SMU Science and Technology Law Review

Volume 13 | Number 3 Article 5

January 2010

Definitional Vagueness in the CFAA: Will Cyberbullying Cause the Supreme Court to Intervene

Brandon Darden

Definitional Vagueness in the CFAA: Will Cyberbullying Cause the Supreme Court to Intervene?

Brandon Darden[1]

I. INTRODUCTION

Computers and the Internet play an essential part in almost every aspect of modern society; individuals use the internet for everything from checking their local news to paying their bills to chatting with a friend on a social networking site. Few, if any, stop to think if they just committed a crime by exceeding their computer's authorized access. Nevertheless, many users have the potential to be considered criminals by the government. Unfortunately, this surprising outcome often depends on what stance a court takes in analyzing the term "authorization." This variance results from the definitional vagueness in the federal computer crime statute, the Computer Fraud and Abuse Act (CFAA).

The majority of the CFAA's violations require either that the individual access a computer "without authorization" or by "exceeding authorized access."[2] The problem facing courts is that the CFAA does not define what constitutes "without authorization." Circuit courts are split about what the phrase "exceeding authorized access" actually means. In fact, three distinct approaches to understanding the term "authorization" in the CFAA have arisen across the country: an agency-based approach, a code-based approach and a contract-based approach.[3] Each of these approaches results in courts using a different application of the term.[4] At this point in the statute's history, it is clear that the words of the CFAA do not speak for themselves and we need some clarity.

This comment discusses the current state of the CFAA and the problems presented by the statute's definitional vagueness as exemplified by the recent federal district court decision of *United States v. Drew*. The holdings in *Drew* and another recent 9th Circuit decision, *LVRC Holdings, LLC. v. Brekka*, conflict with other federal court decisions and raise the real possibil-

---

1. Brandon T. Darden is a May 2011 candidate for Juris Doctor at Southern Methodist University Dedman School of Law. He graduated in 2008 from Southern Methodist University with a Bachelor of Arts in History and Medieval Studies. He would like to thank his father for his love and guidance, both in the law and in life.

2. Nick Akerman, Editorial, *Will the Justices Rule on the Computer Fraud and Abuse Act?*, NAT'L L.J., Sept. 23, 2009, at 1, *available at* http://www.dorsey.com/files/upload/akerman_computer_fraud_july09.pdf.

3. Katherine Mesenbring Field, *Agency, Code Or Contract: Determining Employee's Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 821 (2009).

4. *Id.* at 821–22.

ity that the Supreme Court may choose to rule on the definitional vagueness in the CFAA for the first time in the statute's history to provide some clarity for the future.[5] Part II of this comment will focus on the initial history of the CFAA and explain the origins of the *Drew* case within the context of the definitional confusion in the statute and the CFAA's potential misapplication in future cyberbullying cases. Part III will clarify the current state of the law, focusing on the three approaches taken by circuit courts and discussing several cases that provide examples of how courts use these different approaches and legislative history to justify their particular rulings. Finally, Part IV will analyze the rulings of *Drew* and *Brekka* and consider if these different approaches can continue to coexist with the three current approaches without the statute's interpretation remaining in disarray. *Lockheed Martin v. Speed* and *Shamrock Foods Co. v. Gast* will be discussed and their analysis offered as a potential solution to help clarify the confusion. The Supreme Court's intervention may be needed to clarify the definitional vagueness. Or a new series of laws should be promulgated to specifically address cyberbullying and actions that the CFAA fails to adequately cover.

II. History and Background

A. The Origins of the Computer Fraud and Abuse Act

Congress enacted the predecessor to the CFAA, codified as 18 U.S.C.A. § 1030, in 1984.[6] The original purpose of the CFAA was to fight the growing threat posed by computer hackers.[7] Until its enactment, prosecutors relied on mail- and wire-fraud statutes to attack the emerging problems of cyber crime.[8] These statutes were woefully inept at dealing with computers—something the legislators who passed them never intended for the statutes to address. The early statutes proved "incapable of combating computer crime that did not involve interstate commerce."[9] Originally, in an effort to address these concerns, Congress added certain provisions to the Comprehensive Crime Control Act of 1984 that focused specifically on the unauthorized access and use of computers and computer systems.[10] Early

5. Akerman, *supra* note 1.

6. Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse* Act (18 U.S.C.A. § 1030), 174 A.L.R. Fed. 101 at 1 (2001).

7. Field, *supra* note 2, at 820.

8. Buckman, *supra* note 5, at 14; *see also* U.S. Dep't of Justice: Computer Crime and Intellectual Prop. Section Criminal Div., Prosecuting Computer Crimes 1 (Feb. 2007) (quoting H.R. Rep. No. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692), *available at* http://www.cybercrime.gov/ccmanual/01ccma.pdf.

9. Buckman, *supra* note 5.

10. U.S. Dep't of Justice, *supra* note 7.

legislative history indicates that Congress wanted this new statute to give "'a clearer statement of proscribed activity' to 'the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access.'"[11] With passage of the 1984 Act, it became a felony to access classified information in a computer without proper authorization, whereas accessing financial or credit information from a financial institution or entering a government computer without authorization became misdemeanor.[12] Even though computer crime finally had its own statute under 18 U.S.C. § 1030, Congress continued to hold hearings to improve the crime bills, which eventually lead to the creation of the CFAA in 1986 by an amendment to Section 1030.[13]

The first version of the CFAA tried to strike the proper balance of addressing a new area of potential criminal activity while still not being so overbroad as to cause federalism concerns by infringing on the States' own rights to define criminal conduct.[14] The CFAA specifically covered instances when the crime was interstate, when harm was done to financial institution computers, or when the crime was perpetrated against the federal government's own computers.[15] Currently, all computer use is interstate, but at that time, the CFAA presented more "penalties for fraud and related activities in connection with access devices and computers."[16] The strict definition of what constitutes criminal conduct presented several loopholes. The loopholes exposed the statute's deficiencies—namely that it did not address harms occurring from anything other than unauthorized access.[17] The statute failed to address two large problems: people with authorization who still caused harm to protected computers and individuals without authorization who found authorized persons to do the criminal act for them.[18]

In response to mounting criticism from the Justice Department, Congress amended the CFAA in 1986 and made several substantial changes. The 1986 Act provided greater protection to computer systems, but it also showed that Congress still resisted political pressure to make the CFAA broad enough to cover all computer crimes.[19] Instead, the Act limited the CFAA to crimes involving a compelling federal interest.[20] While neither the original

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.* at 2.

15. Buckman, *supra* note 5, at 14.

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

version nor the 1986 amendment contained a provision for a private right of action, the 1986 version added the phrase "exceeds authorized access" to override the earlier version's phrasing: "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend."[21] This was an attempt to eliminate a confusing middle ground where an individual has legitimate access to computer data in particular circumstances.[22] But that same access instantly becomes criminal when they barely exceed their authorization, sometimes unbeknownst to the user.[23]

Originally, the CFAA was only a criminal statute, but with another amendment in 1994, civil violations made their appearance under § 1030(g).[24] This amendment allowed for anyone damaged by a violation of the CFAA to bring a civil suit against the perpetrator for equitable relief or damages as well as injunctive relief.[25] Earlier problems were also addressed by amending § 1030(a)(5), "to further protect computers and computers systems covered by the statute from damages both by outsiders, who gain access to a computer without authorization and by insiders, who intentionally damage a computer."[26] These changes were significant because the focus shifted from technicalities in the understanding of computer access to the individuals who violated the statute, their intent, and the subsequent harm caused by their actions.[27] Computer technology continues to expand at a rapid pace, placing a burden on Congress to monitor the CFAA continually so it remains up to date and assists the government in its goal of prosecuting cyber criminals in an effective and efficient manner.[28] As a result of these and further amendments in 1988, 1989, 1990, 1994, 1996, 2001, and 2002, the scope of the CFAA and the criminal conduct it covers has expanded significantly since its creation.[29]

21. Kyle W. Brenton, *Trade Secret Law and The Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 452 (2009) (citing S. REP. No. 99–432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.).

22. *Id.*

23. *Id.*

24. 18 U.S.C. § 1030(g) (1994) (current version at 18 U.S.C. § 1030(g) (2006)).

25. Buckman, *supra* note 5, at 14.

26. *Id.* at 113.

27. *Id.*

28. *Id.* at 114.

29. U.S. Dep't of Justice: Computer Crime and Intellectual Prop. Section Criminal Div., Prosecuting Computer Crimes 1 (Feb. 2007), *available at* http://www.cybercrime.gov/ccmanual/01ccma.pdf.

The current version of the CFAA criminalizes accessing a computer without authorization or access that exceeds the authorization given.[30] Additionally, a civil remedy is available for those who suffer damage or loss because of a violation of the CFAA.[31] The specific types of conduct addressed in the statute are: obtaining national security information, compromising the confidentiality of a computer, trespassing in a government computer, accessing a computer to defraud and obtain value, knowing transmission and intentional damage, intentional access and reckless damage, intentional access and damage, trafficking in passwords, and extortion involving threats to damage computer.[32] While attempts to commit these crimes are punishable under Section 1030(b), the CFAA purposefully excluded acts by law enforcement or intelligence agencies in Section 1030(f).[33]

"Unauthorized access" is not defined anywhere in the statute. But the CFAA does indicate that the term, "can take one of two different forms: one is to gain access to a computer system when the accesser has no authority to do so, and the other is to gain access to a computer system with authority but the accesser's use of such access exceeds his authority."[34] Section 1030(e)(6) defines "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[35] Congress may have seen the need to define the phrase "exceeds authorized access" because the individuals who exceed their access, "are likely to be insiders, whereas persons who act without authorization are likely to be outsiders."[36] Apparently Congress felt the statute addressed those without authorization—those who were never supposed to access the restricted information or trespass into the computer in the first place. Its focus shifted to the insiders who have some authorization but who will only face criminal sanctions if they "intend to cause damage, not for recklessly or negligently causing damage."[37] Outsiders without authorization are subject to a much broader range of criminal punishment and can be convicted under any of the access offenses in the CFAA, from Sections (a)(1) to (a)(5).[38] However, insiders—who have some sort of initial authority to begin with—are liable under more narrow circumstances and their crimes can only fall within Sec-

30. Akerman, *supra* note 1, at 1.

31. *Id.*

32. U.S. Dep't of Justice, *supra* note 28.

33. *Id.*

34. Jay Dratler, *Special Problems in Licensing: §11.04 Breach of License as Computer Fraud*, LICENSING INTELL. PROP. § 11.04 (2009).

35. 18 U.S.C. § 1030(e)(6) (2006).

36. U.S. Dep't of Justice, *supra* note 28.

37. *Id.*

38. *Id.* at 5.

tions (a)(1), (a)(2), and (a)(4).[39] Based on prior jurisprudence on the subject, courts are very fact-oriented when defining authorization.[40] Courts have seen numerous cases involving the CFAA over the statute's twenty-five-year history and have not only held the statute was (mostly) clear in its interpretation, but have continually analyzed the statute using the three distinct approaches listed above. This variation in courts' analyses has led to confusion on what conduct the statute covers, which approach is correct, or if all three play a very specific role in the statute's analysis. Ironically, it is the confusion in the statute and federal prosecutors' attempts to stretch the statute to cover all types of online behavior that may eventually lead to some clarity.

B. *United States v. Drew*: How a Teen's Suicide Raised the Authorization Question Within the Void-for-Vagueness Doctrine

Unfortunately, it took a young girl's tragic suicide, as opposed to a simple hacker invading restricted files, to bring the language of the CFAA before the courts once again. Lori Drew, an adult resident of O'Fallon, Missouri, allegedly created a conspiracy to access a computer and commit the tort of intentional infliction of emotional distress by "cyberbullying" a young girl on the social networking website MySpace.[41] After the girl committed suicide, the government indicted Drew on three felony counts of violating the CFAA's prohibition, found in 18 U.S.C § 1030, of accessing "a computer without authorization or in excess of authorization and obtaining information from a protected computer where the conduct involves an interstate or foreign communication and the offense is committed in furtherance of a crime of tortuous act."[42]

In response to the indictment, Drew brought a motion to dismiss based on "vagueness, failure to state an offense, and unconstitutional delegation of prosecutorial power."[43] In addition, she alleged that the indictment criminalizes a breach of contract involving computers.[44] The court found that the felony provisions of the CFAA's scienter requirement defeated Drew's initial challenges and allowed the indictment to go to trial.[45] At trial, the jury found Drew not guilty of the felony violations of the CFAA, but found her guilty, per the court-permitted instruction, of the lesser misdemeanor charges of the

39. *Id.*

40. *Id.* at 10.

41. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).

42. *Id.* at 452.

43. *Id.* at 451.

44. *Id.*

45. *Id.*

same CFAA provisions.[46] After her conviction on a misdemeanor violation, the case no longer turned on cyberbullying issues but focused entirely on the proper application of the CFAA—using one of the three approaches—to violations of a website's terms of service.[47] The initial question before the Court was whether a user's intentional breach of these terms of service, which the user agreed to, is sufficient to meet the first element of Section 1030.[48] After the trial, Drew filed a Rule. 29(c) motion challenging her convictions.[49] Before discussing how the court approached Drew's post-conviction motion, it is necessary to turn to the current state of the law and explain the three different forms of analysis that courts have used to interpret the meaning of the term "authorization" within the CFAA.

III. CURRENT LAW

Because Congress did not define the term "authorization" at any point during the statute's twenty-five-year history, courts across the country have struggled to apply the vague language of the statute. As a result, three different approaches to understanding what constitutes "authorization" have arisen: agency-based, code-based, and contract-based.[50] This comment will briefly discuss each in turn by highlighting significant cases that use each approach, while explaining the benefits and limitations that each present.

A. Agency-Based Approach

Much like the law of agency itself, the agency-based approach to analyzing "authorization" in the CFAA is predicated on the understanding that employees owe a fiduciary duty of loyalty to their employer, forcing them to act for their employer's benefit over their own personal gain.[51] The limitations of this approach are apparent: there must be a fiduciary duty of loyalty between the employee and employer. During an employment relationship, the employer authorizes the employee to act on his behalf, but this authority automatically ceases when the employee begins to act adversely to the em-

46. *Id.* at 453. The court instructed the jury that "if they unanimously decided that they were not convinced beyond a reasonable doubt as to the Defendant's guilt as to the felony CFAA violations of 18 U.S.C. §§ 1030 (a)(2)(C) and 1030(c)(2)(B)(ii), they could consider whether the Defendant was guilty" of the lesser misdemeanor violations of the same provisions.

47. *Id.* at 451 n.2.

48. *Id.* at 457.

49. *Id.* at 451; *see* FED. R. CRIM. P. 29(c).

50. Field, *supra* note 2, at 821.

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

ployer's interest.[52] Under the CFAA, an employee ends his authorization when he accesses a computer against his employer's interests.[53]

In the Senate Reports after the 1986 amendments, the drafters of the CFAA specifically wanted "to avoid the danger that every time an employee exceeds his authorized access to his department's computers . . . he could be prosecuted."[54] But there are clear limits to how far someone who has "authorization" will initially be allowed to go. In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage*, the court used the agency-based approach in deciding that a former employee of Shurgard acted as an agent for Safeguard by sending emails to himself containing confidential materials while still employed by Shurgard and with full access to Shurgard's confidential business plans and trade secrets.[55] The court ruled that Shurgard stated a valid claim under Section 1030(a)(2)(C) because the employees "lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via email."[56] Since the employees' authorization ended the moment they began to act contrary to their principle's interest, the court found it unnecessary to consider whether they ever exceeded their authorized access.[57] This holding implies—and is supported by the Eleventh Circuit's decision in *United States v. Salum*—that the term "without authorization" depends on the defendant's state of mind.[58] In *Salum*, a jury convicted a police officer of computer fraud for releasing personnel records of individuals in his department.[59] The court concluded that "although Salum may have had authority to access the . . . database, there was sufficient evidence to establish that . . . Salum [knew he had] exceeded his authority by accessing it for an improper purpose."[60]

The leading case in the agency-based approach is the Seventh Circuit's 2006 decision, *International Airport Centers, LLC v. Citrin*. The defendant, Citrin, was an employee of International Airport Centers' (IAC) real estate division, when he breached his employment contract and went into business on his own.[61] Before he left, he returned his company-owned laptop but

52. Buckman, *supra* note 5, at 3.

53. *Id.*

54. *Shurgard*, 119 F. Supp. 2d at 1128 (citing S. REP. NO. 99–432, at 7-8 (1986)).

55. *See id.* at 1123 (plaintiffs alleged that Safeguard "hired away other [former] employees . . . who [had] intimate knowledge" of company secrets and continued to actively recruit them from Shurgard).

56. *Id.* at 1125.

57. *Id.* at 1125 n.4.

58. Akerman, *supra* note 1; *accord* United States v. Salum, 257 F. App'x 225, 230-31(11th Cir. 2007).

59. *Salum*, 257 F. App'x at 225.

60. *Id.* at 230.

61. Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

destroyed all of its data using a program that ensured permanent deletion, including data that revealed some improper behavior he engaged in while an employee.[62] IAC filed suit under Section 1030(a)(5)(A)(i) of the CFAA, and the court ruled that Citrin's "authorization to access the laptop terminated when, having already engaged in misconduct . . . he resolved to destroy files that incriminated himself . . . in violation of the duty of loyalty that agency law imposes on an employee."[63] The court explained that "the difference between 'without authorization' and 'exceeding authorized access' is paper thin," but regardless, Citrin ended his employment with IAC and with that, he terminated his authorization to access the computer.[64] He breached his duty of loyalty because "the only basis of his authority had been that relationship."[65] The use of agency law, and more specifically, the focus on the duty of loyalty inherent to it, has resulted in employers favoring this approach because employee liability will likely arise so long as the employer characterizes an employee's actions as contrary to its own interests.[66]

Recently, the agency approach has come under attack, suggesting that the only way to resolve the conflict between the circuits is an intervention by the Supreme Court. Late in 2009, the Ninth Circuit handed down its decision in *LVRC Holdings LLC v. Brekka*, and the court specifically pointed out that it was "unpersuaded by [*Citrin's* agency-based] interpretation."[67] LVRC hired Brekka, though the court notes there was no written employment agreement, and part of Brekka's duties included using a company computer to conduct internet marketing programs.[68] While working for the company, Brekka regularly commuted between LVRC's office in Nevada and his home in Florida, and he often emailed work-related documents to his home computer.[69] He used his own administrative user name, "cbrekka," which LVRC gave him to gather usage statistics about LVRC's website so that he could use the statistics in the company's internet marketing.[70] Right before Brekka left LVRC's employment, he sent a master report containing sensitive com-

62. *Id.*

63. *Id.*; *see also* 18 U.S.C. § 1030 (a)(5)(A), *stating* "whoever knowingly causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." A "protected computer" is a defined term that includes Citrin's laptop. *Citrin*, 440 F.3d at 418.

64. *Citrin*, 440 F.3d at 420–21.

65. *Id.*

66. Field, *supra* note 2, at 824.

67. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009).

68. *Id.* at 1129.

69. *Id.*

70. *Id.*

pany information to his and his wife's personal email accounts.[71] After Brekka left the company, an employee noticed that "cbrekka" logged into the system and accessed the company statistics.[72] LVRC brought suit under Section 1030(g) alleging a private right of action for Brekka's violation of two of the CFAA's criminal provisions, Section 1030(a)(2) and Section 1030(a)(4).[73]

Instead of using case law, the court defined "authorization" by the Random House Dictionary's definition as "permission or power granted by authority" because the "CFAA does not define 'authorization,' and . . . unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning."[74] Using this definition, the court dismissed LVRC's argument that Brekka acted "without authorization" since LVRC, as his employer, gave him authorization to access their computer files when they gave him permission, by issuing him a password, to use it.[75] In contrast to the holdings in *Citrin* and *Salum*, the *Brekka* court believed that nothing in the CFAA implies that an employee loses authorization when he uses his computer to violate a duty of loyalty to his employer.[76] Instead, Congress' inclusion of Section 1030(e)(6), which defines "exceeds authorized access," implies that Congress never intended to limit the meaning of the phrase in that way.[77] A person who exceeds his or her authorized access is someone who has the necessary initial authorization to access a computer for a particular reason, but surpasses this reason. In contrast, a person who accesses a computer without authorization does not have the initial right or permission to access the computer.[78] LVRC gave Brekka permission to use a computer and access its secure materials when they hired him, and therefore he "re-

71. *Id.* at 1129–30.

72. *Id.* at 1130. The master report contained a list of the names of patients at LVRC's Fountain Ridge Facility, a rehabilitation facility in Nevada.

73. *Id.* at 1131-32. A claim under § 1030(g) for a violation of § 1030(a)(2) requires a showing that the defendant "(1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer, and that (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value." Whereas a claim under § 1030(g) for a violation of § 1030(a)(4) requires that the defendant: "(1) accessed a protected computer, (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value,' causing (5) a loss to one or more persons during any one year period aggregating at least $5,000 in value."

74. *Id.* at 1132–33.

75. *Id.* at 1133.

76. *Id.*

77. *Id.*

78. *Id.*

main[ed] authorized to use the computer even if . . . [he] violate[ed] those limitations."[79] This approach shifts the court's focus away from the law of agency and toward the employee's mental state changing "from loyal employee to disloyal competitor" and the actions of the employer, such as granting access or terminating the employee.[80] Without his employer notifying him that his previous authorization was no longer allowed and thereby opening the door for him to "exceed [his] authorized access," Brekka "would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation . . . ."[81] Specifically, the holding limits the term "without authorization" to a person who does not have permission to use the computer for any reason, such as a hacker, or "when the employer has rescinded permission to access the computer and the defendant uses the computer anyway."[82] Despite the differences in the *Brekka* and *Citrin* decisions, the agency-based approach still has become the favorite for employers to use against disloyal employees.[83] The code-based approach presents a more challenging situation since the employee usually possesses the requisite authorization to access the computer initially.[84]

B. Code-Based Approach

The second interpretation of "authorization" is more limited because it centers on an understanding of computers and their systems, and it seems to require that the violator possess advanced knowledge to sidestep "code-based protections designed to limit his use of the computer system."[85] Since the user needs to manipulate the computer into providing more access than he was originally given, authorization cannot be challenged under the code-based analysis in situations where individuals have been already been granted access.[86] Since its application in *United States v. Morris*, this approach appears to fit within the CFAA's original goal of targeting outside hackers from accessing computers they never had authorization to use.[87] Unlike the agency-based approach, which is very employer friendly, the code-based approach presents more problems for employers, as employees usually

79. *Id.*

80. *Id.* at 1134.

81. *Id.* at 1135.

82. *Id.*

83. Field, *supra* note 2, at 824.

84. *Id.* at 827.

85. *Id.* at 825.

86. *Id.*

87. *See* United States v. Morris, 928 F.2d 504, 507-08 (2d Cir. 1991).

have authorization, and the employees' subjective state of mind is not considered.[88]

The code-based interpretation was one of the earlier forms of analysis and is best exemplified in the Second Circuit's 1991 decision, *United States v. Morris*.[89] Morris, a graduate student at Cornell's computer science Ph.D. program, had access to an account and permission to use the computers at Cornell.[90] In an attempt to show the deficiencies of computer security, Morris created a worm to prove the system's defects.[91] However, he underestimated its programming and the worm eventually spread across the country, crashing university, military, and research computers. A jury found him guilty of violating Section 1030(a)(5)(A), which provides for criminal punishment for anyone who "intentionally accesses a federal-interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information."[92] Morris appealed, arguing that his actions were not without authorization because he was authorized originally to use the federal-interest computers at Cornell, but he exceeded his authorization by planting the worm.[93] The court disagreed with his interpretation, saying the legislative history of the CFAA (an earlier version) intended Section 1030(a)(5)(A) to focus on individuals—like hackers—lacking the authorization to access any federal interest computer, outsiders, or "interdepartmental" offender trespassers.[94] Congress did not want to narrow the statute's effectiveness when individuals within the government could technically commit the same crimes.[95] Individuals with prior access must also be subject to liability for gaining unauthorized access to other computers of federal interest, which Morris did when his worm infected military, research, and other university computers.[96] His conduct was unauthorized because he did not use the computer for its intended purpose. Instead, "he found holes in both the programs that permitted him a special and unauthorized access route into other computers."[97] The code-based approach is especially effec-

88. Field, *supra* note 2, at 826.

89. *Morris*, 928 F.2d at 507-08.

90. *Id.* at 505-06.

91. *Id.* at 506.

92. *Id.*; 18 U.S.C. § 1030(a)(5)(A) (1988), *amended by* § 1030(a)(5)(A) (1999). The current version of § 1030(a)(5)(A) reads: "whoever knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cases damage without authorization, to a protected computer."

93. *Morris*, 928 F.2d at 509.

94. *Id.* at 510.

95. *See id.*

96. *Id.*

97. *Id.*

tive when prosecuting hackers, but it did not play as large a role in the CFAA's definitional vagueness debate in *United States v. Drew* as did the agency or contract-based approaches, both of which focus more on the user's relationship with the one who gives the access than any knowledge of computers.[98]

C. Contract-Based Approach

The third and final form of analysis for authorization, which the court in *Drew* used, is the contract-based approach, but this too has limitations. For a breach of contract claim to arise, a court must be able to find an explicit or implied contract that defines the user's authorization and that the user breached that contract, thereby making his actions unauthorized or in excess of his original authorization.[99] The usefulness of this approach is shown in situations where there is an express contract, such as between an employer and an employee, or like in *Drew*, where there are clear website terms of service agreements outlining what is and is not authorized.[100]

In 1997, the First Circuit used the contract-based approach in deciding the case of *United States v. Czubinski*.[101] Czubinski, a contact representative for the IRS's Taxpayer Services Decision, regularly accessed information from the IRS's computer database in the course of his job, which included looking at individuals' private income tax return information.[102] Czubinski knew the IRS's policy because he signed the IRS Rules of Conduct, which stated that employees, like Czubinski, who had passwords and access codes, were not allowed to access files outside the course of their official duties.[103] He knowingly disregarded these rules and performed unauthorized searches to observe confidential tax information, apparently with the intent to compile dossiers on members of the Ku Klux Klan.[104] But the government conceded he did not do "anything more than knowingly disregard IRS rules by observing the confidential information he accessed" because he never used the information.[105] At trial, a jury convicted Czubinski of violating the felony provisions of 18 U.S.C. § 1030(a)(4), which required that he access the computer, either without authorization or in excess of authorization, and obtain something of value.[106] The court agreed that Czubinski exceeded his author-

98. *See generally* United States v. Drew, 259 F.R.D. 449, 459-62 (C.D. Cal. 2009).

99. Field, *supra* note 2, at 827.

100. *Id.*

101. *See* United States v. Czubinski, 106 F.3d 1069, 1078-79 (1st Cir. 1997).

102. *Id.* at 1071.

103. *Id.*

104. *Id.* at 1072.

105. *Id.*

106. *Id.* at 1078.

ized access, which the IRS Rules clearly outlined, but Section 1030(a)(4) "emphasizes that more than mere unauthorized use is required: the 'thing obtained' may not merely be the unauthorized use."[107] In reversing his conviction, the court held that legislative history supported this additional "value" requirement, and Czubinski did not deprive the IRS of any property of value when he merely exceeded his authorized access in viewing files outside of his official duties.[108] While the court dismissed his convictions, the holding nonetheless supports the premise that individuals are able to "contractually define the limits of authority," and courts can use these contracts to determine if an individual exceeded his authorized access.[109] Perhaps most importantly for the *Czubinski* decision, the First Circuit Court concluded its discussion with a warning on the vagueness of the CFAA's words and the inherent danger it presents because "[Czubinski's conduct,] albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected to form the basis of a federal felony."[110]

Judge Wu reiterated this vagueness warning twelve years later in *United States v. Drew*. Around September 20, 2006, Drew and her co-conspirators created a fake MySpace profile and posted a picture of a fictitious sixteen-year-old boy named "Josh Evans," in violation of MySpace's online terms of service.[111] Soon after, Drew contacted and flirted with Megan Meier—the victim of Drew's harassment and a thirteen-year-old classmate of Drew's daughter.[112] "Josh" continued his flirtatious behavior until October 7, at which time, "Josh" informed Meier he was moving.[113] On October 16, Drew, posing as Josh, told Meier that "he no longer liked her and that 'the world would be a better place without her."[114] Later in the day, Meier committed suicide, and Drew quickly deleted the "Josh Evans" account.[115]

---

107. *Id.*

108. *Id.* at 1078–79, (citing S. REP. No. 432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488). "The Committee remains convinced that there must be a clear distinction between computer theft, punishable as a felony . . . and computer trespass, punishable in the first instance as a misdemeanor."

109. Field, *supra* note 2, at 828.

110. *Czubinski*, 106 F.3d at 1079.

111. United States v. Drew, 259 F.R.D. 449, 452–54 (C.D. Cal. 2009). The applicable terms of service include a representation that all registration information is accurate and true, the user will maintain the accuracy of their account, the user is over fourteen years old and that the use of MySpace's services "does not violate any applicable law or regulation." The MSTOS also prohibits a wide range of offensive or harmful content.

112. *Id.*

113. *Id.*

114. *Id.*

115. *Id.*

To become a member of MySpace at the time Drew created the fake profile, a member had to meet a minimum age of fourteen and agree to the MySpace Terms of Service (MSTOS).[116] MySpace uses two types of agreements for its terms of service. Simply by visiting the site and obtaining information, a "browsewrap" agreement binds the visitor to the terms of service.[117] Conversely, if a user chooses to become a member of MySpace, they must proactively check the box and agree to a "clickwrap" agreement, thereby affirming their awareness of the terms of service, before they can proceed.[118] The MSTOS, which prohibited such conduct as harassment, providing false information and posting photographs without the subject's consent, were not on MySpace's registration page, so an individual could become a member without ever viewing the terms by simply clicking the "check box," and then clicking the "Sign Up" button.[119] To access these terms, a potential member needed to click on the hyperlink marked, "Terms," which appeared further down the page.[120] Part of the terms of service explained that MySpace could unilaterally modify the agreement without notifying its members; therefore, a member must review the MSTOS every time they entered the website to "ensure that they were aware of any updates in order to avoid violating some new provision of the terms of service."[121]

To show that Drew's crime fit within the CFAA's requirements, the government argued that Section 1030(a)(2)(c) possesses a scienter requirement: the intentional accessing of the computer without authorization or in excess of the viewer's authorization.[122] The government believed this scienter requirement eliminates any arguments concerning the statute's vague definitions or lack of guidelines.[123] It claimed the scienter requirement was met by Drew's conscious violation of her agreement with MySpace when she violated the MSTOS by creating a fake account, although it had to concede that the sole foundation of her violation of the statute was the intentional creation of the "Josh Evans" profile.[124]

At the beginning of the opinion, the court noted that "nothing in the legislative history of the CFAA" suggests that Congress envisioned a cyberbullying prosecution under the statute.[125] The relevant criminal ele-

116. *Id.* at 453–54.

117. *Id.* at 462 n.22.

118. *Id.*

119. *Id.* at 453.

120. *Id.*

121. *Id.* at 454.

122. *Id.* at 467.

123. *Id.*

124. *Id.* at 461.

125. *Id.* at 451 n.2.

ments of Section 1030(a)(2)(C) are: (1) the defendant intentionally accessed a computer, either without authorization or in excess of their authorization; (2) the defendant's accessing of the computer involved a foreign or interstate communication; and (3) by accessing the computer, the defendant obtained information used in foreign or interstate commerce or communication.[126] When a computer contacts and communicates with a website on the internet, the user immediately satisfies the second and third elements because "a computer providing a 'web-based' application accessible through the internet [satisfies] the [second] 'interstate communication' requirement" and "the internet is an instrumentality and channel of interstate commerce."[127]

The court noted that three important terms are not defined sufficiently within the first element: "intentionally," "access a computer," and "without authorization."[128] The court chose to examine "without authorization" in the breach of contract context where "most courts . . . have held that a conscious violation of a website's terms of service/use will render the access unauthorized."[129] Based on this interpretation, the court held "that an intentional breach of the MSTOS can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statue" satisfying the first element of Section 1030(a)(2)(C).[130] *Drew*'s ruling is consistent with other cases, such as *EF Cultural Travel BV v. Zefer Corp.*, which held that "a lack of authorization could be established by an explicit statement on the website restricting access."[131]

Once the Court established that Drew's conscious violation of the MSTOS constituted a violation under the CFAA, the next question was whether Section 1030 withstands the void-for-vagueness doctrine.[132] Judge Wu focused specifically on whether the statute places an ordinary person on

126. *Id.* at 456-57 nn.11–12; *see also* 18 U.S.C. § 1030(a)(2)(C). In 2008, an amendment modified the CFAA to remove the "interstate or foreign communication" wording.

127. *Drew*, 259 F.R.D. at 457–58.

128. *Id.* at 458.

129. *Id.* at 460.

130. *Id.* at 461.

131. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003). In *Zefer*, a start-up travel agency, Explorica, hired Zefer Corp. to build a computer device that could take prices from its competitor's website and place them into an Excel spreadsheet, allowing Explorica to undercut the prices. The issue before the court was whether this "scraper" device constituted "exceeded authorized access," since the public had access to the website and anyone could take the time to gather the prices themselves. The court noted the competitor's website did not contain an explicit ban on "scraper" programs, but if it did, the ban notice would constitute "an explicit statement on the website restricting access."

132. *Drew*, 259 F.R.D. at 462.

notice.[133] Criminal statutes such as the CFAA must give a "fair warning."[134] One manifestation of this requirement is the void-for-vagueness doctrine, which prohibits enforcing a statute containing terms so vague "that men of common intelligence must necessarily guess at its meaning and differ as to its application."[135] It requires reasonable clarity in a statute's wording or interpretation to notify the defendant that their conduct was criminal.[136] The void-for-vagueness doctrine has two requirements: (1) the offense must have "relatively clear guidelines" so an ordinary person can understand what conduct is illegal; and (2) the law must give some minimal "objective criteria" to assist law enforcement agencies in its application.[137] The Court concluded that basing a violation of Section 1030(a)(2)(C) on the conscious violation of a website's terms of service fails both requirements, especially its complete lack of guidelines for law enforcement.[138]

The Court used five arguments to conclude that the CFAA neither implicitly suggests nor explicitly states that breaches of contract are criminalized.[139] First, ordinary people, while reasonably foreseeing civil penalties, would not expect criminal punishment for contract breaches.[140] Second, Section 1030 does not explain which violations, if any, constitute unauthorized access.[141] If the terms of service—like MySpace's—do not explain what constitutes a violation, then "*any* violation of *any* term" could make the access unauthorized, thereby eliminating a need to provide guidelines for law enforcement since every violation is criminal.[142] Third, criminalizing breaches of a website's terms of service places the website's owner in the position of the "lawmaker" by allowing them to define what conduct is illegal. Website agreements that allow for unilateral modification by the owner mean that conduct can be criminalized without any notice to the user.[143] Fourth, the MSTOS included an arbitration clause, raising a question as to whether any findings of unauthorized access can occur without the website

133. *Id.* at 464.

134. *Id.* at 462.

135. *Id.* at 463 (quoting Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926)). Additionally, the principles of strict construction towards criminal statutes and due process prevent a new interpretation of statute to cover conduct the statute or a court has not revealed to the public.

136. *Drew*, 259 F.R.D. at 463.

137. *Id.* at 462-63.

138. *Id.* at 464.

139. *Id.*

140. *Id.*

141. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

142. *Drew*, 259 F.R.D. at 464-65.

143. *Id.* at 465.

first bringing the accused party to arbitration.[144] Finally, under California law, material breaches of contract did not release MySpace from performance instantly.[145] Instead, it "excuses the injured party's performance, and gives him or her the election of certain remedies."[146]

In addition to failing the actual notice requirement, Section 1030 fails to provide minimal guidelines for law enforcement and allows a violation of a website's terms of service to establish a violation of the CFAA.[147] This "results in transforming Section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent internet users into misdemeanant criminals."[148] Finally, the court addressed the government's argument that Section 1030(a)(2)(C) possesses a scienter requirement and therefore overcomes the void-for-vagueness challenge.[149] In dismissing the argument rather quickly, the court noted that the only scienter requirement is that the unauthorized access is "intentional," and as detailed earlier, "intentional" is subject to different interpretations.[150] If the court were to accept the government's position, the statute would criminalize every breach of contract regardless of the severity, making the law overbroad once again since it fails to provide "criteria as to which of the breaches should merit criminal prosecution."[151]

IV. ANALYSIS

A. A Cry for Help!

Sadly, Megan Meier is not the only young teenager to fall victim to online harassment. Phoebe Prince, a 15-year-old girl in South Hadley, Massachusetts, committed suicide on January 14, 2010 due to cyberbullying through "text messages, the computer, and on Facebook and other social networking sites."[152] The taunting and abuse continued even after her death, and certain messages had to be removed from her Facebook memorial page.[153] Facebook representatives immediately responded to the claims stating that, "most reports are 'acted on' within 24 hours and the site's policies

144. *Id.*

145. *Id.* at 465-66.

146. *Id.*

147. *Id.* at 466.

148. *Id.*

149. *Id.* at 467.

150. *Id.*

151. *Id.*

152. *Mass. High School Girl Takes Life After Allegedly Taunted by Cyber Bullies*, Jan. 26, 2010, http://www.foxnews.com/story/0,2933,583948,00.html?test=latestnews (last visited January 29, 2010).

153. *Id.*

spell out that users can't harass, bully, or threaten anyone. Depending on the situation, we would certainly disable the accounts of people that were engaging in that kind of behavior."[154] Disabling the accounts of these cyberbullies may be an option for Facebook, but can federal prosecutors use the CFAA to send these bullies to jail? The bullies had access to use and interact with the networking site by joining, so the code-based approach fails.[155] And there was no duty of loyalty between Facebook and the victims of cyberbullying, since the injured parties were not employees.[156] Furthermore, abusive posting can hardly be considered contrary to Facebook's interest in a strict sense of agency law.[157] A contract-based approach seems destined to run into the same problems as under the *Drew* conviction, as bullies do not foresee a criminal prosecution coming from violating Facebook's terms of service. Has a loophole emerged within the vagueness of the CFAA that forces federal prosecutors to search elsewhere for a statute or law that can effectively punish these bullies' conduct?

In *Morris*, the Second Circuit agreed with the district court's decision not to define the term "authorization" for the jury since "the word is of common usage, without any technical or ambiguous meaning," and the CFAA statute was clear and unambiguous.[158] As later case law proves, nothing could be further from the truth. Not only has the term "authorization" been muddled and debated over in terms of what constitutes "exceeding authorized access" or access "without authorization," but Part III explained that three distinct lines of analysis have arisen to tackle this "word of common usage." In the search for clarity, courts turn to the legislative history of the statute only to realize that support exists for whichever interpretation is preferred.[159]

B. The Impact of *Drew* and *Brekka*

While the *Drew* case will forever be marred with the tragic death of a young girl, the court correctly ignored emotions by focusing on the real issue: violations of the MSTOS. The court correctly granted Drew's motion for acquittal because of the vagueness inherent in the CFAA.[160] Typically, prosecutors use Section 1030 to indict hackers, though Congress never intend to apply it criminally against individuals who breached a website's terms of

154. Jessica Heslam, *Safety "Key" on Facebook, Rep Says*, BOSTON HERALD, Jan. 26, 2010, *available at* http://www.bostonherald.com/news/regional/view.bg?articleid=1228265 (last visited January 29, 2010).

155. *See id.*

156. *See id.*

157. *See id.*

158. United States v. Morris, 928 F.2d 504, 507–11 (2nd Cir. 1991).

159. Field, *supra* note 2, at 829–30.

160. *See* United States v. Drew, 259 F.R.D. 449, 468 (C.D. Cal. 2009).

service.[161] While possessing grave consequences, Drew's conduct in creating the "Josh Evans" profile was not criminal under the CFAA at the time, and if it was, Section 1030 still failed to provide her with sufficient notice.[162] It is important to remember that this case originated in the context of cyberbullying, an issue of first impression at the time, and it is apparent the government attempted to twist the CFAA to cover criminal conduct it was never supposed to address. Much like the early wire fraud statutes that were marked by an ineptitude at punishing hackers and gave rise to the CFAA, a new statute—or intervention by the Supreme Court—may be needed to ensure that these types of crimes are prosecuted. The decision of the *Drew* court provides a fair warning to the government to define what constitutes criminal conduct before overreaching with its indictments, despite the public's outcry for justice. Overall, "the decision is a setback for the federal government's efforts to criminally prosecute violations of end-user license agreements concerning Web sites and software."[163]

Drew's holding "overlooks the well-established fact that a breach of contract can, in certain instances, constitute a crime."[164] Just like a "No Trespass" sign has the ability to form the basis for a criminal trespass suit in some jurisdictions, website owners can argue that they should be able to dictate "explicitly what is forbidden" on their own pages.[165] Had the court held that Drew's conscious violation of the terms of service was enough to meet the requirements within Section 1030, internet users would live in perpetual fear of breaking the law, since a website owner would control the definition of criminal conduct, no matter how reasonable or unreasonable the terms.[166] The court's approach explained that the lack of actual notice centered on what "ordinary people" would expect.[167] While a user could expect to be banned from the website for violating an online version of a "No Trespass" order, hardly anyone expects criminal penalties for violation of a website's terms of service—especially when the violation is "harmless," as in not for profit or not in an attempt to defraud.[168] In 2006, MySpace's terms of service read as an extensive "do not" list, prohibiting a myriad of conduct such as "gambling," "advertising to any member," "disclosing your password," and

161. *See generally TOS Violation Can't Justify Woman's Prosecution Under CFAA*, Sept. 16, 2009, *available at* 27 ANDREWS COMP. & INTERNET LITIG. REP. 6., at 1.

162. *See generally Drew*, 259 F.R.D. at 449–68.

163. *TOS Violation Can't Justify Woman's Prosecution Under* CFAA, *supra* note 160, at 1.

164. Akerman, *supra* note 1, at 2.

165. *Id.*

166. *Drew*, 259 F.R.D. at 464–66.

167. *Id.* at 464.

168. *See id.*

curious statements prohibiting "content intended to draw traffic to the profile."[169] While effective in protecting MySpace from liability, these vague and often cryptic restrictions would become the virtual Ten Commandments of the Internet, making criminal punishment subject to change at mighty MySpace's whim.

The *Drew* Court's analysis concerning the statute's lack of minimal guidelines focused on how the government clearly targeted Drew because of the consequences of her conduct and the shock it caused the public. Based on the government's position, innumerable individuals, many no one would ever accuse of being "criminals," have criminally violated the CFAA, including Megan Meier, who lied about her age to join MySpace.[170] "[T]he Constitution does not permit a legislature to 'set a net large enough to catch all possible offenders, and leave it to the courts'" to determine who is *really* guilty of being a criminal and who was merely playing around on the internet.[171] Realistically, the legislature did not intend for its "net" to cover these "criminals."

The court dismissed the government's argument that the CFAA already possesses a scienter requirement, met by the conscious violation of the terms of service, because the statute does not explain to law enforcement whether every intentional breach, like a user lying about their age, is sufficient to constitute "intent to access the site without authorization."[172] The statute lacked any distinction about the weight of different "criminal" violations, which made posting pictures of others without their permission equal to child pornography.[173] The MSTOS did not specify which specific actions terminated the visitor's access, resulting in its application under the CFAA as being too vague. However, picking and choosing what constitutes criminal behavior would leave the legislature's constitutional job to a website owner's discretion. Conversely, specifying that all the conduct listed in the terms is criminal conduct would result in a "standardless sweep" and could give law enforcement officers the ability to "pursue their personal predilections."[174] While the standard created by the court would survive a vagueness challenge without a court finding the statute excessive and overbroad, the decision leaves a very narrow range of what constitutes actual notice of permissible authorization for law enforcement purposes.[175]

169. *See id.* at 464-65.

170. *See id.* at 466.

171. *See* City of Chi. v. Morales, 527 U.S. 41, 60 (1999).

172. *See Drew*, 259 F.R.D. at 467–68.

173. *See id.* at 467.

174. *See id.*; *see also* Kolender v. Lawson, 461 U.S. 352, 357–58 (1983).

175. *See Drew*, 259 F.R.D. at 464–68.

C. Can We Keep It Simple, Please?

In his opinion in *United States v. Mitra*, Judge Easterbrook explains why the defendant's argument fails to persuade the Seventh Circuit of his innocence:

> Mitra's problem is not that § 1030 has been turned in a direction that would have surprised reasonable people; it is that a broad statute has been applied *exactly as written*, while he wishes it had not been. There is no constitutional obstacle to enforcing broad but clear statutes. The statute itself gives all the notice that the Constitution requires.[176]

If Judge Easterbrook is right, and the CFAA is clear enough to place defendants on reasonable notice as to what constitutes criminal conduct, where have all the other courts gone wrong? The answer may be staring us all in the face: we have made it too complicated. The U.S. District Court for the Middle District of Florida took this approach in 2006 in *Lockheed Martin Corp. v. Speed*.[177] Lockheed sued its rival, L-3, and three former employees who left Lockheed for L-3, for conspiring together to "wrongfully obtain ATARS trade secrets" in an attempt to give L-3 an unfair advantage in bidding on the government contract for the new ATARS II.[178] The employees included a program manager who "had complete access to ATARS confidential and proprietary and trade secret protected information," a senior manager who "had unrestricted access to [Lockheed's] shared network drives," and a site manager who "had access to confidential and proprietary and trade secret protected financial, technical and strategic data.[179] Early in its discussion, the court noted that it is not influenced by the decisions of *Citrin* and *Shurgard* or the agency-theory rationale, which relied too strongly on extrinsic material, because the plain language of the statute sufficed.[180]

Using the plain language of the statute and what the court considered the clear meaning of "authorization," the court explained that Congress singled out two groups of "accessers, those 'without authorization' (. . . meaning those having no permission to access whatsoever . . .) and those

176. United States v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005). The jury convicted Mitra on two counts of "intentional interference with computer-related systems used in interstate commerce" under § 1030(a)(5) for interfering with Madison, Wisconsin's computer based emergency radio system. *Id.* at 493.

177. *See generally* Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *18–19 (M.D. Fla. Aug. 1, 2006).

178. *Id.* at *2–3. Lockheed beat out L-3 for the USAF contract for the original Aircrew Training and Rehearsal Support ("ATARS I") in 2000. The ATARS II contract, which both companies planned to bid on in 2006, was valued at over 1 billion dollars. *Id.*

179. *Id.* at *2–4.

180. *Id.* at *12.

exceeding authorization (. . . meaning those that go beyond the permitted access granted to them . . .)."[181] Lockheed's former employees fit within a very narrow category of those who access with legitimate authorization, regardless of the employee's intent—which Congress specifically chose not to target in the CFAA.[182] Lockheed gave the employees access to company computers, so they were not without original authorization, and gave them access to the particular files in question, so they did not exceed their authorized access.[183] Lockheed's complaint does not concern the employees' level of authorization. Its argument centers on the employees' bad behavior *after* they used their authorization to access the information—something that the CFAA does not cover.[184] Finally, the court noted that the claim also failed because the CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information."[185] Using this definition, the access did not cause any damage since they simply took the data rather than impairing it.[186] Without any damages and without someone who exceeded their authorization, the court granted the employees' motion to dismiss.[187] The *Lockheed* court did not need to use an agency-based, a code-based, or a contract-based approach, but the court seems to have provided some answers to the definitional vagueness within the CFAA. *Lockheed* is not alone in this trend.

In 2008, the U.S. District Court for Arizona decided *Shamrock Foods Co. v. Gast* using a similar approach to the one used in the opinion in *Lockheed*.[188] Gast, a Shamrock Foods Company employee, signed a Confidentiality Agreement that prevented him from disclosing the company's trade secrets.[189] After being promoted to Regional Sales Manager for Southern Arizona, Gast began negotiating with a competitor of Shamrock, Sysco Food Services, about switching employment.[190] Over a week before he resigned from Shamrock, Gast emailed several documents containing confidential information to his personal account.[191] After performing a forensic analysis on his work computer, Shamrock learned of the action and sued under the

181. *Id.* at *14–15.

182. *Id.* at *15, *21.

183. *Id.* at *15.

184. *Id.*; *see* 18 U.S.C. § 1030(a)(4) (2008).

185. *Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *27–28; *see* 18 U.S.C. § 1030(e)(8) (2008).

186. *Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *27–28

187. *Id.* at *28.

188. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 962–63 (D. Ariz. 2008).

189. *Id.* at 963

190. *Id.*

191. *Id.*

CFAA, alleging that Sysco now possessed and used the confidential information against them.[192]

The court began by explaining that this dispute exemplified the discussion over the meaning of "authorization," and acknowledged that Shamrock wanted to use the agency-based approach to hold Gast liable for accessing confidential information after acquiring a conflict of interest.[193] Despite stating that the plain meaning of "without authorization" eliminates any need to use extrinsic materials, like those relied upon in the *Citrin* decision, the court noted that other courts and the legislative history support a narrower reading of the word.[194] Senate reports on the CFAA differentiate between "without authorization" and "exceeding authorized access" by distinguishing between system insiders and outsiders: "[i]nsiders are those with rights to access computers in some circumstances . . . , whereas outsiders had no right to access computers at all (such as hackers)."[195] Simply put, accessing "without authorization" occurs where the initial access is not allowed, while "exceeding authorized access" occurs where the initial access is allowed, but entry to certain information is not.[196] Disavowing the three approaches, and using this simplified interpretation, the court concluded that Gast possessed both the requisite initial authorization to use the Shamrock system and the specific permission to see the files. Therefore, Gast did not access the files without authorization or in excess of his authorization, and Shamrock failed to state a claim under the CFAA.[197] Like *Lockheed*, *Shamrock* seems to suggest that courts are willing to diverge from the traditional interpretation of "authorization" and realize that either the CFAA may not cover certain conduct or the statute no longer fits the modern crime.

i. What *Brekka* and *Drew* Can Learn From *Lockheed* and *Shamrock*

Despite the seemingly unrelated situations that brought the respective cases to trial, *Brekka* and *Drew* have something in common: after the decisions of *Lockheed* and *Shamrock*, courts can choose to see them in a new light. The *Brekka* court used the agency-based approach and the *Drew* court used the contract-based approach, but both can be analyzed more simply, and *Lockheed* and *Shamrock* provide an interesting starting point for a much clearer analysis.

192. *Id.*

193. *Id.* at 964.

194. *Id.* at 965–66.

195. *Id.* at 966 (quoting Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1630 (2003)).

196. *Id.* at 967.

197. *Id.* at 968.

When Brekka emailed himself the master report containing sensitive company data and later when he logged in as "cbrekka," he did not exceed his authorization.[198] LVRC, through its email service provider, LOAD, granted him access to the statistics in their files and, as proof of his authorization, gave him a user name and password to retrieve them.[199] He did not exceed his own authorization because LVRC hired him to interact with LOAD.[200] As such, when LOAD gave him specific access to those files to assist him in his duties of conducting internet marketing programs, designed the "cbrekka" user name specifically for his use, and had not deactivated it when Brekka left, Brekka's accessing of the computer and the usage statistics with the proper authorization does not seem to fall within the "very group that Congress chose not to reach."[201] Like in *Lockheed*, Brekka's access of the computer system did not cause any damage according to the CFAA's definition contained in Section 1030(e)(8).[202] He did not impair any data or harm the system, he simply sent himself an email he created in the scope of his employment and looked at data he used in the regular course of his work.[203] If Brekka was an outsider hacking into the system or a minor company computer programmer snooping around without access to the usage statistics, a court would be justified in finding that he accessed the system without authorization or even in excess of authorization. If he planted a *Morris*-like virus, the court could find he caused damage to the integrity of LVRC's systems.[204] But LVRC's real complaint focused on Brekka's subjective state of mind when he accessed information that he had no personal use for and the public relations damage that could occur if his post-access actions resulted in a list of patients in their Fountain Ridge Rehabilitation Facility becoming public knowledge.[205] Under the analysis used in *Lockheed* and *Shamrock* and the plain language of the CFAA, LVRC's complaint re-

198. LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

199. *See id.*

200. *See id.* at 1129–30.

201. *See id.* at 1130. After noticing Brekka logged in, LVRC deactivated the account the same day. *Id.*; *Compare* Lockheed Martin Corp. v. Speed, 2006 U.S. Dist. LEXIS 53108, at *15 (Congress chose to ignore the group who access with authorization), *and Shamrock*, 535 F.Supp.2d at 968 (holding employee who was authorized to use computer at Shamrock and granted access to specific files did not access either "without authorization" or "exceed" his authorized access), *with Brekka*, 581 F.3d at 1135 (holding the term without authorization is limited to someone who has no permission to use a computer, like a hacker, or when an employer specifically removes the employees access to use the computer, but the defendant still accesses it).

202. *See Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *27–28.

203. *See Brekka*, 581 F.3d at 1130.

204. *See generally* United States v. Morris, 928 F.2d 504 (2nd Cir. 1991).

205. *Brekka*, 581 F.3d at 1130, 1132.

garding Brekka's subsequent actions was not governed by the CFAA provisions.[206]

The *Drew* court's decision to interpret the CFAA under the breach-of-contract analysis presents a different parallel to *Lockheed*'s plain-meaning analysis and requires more attention to the specific facts of Drew's MySpace account. When Drew joined MySpace in 2006, she had to "check the box" affirming she agreed to the MSTOS, thereby committing to the site's "browsewrap" and "clickwrap" agreement.[207] However, the sign-up page did not contain the MSTOS and visitors had to click one of several hyperlinks before they discovered them, which allowed someone like Drew to click the sign-up box without reading the terms.[208] While courts have routinely upheld "clickwrap" agreements, the enforceability of "browsewrap" agreements turn on the knowledge of the user, be it actual or constructive, before they use the site.[209] With the "check the box" clickwrap agreement on the sign-up page and not specifically on the MSTOS page, a court cannot definitively impart actual or constructive knowledge of MySpace's terms of service on Drew.[210] Without the actual or constructive knowledge of the myriad of activities MySpace chose to deem a violation of their terms, a court would have to stretch to find Drew's creation of a fake profile an "intentional breach" of a contract, which is the scienter element needed to find Drew accessed MySpace "without" or "in excess" of her given authorization.[211] One of the reasons the court chose to void Drew's convictions for vagueness rested in the very fact that it was unsure if every intentional, let alone unintentional or unknown, breach of a public website's terms of service is equivalent to accessing the site in excess or without authorization.[212]

Like the defendants in *Brekka*, *Lockheed*, and *Shamrock*, MySpace granted Drew permission to use its server when she initially signed up as a member, subject to certain limitations within the MSTOS, and Drew "remain[ed] authorized to use the computer" even if she violated those limitations.[213] Drew retained this access even when she had no knowledge of violating any restriction or may have been unsure what restrictions actually constitute exceeding authorized access and which ones are harmless mishaps. Because "authorization" turns on the actions undertaken by the one who defines the scope of the access, it was MySpace's decision whether to allow Drew to continue to use their site or immediately terminate her authoriza-

206. *See Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *15.

207. United States v. Drew, 259 F.R.D. 449, 453 (C.D. Cal. 2009).

208. *Id.*

209. *Id.* at 462.

210. *Id.* at 453–54.

211. *See id.* at 461.

212. *See id.* at 467.

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

tion.[214] It is irrelevant that this task was either impossible or impractical since MySpace gained several hundreds of thousands of new members a day and that the company chose not to ensure every new account complied with the MSTOS.[215] MySpace never notified Drew it planned to terminate her access; in fact, Drew deleted the profile herself.[216] Like Brekka, Drew had access as an inside user, not an outside hacker who had gained access to the site and was communicating with an authorized member.[217] While it eventually led to harassment and tragedy, Drew did not exceed the authorization that the general public has on MySpace.[218] If anything, the MSTOS resembles the confidentiality agreement Gast signed while employed by Shamrock, which the court did not find relevant to his potential liability, because signing or even breaching the contract did not change the fact that Shamrock originally granted him access to their system and the files in question.[219] By agreeing to allow Drew to join MySpace, the website granted her access to the site and to other members' profiles.[220] Therefore, Drew accessed the website with authorization and seems to fit "within the very group Congress chose not to reach."[221]

Drew's actions of viewing another member's profile and posting or sending comments to it did not cause damage as Section 1030(e)(8) defines it, and Drew's actions, while eventually resulting in the death of a young girl, did not result in a loss of anything of value through the computer.[222] Here, the actions the government focused on are the exact same type that the complaint in *Lockheed* addressed: that Drew's actions after she accessed the information and interacted with Megan on MySpace provided a way to try to

214. *See id.* at 1133–35. While discussing the agency-based approach, the court notes that without the employer removing 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 . . . would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner." *Id.*

215. *Drew*, 259 F.R.D. at 454–55. MySpace would only monitor new accounts on a "limited basis" and even then usually just to make sure they followed the guidelines on posting photographs, not the new member's interaction with other members or on the truthfulness of their account. There were options on the website for "Safety Tips" and to "Report Abuse," but these were merely available for use at the user's discretion. *Id.*

216. *See id.* at 452.

217. *See Brekka*, 581 F.3d at 1135.

218. *See Drew*, 259 F.R.D. at 453-55; *see also Brekka*, 581 F.3d at 1133.

219. *See* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 963 (D. Ariz. 2008).

220. *See Drew*, 259 F.R.D. at 453.

221. *See* Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *15 (M.D. Fla. Aug. 1, 2006).

222. 18 U.S.C. § 1030(e)(8).

punish her for the comments that led to Megan's suicide.[223] Without criminalizing breaches of contract (which the CFAA does not do and as *Drew* notes, ordinary people would never expect), the liability of an authorized individual who accesses a website within the limitations of that authorization cannot turn on the supposed change in the individual's mental state when they violate a website's terms of service, of which they may have no knowledge.[224] By keeping it simple, like *Lockheed* and *Shamrock* recommend through the use of the plain meaning of "authorization" and the plain language of the CFAA, the definitional vagueness becomes a little clearer. Ignoring the agency-based, code-based, and contract-based approaches and focusing on the plain meaning of the word would require courts to acknowledge that there is a group Congress chose not to cover under the CFAA. But it would finally confirm "that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."[225]

D. How to Find Clarity in the CFAA

With many different interpretations of what exactly constitutes "authorization," courts and Congress are left with a choice: choose one of three approaches currently in use, accept that the statute ignores those who access with authorization and find another way to punish the *subsequent* actions, or create a new statute that specifically addresses the issues the CFAA continually fails to cover. At this point, it seems the first option is hopeless without Supreme Court intervention, which would be the Court's first look at the statute in the CFAA's history.[226] As evidenced by several cases discussed in this comment, courts are set in their ways, and based on the facts of the case, the agency-based, code-based, or contract-based approaches could all be appropriate. On a case-by-case basis, these three approaches work well to resolve the particular issues presented to the courts. It is when you view the entire jurisprudence of the CFAA that confusion is readily apparent. Legislative history offers little clarity on which approach is correct. When courts turn to legislative history for answers, they quickly realize it supports all three approaches.[227] Based on the recent decisions in *Lockheed* and *Shamrock*, it no longer appears that an employee/employer fiduciary relationship or a contract will guide a court towards one particular approach.[228] Either

223. *See Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *15.

224. *See Drew*, 259 F.R.D. at 464; *see also Brekka*, 581 F.3d at 1134.

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

226. Akerman, *supra* note 1, at 1.

227. Field, *supra* note 2, at 829–30.

228. *See Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *12 (holding the court is not persuaded by the agency approach despite the fact that the defendants were employed by Lockheed); *see also Shamrock*, 535 F. Supp. 2d at 963 (employee's signed Confidentiality Agreement did not result in the court using the contract-based approach).

clarity or a detailed, systematic test explaining what factors a court can take into consideration is needed desperately and one of the three branches of federal government will likely have to provide it.[229]

Both *Lockheed* and *Shamrock* represent a promising trend of simplifying the language in the already convoluted CFAA for the second option. But this too may require the highest court's intervention to place all the lower courts on the same page. The methods used in these decisions are far from an obvious answer to the definitional problems within the CFAA and often require extensive explanation to justify separation from the three traditional approaches.[230] Moving toward this simplified analysis also presents the problem that potential loopholes will emerge. Is a defendant in a case like *Morris*, where the court uses the code-based approach perfectly, now free to use his or her authorization to infect government computers with homemade viruses without fear of reprimand?[231] Is the only punishment facing cyberbullies who harass one of their classmates expulsion from their high school?[232] These questions may be answered soon if the Supreme Court chooses to intervene and set a test for the CFAA's analysis.

Another option still exists: create new laws that specifically address cyberbullying and the subsequent actions undertaken when an individual, with the proper authorization, accesses the computer and then uses that access for criminal or damaging ends. When Congress enacted the CFAA, it did so to replace the outdated mail- and wire-fraud statutes that federal prosecutors used to prosecute cybercrime, which had become ineffective in addressing the new criminal conduct occurring online.[233] The same problem facing the CFAA right now has happened before, and will happen again, unless Congress continually updates the CFAA to keep abreast of modern computer technology or creates a new statute to address the evolving criminal conduct on the internet. Sadly, the deaths of Megan Meier and Phoebe Prince could not be prevented, but hopefully Congress will continue to take the necessary steps to prevent these tragedies from reoccurring. The public outcry over these deaths has led to a demand for action and at least for now, Congress seems to be listening. On April 2, 2009, the U.S. House of Representatives introduced House Resolution 1966, the "Megan Meier Cyberbullying Prevention Act," which amends Chapter 41 of Title 18 to make conduct

229. Akerman, *supra* note 1, at 1.

230. *See generally Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *1; *see also Shamrock*, 535 F. Supp. 2d at 963–65.

231. *See generally* United States v. Morris, 928 F.2d 504, 504–11 (2nd Cir. 1991).

232. *2 Students Reportedly Expelled from Mass. High School After Cyber Bullying Suicide*, Feb. 24, 2010, http://www.foxnews.com/story/0,2933,587340,00.html?test=latestnews (last visited February 25, 2010). (The school refused to comment on whether they expelled the students who harassed Phoebe Prince, but the Superintendent did say they "will not be returning.").

233. Buckman, *supra* note 5, at 14.

like Drew's open to fine or subject "to imprisonment not more than two years."[234] The application of this law, and any similar ones passed at the state level, will shed new light on "cyberbullying," the definition of "authorization" in the CFAA, and the *Drew* decision.

V. CONCLUSION

Although the recent decisions of several federal district courts appear to show there is a chance the definitional vagueness present in the CFAA will soon become clear, the statute is not out of the woods yet. In 2001, the First Circuit summarized the definitional difficulties courts struggle with in the CFAA because "Congress did not define the phrase 'without authorization,' perhaps assuming the words speak for themselves. The meaning, however, has proven to be elusive."[235] Elusive, yes; but not impossible if Congress and the courts begin to accept the CFAA for what it is: a statute limited by the speed at which the internet is evolving.

When Congress created the CFAA, it did so to prosecute hackers, the outsiders who never had any authorization to begin with. Eventually, through numerous revisions to keep the statute current, it grew to include a civil cause of action and addressed those who had initial authorization, but subsequently exceeded their level of access. The definitional problems in the CFAA began to emerge when prosecutors and plaintiffs attempted to stretch the statute's reach to the very group that Congress chose to leave alone—individuals who have specific access to the files in question. Unless they cause damage to these files, the individuals with the proper access do not violate the CFAA. However, the statute has been stretched to try to cover the actions these individuals take with this information after they access it. As the *Lockheed* court correctly explained, "as much as Lockheed might wish it to be so . . . [the CFAA] does not reach the actions alleged in the Complaint."[236] The CFAA only becomes vague and unclear when prosecutors and plaintiffs use it in ways that Congress never intended it. A cybercrime statute like the CFAA regulates conduct on the computer and addresses the violations that occur there. It does not regulate the actions taken after the computer no longer plays a role in the alleged crime.

With the recent decisions in *Drew* and *Brekka*, the definitional vagueness of the CFAA came under fire again, especially in *Drew*, where there was additional public outcry for justice. Despite this, Judge Wu correctly voided Drew's convictions for the same reason prosecutors should not have charged her under the statute—it fails to address her conduct adequately.

234. Megan Meier Cyberbullying Prevention Act, H.R. Res. 1966, 111th Cong. (2009).

235. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001).

236. Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *15 (M.D. Fla. Aug. 1, 2006).

Like the defendants in *Brekka*, *Lockheed*, and *Shamrock*, Lori Drew was an insider who had the proper authority to access MySpace's website, especially since it was not required for her even to read the MSTOS before she signed up. Once she crossed this threshold, the CFAA was powerless against her subsequent actions because Congress did not originally design the statute for that purpose. The Internet is constantly evolving at a rapid pace, and this fact places a burden on Congress to stay current on the cyber crimes that are currently at issue, including cyberbullying.

The analysis presented in *Lockheed* and *Shamrock* and this comment's proposed interpretation of the decisions in *Drew* and *Brekka* do not suggest that the three favored approaches to interpreting "authorization" under the CFAA are moot. On the contrary, each can play a very specific role in the analysis of the statute, provided their limitations are acknowledged. The agency-based approach will continue to work for the lower-level employee who exceeds his authorization and accesses information above his pay grade, provided the claim does not focus on the employee's change in mental state. The code-based approach is still effective at prosecuting outside hackers who have no authorization or *Morris*-like individuals whose computer knowledge allows them to exceed their authorization. Finally, the contract-based approach, with an actual contract delegating the individual's authorization, will continue to provide a civil course of action for breach of contract at the very least. It is possible that the Supreme Court's intervention will affirm each of these approaches.

Even though intervention by the Supreme Court is both plausible and necessary, the inherent limitations of the CFAA present the same problems as the mail- and wire-fraud statutes it supposedly replaced. To address emerging conduct like cyberbullying, online harassment and other post-access crimes, there is a need for Congress to create a new statute addressing these issues, much like the reason for the CFAA's inception. To prosecute and punish these previously unheard of crimes, there must first be a statute that addresses this conduct and provides guidelines for its application by law enforcement to ensure that the public has a fair warning and as such, to avoid it being held unconstitutionally vague. While cyberbullying may have been the issue that brought the definitional vagueness and confusion in the CFAA to the attention of the courts, there is still hope for clarity and resolution in the near future.