned that the confidential business information was the Journal's "property," which made it easier to find specific intent and fraud on behalf of the reporter and his cohorts.[210] Given the Supreme Court's readiness to impute agency principles into mail- and wire-fraud statutes to safeguard an employer's confidential business information, there is "no sound reason why it cannot also proscribe the scope of an employee's authorization to access his employer's computer in the context of the CFAA."[211]

The Supreme Court's handling of RICO cases is also instructive.[212] Specifically, the Court stated in *Boyle v. United States* that reinterpreting statutes does not render them void: "that RICO has been applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth."[213] Following that logic, one can argue that "like the RICO Act, the broad text of the CFAA 'does not demonstrate ambiguity, it demonstrates breadth.'"[214] However, the RICO statute at issue in *Boyle* can be distinguished from the CFAA, because the *Boyle* Court found the RICO statute unambiguous, while the language of CFAA is less clear.[215]

A couple of general trends toward judicial restraint in Supreme Court jurisprudence may also shed light on how the Court is likely to construe the CFAA. The Court has consistently held that statutes should not be construed aggressively in novel ways because doing so

---

207. *Id.* at 27.

208. *Id.*

209. *Id.*

210. *Id.* at 28.

211. Akerman, *supra* note 205.

212. Maxwell S. Kennerly, *Civil Remedies, The Computer Fraud and Abuse Act, and Stolen Trade Secrets,* LITIGATION & TRIAL (July 7, 2009), http://www.litigationandtrial.com/2009/07/articles/litigation/news/civil-remedies-the-computer-fraud-and-abuse-act-and-stolen-trade-secrets.

213. Boyle v. United States, 129 S. Ct. 2237, 2247 (2009).

214. Kennerly, *supra* note 212.

215. *See Boyle*, 129 S. Ct. at 2246–47 ("Because the statutory language is clear, there is no need to reach petitioner's remaining arguments based on statutory purpose, legislative history, or the rule of lenity. In prior cases, we have rejected similar arguments in favor of the clear but expansive text of the statute. . . . We have repeatedly refused to adopt narrowing constructions of RICO in order to make it conform to a preconceived notion of what Congress intended to proscribe.").

would upset the reasonable expectations of citizens,[216] and that statutes are to be interpreted according to their "plain and unambiguous meaning."[217]

## III. NARROW MINDED

Given the frequent congressional modifications to the CFAA,[218] and the long-standing judicial disagreement over the proper interpretation of "authorization" as applied to employer claims against rogue employees,[219] it is curious that Congress has not taken the opportunity to further clarify the term. Indeed, it appears unlikely that Congress will act before the Supreme Court has an opportunity to provide a fixed meaning to "authorization."[220] Because it created a circuit split, the *Brekka* decision substantially increased the likelihood that the Supreme Court will hear a case involving the interpretation of "authorization," and it likely shortened the wait.[221] After considering the arguments above, this Note proposes that the Supreme Court adopt the narrow construction of "authorization" without tests or conditions.

### *A. Resolving the Split—Keeping it Simple*

The Supreme Court should interpret "authorization" narrowly, finding that an employee who has permission to access an employer's computer is authorized to use that computer. It should be irrelevant what the employee does on the computer, because the statute emphasizes access to the computer, not its use.[222] This interpretation is not only supported by the plain meaning of the statute, the CFAA's legislative history, and the rule of lenity, but also allows for a consistent and predictable application of the statute.[223] If an employee uses her work computer to email a confidential client list to her personal email account, has she accessed the employer's computer without authorization? Clearly not—the employee has done something wrong, but the wrong was not improperly accessing the

216. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) (citing United States v. Santos, 553 U.S. 507 (2008) (plurality opinion)).

217. Robinson v. Shell Oil Co., 519 U.S. 337, 340–41 (1997).

218. *See supra* Part II.

219. *Id.*

220. Kerr, *supra* note 13, at 1563.

221. *Brekka* created a split among circuit courts as to the meaning of "authorization." Due to the presence of this split, the Supreme Court is now more likely to resolve the meaning of "authorization" in the CFAA. *See supra* Part II.

222. 18 U.S.C. § 1030 (2008).

223. *See supra* Part II.

computer. Theft provides another simple example. If a person is invited into someone's home and steals jewelry while inside, the person has committed a crime—but not burglary—because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter.

Not only does a narrow construction of "authorization" make intuitive sense, but it also sets clear boundaries for the application of the CFAA. Litigants continue to use the CFAA in novel ways, and in settings a person would not expect the Act to apply.[224] Lawyers will find any and all claims to bring against defendants and seek creative means to achieve this end, such as suing clients' former employees for misappropriating confidential information.[225] The question remains, what are the boundaries of the CFAA? By construing "authorization" broadly, it is not only uncertain as to how the statute will apply, but also where and when it will apply.

A recent example of the uncertainty engendered by the broad view is *United States v. Drew*, a case brought against a "cyberbully" under the CFAA.[226] Lori Drew set up a MySpace account pretending to be a sixteen-year-old boy named Josh Evans for the purpose of befriending her thirteen-year-old neighbor, Megan Meier.[227] Drew then abruptly ended the friendship, telling the girl that "the world would be a better place without her in it."[228] Later the same day, the young girl committed suicide.[229] Understandably, many people were upset and federal prosecutors sought to bring claims against Drew for setting up the MySpace account and tormenting her young neighbor.[230] However, the only claim actually brought was under the CFAA, on the theory that "the creation of the 'Josh Evans' profile had violated the [Terms of Service (TOS)] of MySpace.com, and that the TOS violation rendered the access to MySpace's computers" unauthorized.[231] This example is a dangerous expansion of the

224. *See infra* note 226.

225. *See supra* Part II.

226. Scott Michels, *Alleged MySpace Hoaxer on Trial Today*, ABC NEWS (Nov. 19, 2008), http://abcnews.go.com/TheLaw/story?id=6281225 ("The case is believed to be one of the first of its kind to use the statute barring unauthorized access to computers, which has previously been used to combat computer hacking, to address so-called cyberbullying. Drew's lawyers and outside legal experts have argued that the unusual prosecution, if successful, could broaden the scope of what's considered criminal conduct on the internet.").

227. *Id.*

228. Kerr, *supra* note 13, at 1579.

229. *Id.*

230. *Id.*

231. *Id.*

CFAA—even if Drew had read the CFAA, it would be unclear that the Act encompassed her conduct.[232]

The *Drew* case is an excellent example of wrongful conduct that does not fit neatly into any crime currently on the books. As a result, prosecutors search to find something close, "even if it's a stretch."[233] However, the judiciary should not "stretch" statutes to reach conduct that Congress did not criminalize.[234] The *Drew* case also illustrates the problems associated with allowing terms of service (or employment agreements) to govern the bounds of "authorization."[235] By allowing these agreements to define what is—and is not—authorized, a simple contract violation would become a federal crime.[236] It is highly unlikely that Congress meant to confer this type of power to private actors.

Under the broad view of "authorization," an employee's access could also vacillate between authorized and unauthorized depending on the circumstances.[237] As the court described in *Lewis-Burke Associates, LLC v. Widder*:

> [Under the broad view, an] employee might have different authorization to access the same document on the same computer throughout his or her employ. For example, an employee might generate a report during the course of his employment, to which he would have authorized access. If, as time progressed, the employee began looking for employment elsewhere, and he accessed the report to refresh his memory as to what he did on the report so that he could better describe his skills and abilities on his résumé or in an interview, under [the broad view] he would have accessed the report without authorization. Then, if the employee was internally promoted, decided not to seek outside employment, and accessed the report to provide an example to one of his new subordinates of how he liked reports written, his interests would again be aligned with the employer, and his access would be authorized. In the extreme example, the same employee's authorization to access a document could concurrently be both with authorization and exceeding authorization. For example, the employee could have authority to access a report to e-mail it out for a superior to review, but his authorization might be exceeded if he then also decided to blind copy his personal e-mail account, so that he would have a copy of the report to use as a writing sample for a future job search. Congress could not have intended a person's criminal and civil

232. *See* Michels, *supra* note 226 ("'It seems this is advancing arguments that are a dangerous expansion of the law . . . . When you think of computer hacking, you think of picking virtual locks. But when we're talking about violating the terms of service [of MySpace], we're no longer talking about breaking a lock, just about breaking a rule that you probably didn't know existed.'").

233. Mary Fulginiti & Bonnie McLean, *Prosecutors Get Creative in MySpace Hoax Case*, ABC NEWS (Mar. 25, 2008), http://abcnews.go.com/TheLaw/story?id=4515995.

234. Separation of power principles reserve lawmaking for Congress, and by "stretching" existing statutes the judiciary is in essence legislating.

235. Kerr, *supra* note 13, at 1581.

236. *Id.*

237. Lewis-Burke Assocs. v. Widder, 725 F. Supp. 2d 187, 193 (D.D.C. 2010).

> liability to be so fluid, turning on whether a person's interests were adverse to the interests of an entity authorizing the person's access.[238]

Part of the problem is that technology is outpacing the law, and the legislature needs to catch up.[239] Courts should not attempt to remedy the situation by contorting existing statutes to fit the situation. Before courts should scrutinize an employee's use of employer computers under the CFAA, Congress needs to authorize such scrutiny by amending the statute to reach misuse.

### *B. Employer Recommendations*

Unless and until the Supreme Court construes the CFAA narrowly, employers should take precautions to ensure the means to pursue a cause of action against disloyal employees. The CFAA currently serves as a fail-safe in situations where no law covers the wrongful conduct at issue; however, this Note proposes the elimination of that backstop, at least until Congress has authorized it. In the meantime, employers are operating in an environment where interpretation of the CFAA is inconsistent and uncertain.[240] Employers should implement policies that will not only strengthen CFAA claims, but also ensure that other claims can be brought against a disloyal employee.

Employers should allow access to key company data only to those employees who need the information, access to which should be monitored.[241] Employers should also define what an employee is permitted to access within its computer system—and put it in writing. By password protecting sensitive files and not allowing employees to access them unnecessarily, employers can more easily establish a CFAA claim. For example, if an employee requires the password of another to access information and then emails it to himself, this situation presents a stronger CFAA claim than if the employee had general access to the employer's computer system.[242] Taking these simple additional steps will not only enhance the chances of a successful CFAA claim in the current legal environment, but will also ensure that an employer has alternative means of redress.

---

238. *Id.* at 193–94.

239. Fulginiti & McLean, *supra* note 233.

240. *See supra* Part II.

241. Robert B. Milligan & Carolyn E. Sieve, *Establishing CFAA Violations By Former Employees*, LAW 360 (Oct. 27, 2009), http://www.tradesecretslaw.com/uploads/file/Establishing%20CFAA%20Violations%20-%20Law%20360.pdf.

242. *Id.*

Additionally, employers should have written employment and confidentiality agreements in place with employees.[243] General guidelines in a policy manual prohibiting the personal use of employer information would also be wise.[244] A company will want to "spell out precisely the scope of an employee's permissible authorization to the company computers, particularly what they are not permitted to do, e.g., access the company computers to retrieve company data for a competitor."[245]

## IV. CONCLUSION

Computer use in the United States has substantially increased over the last 25 years and has become pervasive in nearly every facet of life.[246] Computers have allowed employees to perform their job functions much more efficiently, but they have also presented new challenges to employers, making it more difficult for them to safeguard their business data.[247] One challenging situation is when an employee absconds with proprietary information shortly before resigning to take a position with a competitor or go into business for herself. Traditional claims by an employer against this type of employee misconduct include breach of contract, trade secret misappropriation, unfair competition, or breach of fiduciary duty.[248] Recently, however, employers have become more creative and brought CFAA claims against disloyal employees, asserting that the insider accessed her protected computer "without authorization."[249] Bringing these claims under the CFAA is beneficial primarily because it opens a doorway into federal court and requires a lower burden of proof than traditional claims.[250] This Note confronts the issue of whether an employee's misappropriation of an employer's information in this manner violates the CFAA, which turns on whether the employee's access is "without authorization." In recent years, an employer confronting the disloyal employee has become the most common type of CFAA case.[251]

---

243. *Id.*

244. *Id.*

245. Nick Akerman, *Time to Review Corporate Computer Policies*, LAW TECHNOLOGY NEWS (Feb. 3, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202441909593.

246. *See supra* notes 1–4 and accompanying text.

247. *See supra* notes 5–6 and accompanying text.

248. *See supra* Part I.

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

250. *See* discussion *supra* Part II.

251. Kerr, *supra* note 13, at 1583.

District and circuit court opinions have split. Interestingly, the most recent district courts to confront the disloyal employee situation have construed the statute narrowly, but of the circuit courts that have addressed the question, all but one have construed "authorization" broadly.[252] The largely one-sided circuit court opinions are not representative of the district court opinions discussing this issue, and in most circuits yet to rule on the question, the district court decisions favor a narrow view.[253] Given Congress' reluctance to provide further clarity and the circuit split created by *Brekka,* the Supreme Court may well address this question in the coming years.[254]

Following recent district court opinions confronting the disloyal employee scenario,[255] this Note proposes that the Supreme Court adopt a narrow interpretation of "authorization," and hold that the term does not apply to employees who have permission to access an employer's computer. This interpretation not only comports with the intuitive meaning of the statute but also helps to define the boundaries of when courts will apply the CFAA—a largely impossible task under the broad view. A narrow reading of "authorization" will ensure employee liability does not hinge on the employee's interests towards an entity who has authorized his access at a given point in time and will prevent application of the statute in unforeseen ways. Courts should not interpret the CFAA to reach misuse of an employer's computer, at least not until Congress authorizes them to do so.

*Thomas E. Booms*[*]

252. *See* discussion *supra* Part II.

253. *Id.*

254. *See* discussion *supra* Part II.

255. *Id.*

* J.D. Candidate, Vanderbilt University Law School, 2012; B.S., Accounting & Finance, Miami University, 2007. The author would like to thank the editorial staff of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW for suggestions and assistance during the preparation of this Note as well as John Greiner for introducing me to the topic.