William & Mary Law Review

Volume 52 (2010-2011)
Issue 4

Article 7

March 2011

Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act

Garrett D. Urban

CAUSING DAMAGE WITHOUT AUTHORIZATION: THE LIMITATIONS OF CURRENT JUDICIAL INTERPRETATIONS OF EMPLOYEE AUTHORIZATION UNDER THE COMPUTER FRAUD AND ABUSE ACT

TABLE OF CONTENTS

INTRODUCTION

The Computer Fraud and Abuse Act (CFAA) has recently been described in various publications as "another arrow in the quiver" of legal options for employers to use against former employees,[1] a way "to put some real teeth into your complaint,"[2] and a "gap-filler" obviating the need for congressional action to create federal jurisdiction for trade secret misappropriation.[3] Employers have certainly noticed, bringing an increasing number of CFAA claims against former employees who used their computer access at work to take, misuse, or alter company data during their employment.[4] Congress originally passed the CFAA in 1984 to create criminal liability for newly developing computer crimes, such as hacking.[5] The statute has been amended several times and currently offers a civil cause of action for persons suffering certain damages or losses due to violations of the Act.[6]

Although the CFAA may not be a particularly well-known statute, it lurks in the background of almost every interaction with a computer. The statute prohibits individuals who access any computer connected to the Internet from performing certain actions either "without authorization or exceeding authorized access."[7] The matter of authorization is relatively uncomplicated when applied to

---

1. David W. Garland & Linda B. Katz, *Computer Fraud and Abuse Act: Another Arrow in the Quiver of an Employer Faced with a Disloyal Employee—Part I*, METROPOLITAN CORP. COUNS., May 2006, at 5.

2. Bradley C. Nahrstadt, *Former Employee Sabotage? Invoke the Computer Fraud and Abuse Act*, J. INTERNET L., Feb. 2009, at 17, 25.

3. Graham M. Liccardi, Comment, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155, 157 (2008).

4. *See* Linda K. Stevens & Jesi J. Carlson, *The CFAA: New Remedies for Employee Computer Abuse*, 96 ILL. B.J. 144, 144-45 (2008) (discussing the increasing use of the CFAA by employers against employees).

5. Glenn D. Baker, Note, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER/L.J. 61, 63-65 (1993).

6. 18 U.S.C. § 1030(g) (2006).

7. *Id.* § 1030(a). Any computer "used in or affecting interstate or foreign commerce or communication" is protected under the Act, which effectively expands the scope to any computer connected to the Internet. 18 U.S.C. § 1030(e)(2)(B) (Supp. II 2008); OFFICE OF LEGAL EDUC., PROSECUTING COMPUTER CRIMES 3 (Scott Eltringham ed., 2007).

the traditional hacker, a person without any connection to the affected computer who breaks through some level of security in order to access restricted information.[8] Interpreting the CFAA has proven more difficult when applied to the employer-employee relationship, as employees typically have some permission to access their employers' computers as part of their job duties.[9] Congress did not do the courts any favors by leaving "authorization" undefined in the statute.

Federal courts have taken three general approaches to defining "authorization," broadening the scope of the CFAA in different ways. This split in interpretation has been well documented in court opinions and increasingly in legal scholarship.[10] Some courts have cited agency law to hold that authorization terminates whenever an employee acts against the employer's interests, giving the statute extremely wide reach.[11] Other courts have used contractual relationships between the employer and employee to define the scope of authorization.[12] Finally, some courts have cited the plain language of the statute to determine that an employee permitted to access a computer does so with authorization.[13] These opinions are frequently conflated with a "code-based" approach, because the existence or scope of an employee's authorization often depends on whether some computer restriction, such as a password, must be circumvented prior to the contested use.[14]

---

8. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1576 (2010) [hereinafter Kerr, *Vagueness*] ("If hacking is not unauthorized access, nothing is.").

9. *See, e.g.*, Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 933-34 (W.D. Tenn. 2008) (discussing the "split in legal authority" about whether employee actions in these situations are with or without authorization).

10. *See, e.g.*, Lockheed Martin Corp. v. Speed, 81 U.S.P.Q.2d (BNA) 1669, 1672-76 (M.D. Fla. 2006) (discussing different interpretations courts have given the CFAA). *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) [hereinafter Kerr, *Cybercrime's Scope*]; Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employee's Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819 (2009).

11. *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).

12. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001).

13. *See, e.g.*, *Speed*, 81 U.S.P.Q.2d (BNA) at 1672-73.

14. *See* Kerr, *Cybercrime's Scope*, *supra* note 10, at 1644-46. Court opinions such as *Speed* that have applied a plain-language approach have not specifically referred to code-based restrictions, but their examination of an employee's permission to access computers is

Although arguments have been made for the relative merits of each approach,[15] less analysis has focused on what purposes the CFAA should accomplish in the employer-employee context and whether any of the three leading interpretations can reach *all* of those purposes as the Act is currently drafted. This Note seeks to vocalize what those purposes should be by examining both the legislative history of the CFAA and more general arguments, such as principles of statutory construction and federalism. It especially focuses on the interaction between claims under the CFAA and other state causes of action frequently asserted by employers against their former employees. In the end, no single interpretation courts employ to define authorization meets all of the outlined purposes when applied to employer-employee conflicts.

This Note thus proposes an amendment to the language of the CFAA that would, in conjunction with a code-based interpretation of authorization, strike a proper balance between employer protections and employee rights. Part I provides a brief history of the development of the three different interpretations of authorization courts have used when applying the CFAA to employees. Part II looks at the legislative history of the statute and other legislative principles to develop six criteria that a successful application of the statute should meet. These criteria are then applied to the current interpretations in Part III, demonstrating that agency and contract approaches to the CFAA are overinclusive, whereas a code-based approach renders the statute too narrow. Finally, Part IV proposes new language to replace Section 1030(a)(5)(A), demonstrates its benefits, and discusses its potential application.

I. EMPLOYER-EMPLOYEE AUTHORIZATION UNDER THE CFAA

The CFAA has been in effect, in some form, for twenty-seven years.[16] The first congressional response to computer crime, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, was limited in scope, protecting only information and com-

---

consistent with a code-based interpretation. *See* Field, *supra* note 10, at 826-27.

15. *See supra* note 10.

16. Baker, *supra* note 5, at 63-65.

puters used by the U.S. government and financial institutions.[17] The statute did not reach private computers or networks, nor did it provide for civil liability.[18] Congress expanded its reach two years later with the Computer Fraud and Abuse Act of 1986, which defined six separate computer crimes and expanded the statute's coverage to reach certain interstate computer networks.[19] The statute still did not have a private cause of action, however, and Congress had few worries about its application to the workplace outside of concerns about unintentionally criminalizing innocent employee behavior.[20]

The statute drew distinctions between those who accessed a computer without authorization and those who exceeded authorized access.[21] This distinction, which the present statute retains, was first interpreted in detail in *United States v. Morris*.[22] Robert Morris, a graduate student at Cornell, used his access to university computers to release a virus that ended up crashing computers across the country.[23] Morris argued he could not be liable under the codified Computer Fraud and Abuse Act of 1986 because criminal liability under Section 1030(a)(5)(A) required intentional access of a computer "without authorization," limiting criminal liability to users who lacked "access to *any* federal interest computer."[24] The court rejected this argument, holding that legislative history indicated Congress did not mean to prevent prosecution of any person who had permissible access to at least one such computer.[25] The court focused on the fact that Morris's program had allowed him to

17. *Id.* at 63-66.

18. *Id.*

19. *Id.* at 66-71.

20. *See* S. REP. NO. 99-432, at 7-8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485-86 (discussing the statute's exclusion from liability of "insiders" who have access to some computers but not others).

21. Baker, *supra* note 5, at 67.

22. 928 F.2d 504 (2d Cir. 1991).

23. *Id.* at 505-06.

24. *Id.* at 510-11. The statute at the time protected federal interest computers, defined as those "operated for or on behalf of the Government of [the] United States." *Id.* at 508 (quoting 18 U.S.C. § 1030(A)(3) (Supp. II 1984)). The statute has since been expanded to protect almost all computers. *See supra* note 19 and accompanying text.

25. *Morris*, 928 F.2d at 511.

access other federal interest computers—computers he did not have permission to use.[26]

Morris was the first case to interpret authorization under the CFAA[27] and remains a starting point for discussions of employer-employee liability under the Act. Since *Morris*, the statute has been amended repeatedly. In 1994, Congress added a private cause of action and expanded its protection to all computers involved in interstate commerce.[28] The CFAA currently contains seven separate causes of action that may result in criminal or civil liability.[29] Of these, four are frequently used by employers in civil cases against former employees. Section 1030(a)(2)(C) (Section 2C) reaches anyone who obtains any information from a protected computer through intentional access without or in excess of authorization.[30] Section 1030(a)(4) (Section 4) affects anyone who advances fraud and obtains something of value through access to a protected computer without or in excess of authorization.[31] Section 1030(a)(5)(A) (Section 5A) covers anyone who damages a protected computer without authorization.[32] Finally, Sections 1030(a)(5)(B)-(C) (Sections 5B-C) punish anyone who accesses a protected computer without authorization if that access causes damage, whether or not the person causes the damage recklessly.[33] In order to pursue a civil

---

26. *Id.*

27. *See* Baker, *supra* note 5, at 79.

28. Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661, 666-67 (2009).

29. *Id.* at 667. For a detailed chronological history of the revisions to the CFAA, see Kerr, *Vagueness*, *supra* note 8, at 1563-71.

30. 18 U.S.C. § 1030(a)(2)(C) (2006) ("Whoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer [shall be liable]."). Any computer affecting interstate or foreign commerce is protected by the current statute. *See supra* note 7.

31. *Id.* § 1030(a)(4) ("Whoever ... knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, [shall be liable] unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.").

32. 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008) ("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 [shall be liable].").

33. *Id.* § 1030(a)(5)(B)-(C) ("Whoever ... intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

remedy, a party must also prove damage or loss under the statute, most easily satisfied by showing the defendant's action cost the company more than $5,000.[34]

In examining these four causes of action, some important differences become apparent. Section 2C and Section 4 apply to individuals who lack or exceed authorization, but Section 5A and Sections 5B-C reach only individuals acting without authorization. Although the statute does not define authorization, it does specify that exceeding authorized access means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[35] Also, Section 5A concerns damage caused without authorization, as opposed to access without authorization.[36] Courts have taken these same parameters and applied them very differently in assessing the liability of former employees.

A. Agency Approach

The first approach utilized by some courts in interpreting authorization under the CFAA involves agency law. Employer-employee suits frequently arise when employees access, copy, or alter computer data during their employment and then quit, often to work for a competitor or to start a competing business.[37] Employers want to hold these employees liable for their actions, which adversely affect their companies' interests. Because these actions, such as copying customer lists, taking trade secrets, or deleting files, take place while the defendant is still employed, courts have sometimes taken cues from common law principles of agency.[38]

The Second Restatement of Agency states, "Unless otherwise agreed, the authority of an agent terminates if, without knowledge

---

intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss [shall be liable].").

34. 18 U.S.C. § 1030(g) (2006) (incorporating the types of damages listed in § 1030(c)(4)(A)(i)(I)-(V)).

35. *Id.* § 1030(e)(6).

36. 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008).

37. *See, e.g.*, Lockheed Martin Corp. v. Speed, 81 U.S.P.Q.2d (BNA) 1669, 1670 (M.D. Fla. 2006).

38. *See infra* notes 40-46 and accompanying text.

of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[39] Applying these principles to the CFAA, authorization ceases upon the creation of an adverse interest; therefore, employees may be acting without authorization even while they continue to be employed, possess a password, or have explicit permission to use a computer. The U.S. District Court for the Western District of Washington became the first court to apply this approach in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*[40] Shurgard accused former employees of e-mailing confidential marketing information to a competitor while still employed by Shurgard, then leaving to join the competing company.[41] Because the defendants had adverse interests to their employer, the court held their authorization to use their computers ceased under agency principles, rendering the conduct without authorization and triggering a potential claim under the CFAA.[42]

This interpretation of the CFAA gained further credibility when the Seventh Circuit reached a similar conclusion in 2006 in *International Airport Centers, L.L.C. v. Citrin*.[43] Citrin, an employee of International Airport Centers, deleted information from his laptop before quitting the company to start a competing business.[44] The court held that "Citrin's breach of his duty of loyalty terminated his agency relationship ... and with it his authority to access the laptop."[45] Citrin's employment contract specifically authorized him to destroy data in his laptop upon termination, but the court still held that the breach of his duty of loyalty controlled.[46]

The use of agency principles to define authorization within the CFAA has been lauded as a boon to employers.[47] This definition gives the statute wide application because civil liability attaches to

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

40. 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

41. *Id.* at 1122-23. The court held the plaintiff stated a claim under Section 2C, Section 4, and the contemporary provision currently encoded in Sections 5B-C. *Id.* at 1125-27.

42. *Id.* at 1125.

43. 440 F.3d 418 (7th Cir. 2006).

44. *Id.* at 419.

45. *Id.* at 420-21.

46. *Id.* at 421.

47. *See, e.g.*, Paul S. Chan & John K. Rubiner, *Access Denied*, L.A. LAW., Feb. 2006, at 22, 24 (discussing *Shurgard* and its low pleading standard).

any employee who accesses a computer after acquiring any interest contrary to his employer.[48] Many courts continue to apply agency principles under this line of reasoning, and few other appellate courts have discussed "authorization" so extensively, making *Citrin* strong persuasive authority.[49] Other district courts, however, have increasingly grown worried about the consequences of applying the statute so broadly.[50]

B. Contract Approach

A second approach to interpreting authorization in employment cases focuses on contractual relationships between the parties. Under this approach, employment contracts, or similar documents, are the basis of authorization, and liability under the CFAA may attach if a party breaches its duties under the contract.[51] The First Circuit applied this reasoning in *EF Cultural Travel BV v. Explorica, Inc.*[52] *Explorica* concerned an employee who left EF Cultural Travel and helped form a new company, using knowledge from his previous position to write a program that scraped publicly available information from his old company's website.[53] The court used the violation of his confidentiality agreement to hold that the use of proprietary information exceeded authorized access, without reaching a decision on whether the access was without authorization.[54] The contract between the parties thus formed the basis for a determination of authorization.

Other courts have also used contracts to evaluate authorization. The Eastern District of Virginia, although not considering an employer-employee dispute, ruled that America Online (AOL) stated a claim under the CFAA when the defendant violated AOL's Terms

48. Of course, the employer must still show the requisite damages. *See* 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008) (requiring damage as an element of a CFAA violation).

49. *See, e.g.*, NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1056-59 (S.D. Iowa 2009) (endorsing the agency interpretation of authorization under the CFAA).

50. *See, e.g.*, Lockheed Martin Corp. v. Speed, 81 U.S.P.Q.2d (BNA) 1669, 1675 (M.D. Fla. 2006) (rejecting agency principles while noting that an employee could potentially be liable for damages resulting from checking personal e-mail on company time).

51. *See* Field, *supra* note 10, at 827.

52. 274 F.3d 577 (1st Cir. 2001).

53. *Id.* at 578-80.

54. *Id.* at 581-82.

of Service, making the defendant's action unauthorized.[55] The First Circuit also held that a defendant exceeded authorized access in *United States v. Czubinski* based on the IRS employee handbook, which limited authorized computer access to actions needed for official duties.[56] The court found that by violating provisions in the handbook, the employee had exceeded authorized access under the CFAA.[57]

Perhaps the furthest expansion of this approach occurred in *Register.com, Inc. v. Verio, Inc.*, when the Southern District of New York held that a company acted without authorization when it violated posted restrictions on the use of information from a competitor's web page.[58] The court based its decision largely on the plaintiff's subsequent objection to the use of its website,[59] an interpretation that would seem to give a computer owner complete and subjective power to define the limits of unauthorized access of otherwise public information.[60] The use of the contractual approach has not been widespread, and many courts have not even acknowledged it when interpreting "authorization" under the CFAA.[61] As courts have started to reject agency principles more frequently, however, they have done so in ways that may support an approach that looks to the standards governing the employer-employee relationship to determine the scope of authorization.[62]

C. Code-Based Approach

The final common approach to interpreting authorization within the CFAA looks to code-based restrictions on users' access to a computer. Under the code-based approach, users act without authoriza-

---

55. Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450-51 (E.D. Va. 1998). Note, however, that the defendant could not defend against this claim due to discovery violations. *Id.* at 447.

56. 106 F.3d 1069, 1071 & n.1 (1st Cir. 1997).

57. *Id.* at 1078. However, the court overturned the defendant's conviction because the defendant "did not obtain anything of value." *Id.* at 1078-79.

58. 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000).

59. *Id.*

60. Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass, and Privacy*, 62 BUS. LAW. 1395, 1412 (2007).

61. *See* Field, *supra* note 10, at 848-49.

62. *See infra* notes 66, 73.

tion if they bypass password or security measures to gain access to a computer, whereas users act in excess of authorization if they are allowed to access the computer but bypass additional security measures to reach other information not freely accessible.[63] Bypassing such coding requires a user to fake identification, "exploit a weakness in the code," or affirmatively act to misuse the computer in some way.[64] This approach puts the onus on employers, or other computer owners, to protect their information.[65]

No courts have explicitly adopted a code-based approach to interpreting authorization, but many district courts have issued opinions in accordance with this reasoning.[66] The Middle District of Florida applied what it termed the "plain meaning" of the statute in *Lockheed Martin Corp. v. Speed*.[67] *Speed* concerned employees who allegedly conspired with a competitor to pass along trade secrets

63. *See* Kerr, *Cybercrime's Scope*, *supra* note 10, at 1644-46.

64. *Id.* at 1644-45.

65. *See id.* at 1644.

66. *See, e.g.*, Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008). Courts have termed similar approaches "plain meaning," or just cited the language of the statute. *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) ("[T]he plain language supports a narrow reading of the CFAA."). One possible reason for courts' refusal to adopt this terminology may be the justifications different courts have employed in advancing competing interpretations of the CFAA. The agency and contract approaches to defining the CFAA cite outside sources, such as agency law or existing contracts, to augment interpretation of authorization in the CFAA. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (citing RESTATEMENT (SECOND) OF AGENCY §§ 112, 387 (1958)); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001) (relying on a confidentiality agreement as a contract). In contrast, courts reaching results compatible with the code-based approach have found the CFAA to be clear on its face, and therefore rejected the need to consult such outside sources. *See Black & Decker*, 568 F. Supp. 2d at 934. Because the "code-based" terminology comes from academia, not the statute itself, even courts embracing this approach would likely seek to avoid referring directly to code-based terminology, as such a reference would contradict claims that courts applying agency or contract approaches did not need to go beyond the language of the CFAA to properly interpret authorization. Still, no court has clearly interpreted the CFAA to find that an employee must bypass an employer's code-based restrictions on access to violate the statute, and many of these cases could be equally susceptible to a contract approach based on an employer's documents or policies governing employee computer usage. *See supra* Part I.B.

At least one state computer fraud statute, conversely, has been interpreted to require a code-based approach. In *State v. Riley*, the court interpreted New Jersey's computer crime law, which is based on a similar statutory scheme involving access without or in excess of authorization, to "construe 'authorization' to refer only to a password, or other code-based restrictions to utilizing a computer" after examining case law and scholarship concerning the CFAA. 988 A.2d 1252, 1258 (N.J. Super. Ct. Law Div. 2009).

67. 81 U.S.P.Q.2d (BNA) 1669, 1673 (M.D. Fla. 2006).

from Lockheed Martin.[68] The court held that employees who had been permitted access to a company computer could not act without authorization on that computer, and employees with access to "the precise information at issue" could not exceed authorized access.[69] This mirrors the code-based approach, as the court reasoned that because Lockheed Martin did not restrict the employees' computerized access to the information, they had authorization from their employer.[70] Similarly, the court in *Black & Decker, Inc. v. Smith* held that an employee could not be liable under the CFAA for accessing information on the company network when the company permitted him to access the network.[71] The court stated the statute was not concerned with the permissibility of subsequent uses of the information, only with whether the employee properly accessed the materials.[72] The Ninth Circuit has similarly reasoned that "[t]he plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer."[73] Recently, applying this standard in a criminal case, the court in *United States v. Nosal* dismissed several charges under the CFAA for alleged misuses of information that the defendants had authority to obtain as employees of their company at the time they accessed the material.[74] These cases reflect an interpretation based on a preexisting ability to access the materials, paralleling the code-based approach, rather

68. *Id.* at 1670.

69. *Id.* at 1673.

70. The court in *Speed* did not actually specify that security measures would be needed to prevent authorization, so it is not a textbook example of the code-based approach, but the opinion is consistent with this approach and the court specifically rejected the agency approach used by the Seventh Circuit in *Citrin* as being far too broad. *Id.* at 1673-76. Other commentators have also noted that the court's interpretation is consistent with the code-based approach. *See* Field, *supra* note 10, at 826-27.

71. *Black & Decker*, 568 F. Supp. 2d at 936.

72. *Id.* at 935.

73. LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009). The Ninth Circuit, however, did not specify the actions an employer could take to limit authorization, leaving the opinion open to both code-based and contract approaches to interpretation.

74. No. C 08-0237 MHP, 2010 U.S. Dist. LEXIS 24359, at *22-23 (N.D. Cal. Jan. 6, 2010). The court's inquiry in *Nosal* closely tracked the application of a code-based approach, focusing on the factual allegations against the defendants, including who accessed the material, whose password was used, the employment status of the user at the time of access, and what part of the system had been accessed. *Id.* at *20-26.

than focusing on the mindset of the employee as required by an agency interpretation.

Courts and academics have utilized all three of these approaches when applying the CFAA to disputes between employers and employees in recent years.[75] Courts have frequently attempted to justify applying one approach by examining and weighing the relative consequences of the different interpretations.[76] However, because the text of the statute restricts courts, less attention has been paid to whether any interpretation succeeds absolutely; that is, whether any approach can provide results that consistently support the underlying purposes of the statute.

II. PURPOSES OF THE CFAA

In order to determine whether any of these approaches to interpreting authorization accomplish all of the underlying purposes of the CFAA, those purposes first must be defined. Courts and scholars have frequently used the legislative history of the statute to support their favored approach. In particular, they cite records accompanying the CFAA's enactment in 1984 and its amendments in 1986 and 1996. From these examinations, different authors have reached, at the very least, four different conclusions: (1) Congress

75. There are additional interpretations that arguably do not fit these three categories, although none have clearly been adopted in employment cases under the CFAA. In *United States v. Morris*, the court looked at the "intended function" of the computer to determine the issue of authorization. 928 F.2d 504, 509-10 (2d Cir. 1991). This could be compatible with either the contract or code-based approach, if a contract or computer restriction manifested such intention. However, it could also represent an objective, reasonableness-type standard, an interpretation that has been proposed by at least one commentator. *See* Winn, *supra* note 60, at 1428 (arguing for a two-part test similar to normal trespass that takes into account the reasonableness of a person's expectations of privacy). The Fifth Circuit recently issued an opinion addressing the meaning of "exceeds authorized access" and reached a decision that does not necessarily conform to any of these approaches in upholding the convictions of an employee for using her valid computer access to commit a fraud, though it reached its decision under a clear error standard. *See* United States v. John, 597 F.3d 263, 270-73 (5th Cir. 2010). The opinion could be viewed as an example of the contract-based theory, given the company's explicit corporate policy against employees using their computer privileges to carry out fraud. *See id.* at 272. Alternatively, the holding could be viewed as incorporating a prohibition on illegal activities into the definition of authorization under the CFAA, a result that would seemingly just provide additional liability for separate criminal activity carried out via a computer. *See infra* Part II.A.

76. *See, e.g.*, *supra* note 66.

wanted the courts to employ an agency approach;[77] (2) Congress intended a plain language interpretation based on access;[78] (3) Congress sought to treat computer crimes like common law trespass;[79] and, perhaps in a reaction to the foregoing diversity of opinions, (4) that "the legislative history provides little authority value to the current debate."[80]

Attempting to justify a singular interpretation of authorization from decades of congressional statements is an exercise that may be futile even under ideal circumstances.[81] Instead, this Note will outline six underlying purposes of the statute by taking generalized guidance from the legislative history, justify the six criteria on separate policy grounds, and then judge the effectiveness of each interpretive approach in realizing these goals. This approach receives support from some commentators who have taken the CFAA's vague language and missing definitions as indications that Congress sought outside input and "dialogue" to determine the CFAA's reach.[82]

This Note does not attempt to establish an exhaustive list of purposes, but instead seeks to establish broad, underlying criteria for evaluating the CFAA's application to employer-employee disputes. In this way, this Note seeks to refocus the debate on what purposes the CFAA should serve, rather than which approach should be used under a particular set of facts. Based on this review, any successful approach to interpreting authorization should meet the following six policy goals: (1) liability under the CFAA should not be expansive, (2) the CFAA should be broad enough to cover technological advances, (3) employees should be subject to some

77. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127-29 (W.D. Wash. 2000).

78. *See* Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 934-36 (W.D. Tenn. 2008).

79. *See* Winn, *supra* note 60, at 1435-36.

80. *See* Field, *supra* note 10, at 831.

81. Numerous commentators and academics have discussed the problems with using legislative history to determine congressional intent, including the lack of any coherent vision shared among lawmakers and the lack of documentation of each individual's thoughts. *See generally* William N. Eskridge, Jr., *Legislative History Values*, 66 CHI.-KENT L. REV. 365 (1990); David S. Law & David Zaring, *Law Versus Ideology: The Supreme Court and the Use of Legislative History*, 51 WM. & MARY L. REV. 1653, 1661-62 (2010); Max Radin, *Statutory Interpretation*, 43 HARV. L. REV. 863, 870-73 (1930).

82. *See* Winn, *supra* note 60, at 1436; Field, *supra* note 10, at 839-41.

liability, (4) the CFAA should reach only crimes of computer misuse, (5) the CFAA should not replace traditional state laws providing causes of action against employees, and (6) the CFAA should create liability for all damage to computer data.

A. Liability Under the CFAA Should Not Be Expansive

The first underlying purpose that an interpretation of the CFAA should accomplish is that the resulting liability should be narrow. Concerns about excessively expansive liability date back to the original statute passed in 1984.[83] In fact, only one person was indicted under the statute in the two years before its first amendment.[84] When Congress did expand liability in 1986, the Judiciary Committee expressed concern about broad liability, limiting jurisdiction to violations with "a compelling Federal interest."[85] Congress also sought to ensure that individuals accidentally accessing restricted computers or causing damage would not be subject to liability and that legitimate business operations would not be affected.[86] This congressional desire is reflected in the shift to a higher scienter requirement of intentional conduct.[87]

This argument for narrow liability has limits. Amendments in 1994 and 1996 expanded the statute by adding additional causes of action and civil remedies, and the most recent amendment in 2008 expanded the definition of protected computers.[88] Therefore, Congress's intent to impose narrow liability should not be taken too far. Still, the statute has been crafted in such a way to limit its application to certain situations without creating liability for all unauthorized access or computer damage.

---

83. *See* Baker, *supra* note 5, at 65 (noting that the CFAA was initially criticized for being so limited in scope).

84. *Id.*

85. *See id.* at 66-67; *see also* S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.

86. S. REP. NO. 99-432, at 7-8, 1986 U.S.C.C.A.N. at 2485.

87. *See* Baker, *supra* note 5, at 68 (discussing the reasons that Congress increased the scienter requirement from "knowingly" to "intentionally").

88. *See* Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, 122 Stat. 3560 (2008); Stevens & Carlson, *supra* note 4, at 144. The CFAA now covers, in essence, any computer capable of accessing the Internet. *See supra* note 7 and accompanying text.

This purpose also meets general principles of statutory construction. Although courts frequently apply the CFAA in civil actions against employees, the statute remains primarily a criminal statute.[89] Rules of interpretation dictate that a statute with both criminal and civil liability should be interpreted consistently in both contexts.[90] On top of this, the Supreme Court has consistently cautioned that criminal statutes should not be applied in surprising or unanticipated ways that will impose unexpected liability on defendants.[91] Therefore, any interpretation of "authorization" should not impose criminal or civil liability on actions that would upset reasonable expectations.

Constitutional concerns may also arise from a broad application of liability. To the extent that any approach fails to provide "relatively clear guidelines" or "objective criteria" for criminalizing conduct, enforcement could be prohibited by the "void for vagueness" doctrine.[92] Furthermore, a wide-reaching interpretation could potentially implicate the First Amendment by allowing parties to define the limits of criminalization, leading to prohibitions on thoughts or speech.[93] Thus, an approach resulting in expansive liability would not be a successful interpretation of the statute. This limit does not mean, however, that a viable interpretation of authorization under the CFAA should prohibit any flexibility.

B. The CFAA Should Be Broad Enough To Cover Technological Advances

The continuous and seemingly unchecked pace of technological advancement must also be a concern for any statute that deals with

89. Lockheed Martin Corp. v. Speed, 81 U.S.P.Q.2d (BNA) 1669, 1671 (M.D. Fla. 2006) (referring to the CFAA as "primarily a criminal statute"); *see, e.g.*, United States v. Nosal, No. C 08-0237 MHP, 2010 U.S. Dist. LEXIS 24359, at *20-26 (N.D. Cal. Jan. 6, 2010) (concerning criminal charges under the CFAA).

90. *See* LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) (stating that courts should interpret statutes consistently for "both criminal and noncriminal applications" (citing Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004))).

91. *See id.* (citing United States v. Santos, 553 U.S. 507, 514 (2008) (plurality opinion)).

92. *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (quoting Gonzalez v. Carhart, 550 U.S. 124, 149 (2007)). For a full examination of possible "void for vagueness" challenges to the CFAA in employment cases, see Kerr, *Vagueness*, *supra* note 8, at 1583-87.

93. *See* Kerr, *Cybercrime's Scope*, *supra* note 10, at 1658.

computer crimes. Congress has been cognizant of this concern when passing and amending the CFAA. One of the main revisions in the 1986 amendment targeted newly developing computer crimes, including hackers utilizing "pirate bulletin boards."[94] Legislators widely approved of the prosecution's success in *United States v. Morris*, which concerned a computer virus not contemplated by the 1986 amendment, because it limited the need for additional federal criminal statutes.[95] Additional amendments have also reflected this desire for the CFAA to be adaptable to changes in technology. The Senate report accompanying the 1996 amendments confirmed this flexibility, stating that "[a]s intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology."[96]

Congressional intent for this purpose is clear, and practical enforcement concerns reinforce the statute's aim. Allowing flexibility in the statute prevents technological innovation, whether by society or by criminals, from outstripping liability and leaving gaps in protection.[97] Logistically, it also prevents Congress from having to update the statute or pass new laws even more frequently than it already has.[98] Therefore, any interpretation of authorization should not limit or artificially define the ways in which liability will attach, because future innovation in computer misuse is inevitable.

---

94. Baker, *supra* note 5, at 70.

95. *See* Brenda Nelson, Note, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER/L.J. 299, 302 (1991) ("In Congress, several bills aimed at amending laws used to fight computer crime were dropped upon receipt of the news that the Computer Fraud and Abuse Act—which does not mention computer worms or viruses—had been adequate to convict Morris. Legislators who supported the movement to develop a federal statute were clearly relieved that the 1986 Act proved effective in the Morris case despite the fact that it was drafted prior to the innovation of the computer worm, and thus, without Morris's particular crime in mind.") (internal citation omitted).

96. S. REP. NO. 104-357, at 5 (1996).

97. *See id.*

98. Congress amended the CFAA nine times in its first twenty years. Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 912 (2003).

C. Employees Should Be Subject to Some Liability

Given that this Note focuses on application of the CFAA to employees, an obvious yet necessary question is whether the CFAA should even apply to employees. The statute does not specifically exclude employees, but the focus on authorization muddles the picture. The congressional record accompanying amendments to the CFAA clearly indicates the CFAA was thought to apply to employees, at least in some circumstances. In 1986, the Senate report accompanying amendments to the original Act repeatedly referenced employee liability, usually in distinguishing between actionable conduct by outsiders and incidental or unintentional conduct by employees that the statute would not reach.[99] The Senate was clear, however, that employees could be prosecuted under the statute in certain circumstances, such as when a government employee accessed information from another department's computers.[100] When amending the CFAA in 1996, the Senate again indicated the statute covered certain actions by employees, specifically those functionally equivalent to outsider access.[101] As a general policy provision, this coverage is logical, as it accords with the broader principles of equal application of the law at the core of the American legal system.[102]

A related but equally important aspect of applying the CFAA to employees is that the congressional reports frequently paired insider liability with actions exceeding authorized access.[103] Although "exceeding authorized access" is defined in the CFAA,[104] the failure of Congress to define "authorization" makes it unclear if employees should be liable only under sections of the Act reaching

---

99. S. REP. NO. 99-432, at 7-9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485-87.

100. *Id.* at 7-8, 1986 U.S.C.C.A.N. at 2485-86.

101. S. REP. NO. 104-357, at 9 ("The law currently protects computers or computer systems from damage caused by either outside hackers or malicious insiders 'through means of a computer used in interstate commerce or communications.'").

102. *See* U.S. CONST. amend. XIV, § 1; Bolling v. Sharpe, 347 U.S. 497, 500 (1954) (incorporating equal protection into the Due Process Clause of the Fifth Amendment and thus making it applicable against the federal government).

103. S. REP. NO. 99-432, at 7-8, 1986 U.S.C.C.A.N. at 2485-86.

104. 18 U.S.C. § 1030(e)(6) (2006) ("[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.").

those exceeding authorization. However, it does reinforce the notion that Congress intended a clear separation between access without authorization and exceeding authorized access, because some causes of action are actionable only for completely unauthorized action.[105] General statutory construction also requires that an interpretation give meaning to each term in a statute so that nothing is rendered superfluous.[106] Therefore, any successful interpretation of authorization within the CFAA must result in at least some potential liability for employees and provide distinct meanings between acting without authorization and exceeding authorization.

D. The CFAA Should Reach Only Crimes of Computer Misuse

Given these general parameters for liability and its application to employees, the remaining criteria examine the specific computer uses that should fall within the CFAA's purview. Computer crimes can fall into two general categories: "traditional crimes committed using computers, and crimes of computer misuse."[107] Traditional crimes predated or arose without regard to the development of computers, and typically the use of a computer does not affect the elements of the underlying crime.[108] Conversely, computer misuse refers to crimes that developed only because of computers and are dealt with separately under criminal law.[109]

The legislative history of the development and expansion of the CFAA indicates that Congress formulated the statute in response to new crimes of computer misuse. In the late 1970s, difficulties fitting crimes of computer misuse into existing statues led to calls

---

105. *See, e.g.*, S. REP. NO. 99-432, at 7, 1986 U.S.C.C.A.N. at 2485 ("In the first place, the Committee has declined to criminalize acts in which the offending employee merely 'exceeds authorized access' to computers in his own department.").

106. *See* United States v. Ceballos-Torres, 218 F.3d 409, 412 (5th Cir. 2000) (citing Bailey v. United States, 516 U.S. 137, 145 (1995)) (discussing "the canon of statutory construction that warns against superfluousness").

107. Kerr, *Cybercrime's Scope*, *supra* note 10, at 1602.

108. *See id.* at 1602-03 (discussing examples such as Internet fraud and gambling).

109. *See id.* at 1603-04 ("We can define computer misuse as conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks. Common examples include computer hacking, distribution of computer worms and viruses, and denial-of-service attacks.").

for computer crime laws.[110] The 1984 Act responded to these fears that traditional larceny statutes would not be able to account for the unique problems posed by computer data that, for example, could be stolen without affecting the owner's possession.[111] Two years later, Congress spoke of applying the CFAA to "a new type of criminal" who affected property that traditional laws did not protect.[112] The 1996 amendment reiterated this need to protect against "new forms of computer crimes."[113] Congress clearly intended to focus on conduct that was not currently addressed by federal or state criminal statutes.[114]

Practical concerns should also limit the application of the CFAA to crimes of computer misuse. The increased utilization of computers to carry out traditional crimes did not require new laws to protect against abuses.[115] Laws addressing these traditional crimes have always been implemented and enforced by the states as part of their police powers.[116] Even when national interests are present, the federal government has already acted on such crimes under

---

110. *See id.* at 1613-15 (discussing the rise of computer crime statutes).

111. H.R. REP. NO. 98-894, at 9-10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695 ("It is obvious that traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes."); *see also* S. REP. NO. 104-357, at 7 (1996) ("This information, stored electronically, is intangible, and it has been held that the theft of such information cannot be charged under more traditional criminal statutes such as Interstate Transportation of Stolen Property, 18 U.S.C. 2314. This subsection 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 [is] protected." (citation omitted)); S. REP. NO. 99-432, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2491 ("To date, computer users for providers of computer services have had to wrestle with a criminal justice system that in many respects is ill-equipped to handle their needs. Computer technology simply does not fit some of the older, more traditional legal approaches to theft or abuse of property. For example, computer data may be 'stolen' in the sense that it is copied by an unauthorized user, even though the original data has not been removed or altered in any way.").

112. S. REP. NO. 99-432, at 2, 1986 U.S.C.C.A.N. at 2480.

113. S. REP. NO. 104-357, at 5.

114. *See also* Field, *supra* note 10, at 835-38 (examining the legislative history and concluding "that the CFAA seeks to capture crimes of computer misuse rather than traditional offenses using a computer").

115. See Kerr, *Cybercrime's Scope*, *supra* note 10, at 1603, 1605-13 (discussing how "traditional crimes committed using computers raise few new issues for criminal law" but noting failures of trespass, theft, and burglary law when applied to computer misuse).

116. *See* Gonzales v. Raich, 545 U.S. 1, 66 (2005) (referencing the state's "traditional police powers to define the criminal law and to protect the health, safety, and welfare of their citizens").

different statutes.[117] Unlike crimes of computer misuse, which provoke concerns about gaps in liability and the consequences of bending ill-formed statutes to address the problem,[118] traditional crimes provide little reason for federal intervention, especially without any expressed congressional intent.[119] Therefore, any interpretation of authorization under the CFAA should reach acts of computer misuse without implicating a wide range of traditional criminal activity already addressed by other laws.

E. The CFAA Should Not Replace Traditional State Causes of Action Against Employees

The CFAA should not create liability in the employment context that overlaps or preempts traditional causes of action applying to employees. These tools include, among others, noncompete provisions, trade secret protections, conspiracy, contract law, and the duty of loyalty. In crafting the CFAA, Congress recognized that broad language could impact state laws of all kinds.[120] It sought to balance federal and state concerns rather than displace state actions, so any interpretation of authorization under the CFAA should not duplicate or replace these laws.[121] Congressional understanding that the CFAA did not reach such actions can also be shown through subsequent statutes, such as the Economic Espionage Act, which imposed federal criminal liability for some trade secret violations.[122] This law would not be necessary if the CFAA had a wide reach.

This purpose also aligns with traditional federalism concerns. Although some might recommend that the CFAA function as federal trade secret protection absent an actual statute,[123] federal laws are typically read to not displace or seize traditional state functions

117. *See, e.g.*, 18 U.S.C. § 1831 (2006) (criminalizing certain trade secret violations that benefit foreign governments).

118. *See supra* note 111.

119. *See supra* note 114.

120. *See* S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482 ("Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area.").

121. *See id.* (discussing the appropriate balance between the federal government and states).

122. 18 U.S.C. §§ 1831-39.

123. *See* Liccardi, *supra* note 3, at 156-57.

without clear congressional intent.[124] State laws for computer wrongdoing also vary widely.[125] Applying the CFAA to these situations would substitute a universal federal cause of action without any congressional consideration of the specific elements of the crimes or any congressional findings about the policy implications.[126] On a more fundamental level, it is hard to see why an employee who provides information to a competitor should be subjected to federal civil or criminal liability for providing information obtained on a computer, when another employee who uses a printed report of the same information could be charged solely under existing state law. Even if the elements of each offense were made equivalent, this would likely lead to an abuse of federal jurisdiction.[127] All of these concerns counsel against imposing liability under the CFAA on employees for actions that have traditionally generated liability under state law.

F. The CFAA Should Create Liability for All Damage to Computer Data

Finally, any effective CFAA interpretation must create liability for all damage to computer data. The original legislation passed by Congress in 1984 prohibited only specified improper access to certain computers.[128] However, when the act was amended in 1986, it contained an additional charge, which the House Judiciary Committee described as a "malicious damage felony."[129] This cause

---

124. *See* Gregory v. Ashcroft, 501 U.S. 452, 460-61 (1991) (holding that a statute will be found to interfere with the traditional balance of power between the federal government and the states only if the statute is "unmistakably clear" in requiring such a result (quoting Atascadero State Hosp. v. Scanlon, 473 U.S. 234, 242 (1985))).

125. For example, California does not enforce most noncompete agreements, unlike many other states that enforce them with certain restrictions. *See* Chan & Rubiner, *supra* note 47, at 25.

126. *See, e.g.*, Field, *supra* note 10, at 845-46 (discussing how application of the CFAA to trade secret violations would lower the requirements for proving such a claim that have developed in states due to valid policy reasons).

127. *See* Boyer, *supra* note 28, at 662-63 (describing the inefficiency resulting from federal courts hearing CFAA claims that overlap with state law).

128. Baker, *supra* note 5, at 64-65.

129. United States v. Morris, 928 F.2d 504, 508 (2d Cir. 1991) (quoting H.R. REP. NO. 99-612, at 7 (1986)).

of action is currently codified as Section 5A.[130] Congress stated when passing the 1996 amendments that this section protects against intentional computer damage by both outside hackers and "malicious insiders."[131] The difference in wording between Section 5A, which focuses on "damage without authorization," and other causes of action, which focus on "access without authorization," reflects the desire that any intentional damage result in liability.[132] Although inclusion of a destruction of property provision within a statute primarily concerned with improper computer access might seem unusual, it reflects congressional intent to account for all computer crime in one statute.[133]

Congress's intention to criminalize all intentional damage to protected computers is clear, but Section 5A also makes sense from a policy perspective. The destruction or damage of property, by employees or others, is a traditional crime; however, computers present particular problems for determining damages that are not necessarily covered by traditional statutes.[134] For example, a virus may limit access to a computer for a period, or slow computer response time, without leaving any permanent effects or altering any information. This sort of damage would not necessarily be covered by a state statute preventing destruction of property, and therefore Congress's imposition of liability on those who cause this type of damage accords with the principles discussed in Part II.D.

---

130. 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008) (penalizing "[w]hoever ... 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"). Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8) (2006).

131. *See* S. REP. NO. 104-357, at 10 (1996) ("This would cover anyone who intentionally damages a computer, regardless of whether they were an outsider or an insider otherwise authorized to access the computer."); *id.* at 11 ("In sum, under the bill, insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.").

132. *Compare* 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008), *with id.* § 1030(a)(4) (2006).

133. *See supra* note 96 and accompanying text.

134. *See supra* notes 111-14 and accompanying text.

III. EVALUATING AGENCY, CONTRACT, AND CODE-BASED INTERPRETATIONS OF AUTHORIZATION

With the six purposes of the CFAA established, the next task is to evaluate each of the interpretations of authorization put forth by courts and academics to see if any approach successfully reaches each goal.[135]

A. Agency

The agency approach to defining authorization focuses on the relationship between the employer and employee, such that an employee who acts against the employer's interests does so without authorization.[136] This approach satisfies, at best, three of the six criteria established for a successful interpretation of the CFAA.

1. Expansive Liability

Interpreting authorization with respect to agency law creates expansive liability under the CFAA, contrary to the first established purpose. The courts that have applied the agency theory have typically been addressing allegations of clear wrongdoing on the part of the employee, such as e-mailing proprietary information to a competitor as in *Shurgard*,[137] or destroying files as in *Citrin*.[138] The implications of this approach, however, go much further. The Restatement (Second) of Agency defines "agency" in such a way that every computer access occurring after an employee acquires an adverse interest is legally actionable; an employee's adverse interest terminates any authority, leaving the employee without authoriza-

135. Just to emphasize the intentions of this exercise, many other purposes can surely be ascribed to the CFAA. The six outlined in Part II are broad provisions with strong support from the legislative history of the statute and are intended to generate as wide a consensus as possible from all sources that have examined the statute, while also focusing on the employment contexts of this Note.

136. *See supra* Part I.A.

137. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000).

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

tion.[139] An employee who has decided to quit for a competitor could thus be liable for checking personal e-mail at work, wasting time, or even just carrying out normal business functions, provided the employer can allege the proper damages. Going further, anyone checking personal e-mail might be civilly or criminally liable.[140] The broad implications of an agency interpretation have caused other courts to interpret the CFAA more narrowly, citing the rule of lenity when deciding between competing interpretations.[141]

2. Broad Coverage of Technological Advances

On the other hand, an agency interpretation clearly allows for significant flexibility in dealing with advances in computer technology. Because agency focuses on the relationship between the parties, it does not limit itself to any technological definitions. If a new method of accessing or altering data develops, the CFAA will continue to impose civil or criminal liability as long as the employer can prove the employee acted against the employer's interest and caused the requisite damage. Differences in the underlying actions do not matter, as authorization terminates as soon as an adverse interest is acquired.

3. Some Employee Liability

The agency definition of authorization also means that the CFAA easily applies to employees in many situations, consistent with the third criterion. In fact, the agency approach may be too broad for employees, eliminating the statutory distinction between "without authorization" and "exceeding authorization."[142] An employee will be acting without authorization after an adverse interest is acquired, but that does not leave many situations that will give

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

140. *See* Lockheed Martin Corp. v. Speed, 81 U.S.P.Q.2d (BNA) 1669, 1675 n.9 (M.D. Fla. 2006) (hypothesizing that checking e-mail on the job could constitute an adverse interest, triggering liability).

141. *See, e.g.*, Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010); Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 934-35 (W.D. Tenn. 2008).

142. *See supra* notes 105-06 and accompanying text.

meaning to "exceeding authorization" under the statute, considering that outsiders have no authorization at all. The Seventh Circuit, applying agency law, admitted this approach renders the difference between the two standards "paper thin."[143] Other courts have struggled with defining what this difference would be,[144] but even if some narrow distinction is made, it would not seem to reflect the clear differentiation that the legislative history seems to ascribe to the terminology.

4. Crimes of Computer Misuse

An agency interpretation of authorization in the CFAA certainly does not limit liability to crimes of computer misuse. This can be demonstrated by some of the cases already discussed. In *Shurgard*, an employer sought recovery when an employee e-mailed proprietary information to a competitor.[145] Sharing such information, whether a violation of the duty of loyalty, trade secret protections, or an employment contract, does not require a computer and indeed usually triggers state causes of action.[146] Similarly, in *NCMIC Finance Corp. v. Artino*, an employer accused a former employee of taking information with him to his new job and using it to compete for customers.[147] These are not offenses arising out of the development of computer technology, nor do they require new laws to provide protection for the information. These are simply traditional crimes being carried out utilizing computers, not crimes of computer misuse. An agency approach fails to make this distinction.

5. Leave State Causes of Action Undisturbed

Because the agency approach covers traditional crimes, it causes serious conflicts with traditional employment causes of action, many of which have not been seriously examined by the courts. The first

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

144. *See, e.g.*, *Speed*, 81 U.S.P.Q.2d (BNA) at 1674 n.7.

145. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000).

146. See, for example, the Virginia Uniform Trade Secrets Act. VA. CODE ANN. § 59.1-336 to -343 (2006).

147. NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1061 (S.D. Iowa 2009).

is in the area of trade secret protections. The Uniform Trade Secrets Act, the basis of most state trade secret laws, only protects information that derives economic value from not being generally known and that an employer attempts to keep secret.[148] Typically, the requirements are even more stringent when an employee misuses confidential information and reflect policy choices by lawmakers between protecting employers and maintaining a mobile workforce.[149] Congress has passed a statute protecting some trade secrets, but it also has stringent standards and omits any civil cause of action.[150] Applying an agency interpretation to the CFAA, however, allows employers to seek civil or criminal remedies against employees who distribute information without having to meet these higher standards. It does not require any proof of trade secrets or misuse of the information, nor is there any requirement of secrecy.[151] It also provides greater remedies than most state statutes[152] and would seem to render the additional federal statute largely superfluous. Agency thus allows employers to bypass state law and policies on trade secrets when the information is acquired by an employee via a computer.

An agency approach can cause similar problems with noncompete agreements and employment contracts. States take different approaches to noncompete agreements, often refusing to enforce agreements that are unreasonably restrictive in geographic scope, practice area, or duration.[153] In California, for example, most noncompete agreements will not be enforced in state courts.[154] Here again, however, federal courts using agency law to interpret the CFAA will subject employees in these states to criminal and civil liability for actions taken after an adverse interest is acquired, even if such action would be permissible under a confidentiality or noncompete agreement, or absent any agreement at all.[155]

148. UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 537 (2005).

149. *See* Field, *supra* note 10, at 845.

150. 18 U.S.C. §§ 1831-39 (2006).

151. Chan & Rubiner, *supra* note 47, at 25-26.

152. *Id.*

153. *See generally* 104 AM. JUR. PROOF OF FACTS 3D *Enforceability of Covenant Not To Compete* § 3 (2008).

154. Chan & Rubiner, *supra* note 47, at 25.

155. *Id.* at 25-26.

Agency law may also cause unforeseen consequences and interactions with other charges typically brought by employers against disloyal employees. For example, because agency law requires the employee to acquire an adverse interest to terminate authorization, many of these cases brought under the CFAA also allege a civil conspiracy against the ex-employee and the new employer.[156] One of the most common defenses to conspiracy is the doctrine of intracorporate immunity, which is also based on agency law.[157] In simple terms, the doctrine holds that a principal cannot conspire with its agent, and therefore conspiracy charges cannot be brought against a corporation and its employees.[158] Courts applying agency interpretations to the CFAA, in cases including *Citrin* and *Shurgard*, have held that no agency relationship exists between the employer and employee after the employee acts against the employer's interests.[159]

This reasoning could present two potential problems. First, conspiracy charges may now be viable for outsiders against the employer and its employee for performance of normal job duties, because the agency relationship shielding the company from such a charge may have terminated. Second, in situations in which an employee acts at the behest of a competitor before leaving for a new job, the former employee and his new company could assert that the employee acted as an agent of his new employer, and thus try to invoke the doctrine as a defense. Thus, when an employee acts on behalf of a competitor, such as by e-mailing confidential information, this agency interpretation of authorization potentially could allow recovery under the CFAA but at the same time prevent any successful conspiracy charges. These problems are just some of the many examples of how the wide scope of the agency approach causes many consequences that have neither been addressed by the courts

156. *See, e.g.*, Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378, 384 (E.D. Pa. 2009) (charging violations of the CFAA and civil conspiracy, among others); Vurv Tech. L.L.C. v. Kenexa Corp., No. 1:08-cv-3442-WSD, 2009 WL 2171042, at *2 (N.D. Ga. July 20, 2009) (same).

157. Robin Miller, Annotation, *Construction and Application of "Intracorporate Conspiracy Doctrine" as Applied to Corporation and Its Employees—State Cases*, 2 A.L.R. 6TH 387 (2005).

158. *See, e.g.*, Charles E. Brauer Co. v. NationsBank of Va., N.A., 466 S.E.2d 382, 387 (Va. 1996) ("[A] conspiracy was a legal impossibility because a principal and an agent are not separate persons for purposes of the conspiracy statute.").

159. *See supra* Part I.A.

adopting the interpretation nor reflected in the congressional discussions.

6. Liability for Damage to Computer Data

Turning to the last criterion, an agency interpretation defines Section 5A, dealing with damage to a computer, in a way that punishes employees and outsiders regardless of their status or permission to access the affected information. Any intentional damage or destruction of information will be against the employer's interest and terminate authorization. Therefore such damage will be "without authorization" under Section 5A and will impose liability on employees and outsiders alike.[160]

In sum, an agency approach to interpreting "authorization" within the CFAA poses many problems, mostly as a result of its broad implications. Such an interpretation reaches traditional crimes as well as crimes of computer misuse, with the result that many long-standing state laws are seriously affected or bypassed. It does not provide a clear difference between actions without authorization and actions exceeding authorization, and the wide range of actions classified as without authorization makes all causes of action in the CFAA potentially applicable to most cases. The statute imposes broad criminal liability as well. An agency approach simply does not succeed in carrying out the outlined purposes of the CFAA.

B. Contract

The contract approach to the CFAA looks to an agreement or other policy, such as an employment contract or terms of service, to determine the presence and scope of authorization given by a computer owner to a user.[161] However, the contract approach, like the agency approach, does not satisfy all of the purposes outlined for the enactment and application of the CFAA.

160. Recall that Section 5A imposes liability when someone "intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008).

161. *See supra* Part I.B.

1. Expansive Liability

Perhaps most importantly, a contract interpretation of the CFAA leads to broad, potentially limitless, liability. A contract approach to defining authorization puts the power of defining liability in the hands of the computer owner drafting the contract or corporate policy.[162] In the case of an employee, this means the employer would have the ability to define what uses of a computer would be authorized. Any actions, such as reading e-mail, checking college basketball scores, or simply being inefficient, could be contractually defined as a violation of the statute. Unlike typical employment contracts, a breach would invoke criminal liability as well. Legislatures and courts often have placed limits on the enforceability of employment contracts, such as requiring noncompete agreements to be reasonable.[163] The contract approach to the CFAA has no such inherent limits; an employer could create federal jurisdiction for any dispute it could anticipate that involved a computer, rendering the approach far broader than the purpose of the statute. If a court instead tried to draw limits on permissible terms without any discernable guidance from Congress, it would only compound the confusion concerning the definition of "authorization" under the CFAA, leaving employees to toil under their employer's restrictions with an indeterminable risk of civil and criminal liability for any violation.

2. Broad Coverage of Technological Advances

The broad leeway provided by the contract approach also allows the statute to adapt to advances in computer technology, but unlike the agency approach, it will not occur without affirmative action. Because the drafter of the contract is free to define the terms of authorization, new technological concerns can be added and defined within the terms of new contracts or amendments. This places a burden on the parties, because unanticipated technological advances may create gaps in protection by preexisting agreements. The trans-

162. *See supra* notes 59-60 and accompanying text.
163. *See supra* notes 153-54 and accompanying text.

action costs this approach places on computer owners to protect their information might weigh against this purpose of the statute.

3. Some Employee Liability

The contract approach may impose some liability on employees, depending on the terms of the contract. This flexibility allows for a differentiation in meaning between "without authorization" and "exceeding authorization" under the statute. An agreement between the employer and employee can define the computers that are considered inaccessible and thus would be accessed without authorization, while contractually prohibited uses of an accessible computer would be in excess of authorization. Similarly, persons who had not entered an agreement with a computer owner either could be acting without authorization or potentially be governed by the contents of general terms of services.[164] In this way, a contract approach would allow, but again not require, the type of employee liability intended by the statute.

4. Crimes of Computer Misuse

The onus a contract approach puts on the computer owner to define acceptable uses causes potential problems with the CFAA's purpose of addressing computer misuse. Employers of course could contract to impose liability only when an employee misuses a computer. However, employers could also draft contracts that define authorization such that traditional crimes, such as trade secret misappropriations, also trigger violations of the computer contract, creating federal liability. Because the parties would have the power to define the limits of liability, the statute could not be restricted to reaching computer misuse alone.

164. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 245-46 (S.D.N.Y. 2000) (applying general terms of use posted on a publicly accessible web page as the contractual document governing the authorization of access by any user).

5. Leave State Causes of Action Undisturbed

Contract-defined liability may also conflict with established statutes, as employers would benefit from making the contracted provisions as broad as possible. Any breach by the employee would allow the employer to bring civil charges in federal court under the CFAA and could lead to criminal charges. A contractual approach thus has the same problem as an agency approach, as enforcement can easily conflict with traditional state laws.

6. Liability for Damage to Computer Data

A contract approach to interpreting Section 5A of the CFAA would also permit, though not require, computer owners to impose liability on anyone who intentionally damaged a computer, consistent with the purposes of the statute. Once again, the impetus would be on the employer to draft the contract in such a way to prohibit damage to the system. This requirement would seem to contradict congressional intent for Section 5A to definitively reach all intentional computer damage.[165] In this situation, a contractual reading could very well be underinclusive.

A contractual approach to interpreting authorization in the CFAA would initially seem to accord with the legislative history, which indicated that private industry, and not the government, should have primary control in limiting computer crime.[166] Overall, however, the contractual approach goes too far, as it gives unbridled discretion to employers and computer owners to define the reach and application of federal civil and criminal liability. This discretion permits application of the CFAA in ways that directly contradict the purposes of the statute laid out in Part II, while also failing to ensure that other purposes will necessarily be fulfilled.

---

165. *See supra* Part II.F.

166. S. REP. NO. 99-432, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2481 ("[T]he primary responsibility for controlling the incidence of computer crime falls upon private industry and individual users, rather than on the Federal, State, or local governments.").

C. Code-Based

Having ruled out agency and contractual definitions, only the code-based approach remains. The code-based approach determines authorization by looking at whether a user has programmed permission to access certain information or must bypass security protections.[167] Users act without authorization when they have no encoded right to use a protected computer, and users with some usage rights exceed authorization when bypassing security.[168] The code-based approach is more successful than either agency or contract interpretations, but it still does not accomplish all of the purposes of the CFAA.

1. Expansive Liability

A code-based approach does prevent a broad reading of the CFAA. It restricts statutory protections to information that is already protected by the computer owner through the use of passwords or other security measures. This self-help focus reflects congressional intent that the private sector, and not the government, take responsibility for protecting against computer crime.[169] Such an approach also gives a computer owner the power to decide what information the statute protects, similar to the contract approach, by choosing what information to restrict. The key difference, however, is that the presence of such encoding will require all users who violate the statute to have performed the same underlying action, namely, bypassing the implemented protection. Therefore, unlike with contractual or agency approaches, there will be at least one common element in all cases imposing civil or criminal liability.

2. Broad Coverage of Technological Advances

This narrower focus does not result in the CFAA being inflexible to changes in technology and computer crime. Because authorization is based on the presence of security provisions, the method or

167. *See supra* Part I.C.
168. *See supra* note 63 and accompanying text.
169. *See supra* note 166 and accompanying text.

technique violators use to bypass the system does not matter. If new methods of affecting computers develop, such as the computer virus in the 1980s,[170] liability will attach so long as the computer or information affected was not generally accessible by the public. In this way, a code-based approach reflects the congressional mandate.[171]

3. Some Employee Liability

Employees are still subject to liability under the CFAA with a code-based approach. Employees who do not have a password or other ways of accessing a computer will operate without authorization if they bypass security, while employees properly using a computer can still incur liability if they defeat security provisions to reach information that had been restricted from their use.[172] This prevents employees from incurring any liability from normal business operations or as a result of accidental overstep, as Congress intended,[173] but does not provide blanket protection for all employee actions.

4. Crimes of Computer Misuse

Employees remain liable for misuse when exceeding code-based protections because the code-based interpretation of authorization places an act of computer misuse at the core of any violation. By requiring information or computers to be protected by coding or other restrictions, a code-based interpretation reaches only individuals who break or bypass these computer protections.[174] Such an action is precisely the sort of computer misuse Congress sought to prevent in enacting the statute, as it is a crime that has only arisen due to the influx of computers into modern society and is not

170. *See generally* Robert J. Malone & Dr. Reuven R. Levary, *Computer Viruses: Legal Aspects*, 4 U. MIAMI BUS. L.J. 125, 126-40 (1994).

171. *See supra* Part II.B.

172. *See supra* note 63 and accompanying text.

173. *See supra* note 86 and accompanying text.

174. *See supra* note 63 and accompanying text.

adequately addressed by laws concerning larceny, trespass, or other traditional crimes.[175]

5. Leave State Causes of Action Undisturbed

The nature of a code-based approach prevents it from supplanting other traditional employment actions, such as trade secret protections, because it requires a distinct element of computer wrongdoing to impose liability, rather than the mere utilization of the computer. Returning to the example of two employees who share trade secrets, one by way of a computer report and one from a printout,[176] there is no additional liability imposed by a code-based approach on the computer user. To be subject to liability, the user would perhaps need to break through a password system, an action equivalent to breaking into a locked file room to steal the printed report, which would also impose increased liability. In this way, a code-based approach succeeds in accomplishing the first five purposes of the CFAA outlined in this Note.[177]

6. Liability for Damage to Computer Data

Unfortunately, even a code-based approach is not completely successful. The last purpose reflects congressional intent that the statute reach all instances of intentional damage to protected computers.[178] Applying a code-based interpretation of authorization to Section 5A, which imposes liability on anyone who "intentionally causes damage without authorization,"[179] simply does not create this result. A code-based reading of Section 5A would impose liability only on someone who bypasses security or passwords to cause damage, as coding must normally prevent a user from carrying out

175. *See supra* Part II.D.

176. *See supra* text accompanying notes 126-27.

177. *See supra* Parts II.A-E.

178. *See supra* Part II.F.

179. 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008) ("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 [shall be liable].").

the action.[180] A person intentionally damaging a computer who had coded authority to carry out the action would not violate the statue, contrary to the statute's purpose.[181] At least one commentator has noticed this "arguable flaw" in the language of the statute and recommended interpreting "without authorization" in Section 5A to mean "without permission."[182] Interpreting "without authorization" differently in different sections of the CFAA, as suggested, would be contrary to general rules of statutory interpretation.[183]

More importantly, even interpreting authorization in Section 5A as "without permission" rather than applying a code-based approach would not satisfy the purposes of the statute. The underinclusiveness of either a code-based interpretation of Section 5A or an interpretation of "without permission" may best be demonstrated by an example. *International Airport Centers, L.L.C. v. Citrin*, the Seventh Circuit case discussed in Part I.A, provides an appropriate fact pattern.[184] In *Citrin*, the employer accused a former employee of destroying information on his laptop before returning it to the company after he decided to quit.[185] The laptop contained no code-based protections to prevent destruction of the information, and the employee's contract instructed him to "return or destroy" information on the laptop at his termination.[186] Setting aside the court's discussion of agency law, the employer alleged intentional damage, the exact situation for which Congress intended liability.[187] However, a code-based interpretation of "without authorization" would not impose liability, because the employee had security

180. *See* Kerr, *Cybercrime's Scope*, *supra* note 10, at 1646 ("Regulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act, at least absent circumvention.").

181. *See supra* Part II.F.

182. *See* Kerr, *Cybercrime's Scope*, *supra* note 10, at 1661 (arguing for a code-based approach in interpreting the CFAA with the exception of Section 5A).

183. *See* Estate of Cowart v. Nicklos Drilling Co., 505 U.S. 469, 479 (1992) ("This result is contrary to the basic canon of statutory construction that identical terms within an Act bear the same meaning.").

184. 440 F.3d 418 (7th Cir. 2006).

185. *Id.* at 419.

186. *Id.* at 419, 421.

187. *See* S. REP. NO. 104-357, at 10 (1996) (discussing the portion of the CFAA currently encoded as Section 5A and stating "[t]his would cover anyone who intentionally damages a computer, regardless of whether they were an outsider or an insider otherwise authorized to access the computer").

clearance sufficient on the laptop to delete the information.[188] Similarly, redefining "without authorization" under Section 5A alone to mean "without permission" would also not impose liability.[189] The employee had explicit permission under his employment contract to delete the information. Liability for Section 5A must depend on the intentions of the employee, not permission to undertake the underlying actions.

The underinclusiveness of a code-based interpretation of authorization in Section 5A leaves no approach that satisfactorily meets all of the purposes of the CFAA. It seems clear that a code-based approach satisfies most of these purposes, but fails when applied to the "malicious damage felony" cause of action in Section 5A. This failure is essentially a direct result of Congress's omission of a definition for "authorization" within the statute. Without the benefit of a consistent definition, Congress included "without authorization" in different portions of the statute, failing to distinguish between the types of actions taken by computer users and the intentions of the users.

IV. PROPOSED AMENDMENT TO THE CFAA

In order to meet the purposes of the CFAA established in Part II and eliminate the conflict between the use of "without authorization" in Section 5A and other portions of the statute, this Note proposes that Congress amend the CFAA. This amendment would replace the language in Section 5A with the following: "Whoever ... knowingly *and with intent to defraud*, causes the transmission of a program, information, code, or command, and as a result of such conduct, *intentionally causes damage to a protected computer* [shall be liable]."[190] The first portion of the proposed amendment, requiring knowledge and an intent to defraud, parallels the beginning of the current Section 4 of the CFAA and would be interpreted in the

188. *See supra* note 63 and accompanying text (discussing this interpretation).

189. *See Citrin*, 440 F.3d at 419, 421.

190. Compare this proposal with the current language of 18 U.S.C. § 1030(a)(5)(A) (Supp. II 2008) ("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 [shall be liable].").

same way.[191] "Defraud" in Section 4 has been held to mean "wronging one in his property rights by dishonest methods or schemes,"[192] so the amended Section 5A would reach intentionally dishonest actions. The second change in the statute occurs at the end, where "without authorization" is removed from the language *entirely*, eliminating the conflict discussed in Part III.C.6. The remainder of the amendment follows the language of the current Section 5A.

The benefits of this change are apparent. The amended Section 5A would become the malicious damage provision that Congress intended and courts have sought to impose, as it applies to anyone acting with the requisite intent. Rather than focusing on how the user gained access to the information, the statute would penalize employees based on the improper reasons underlying their actions and the resulting damage. Section 5A would represent a completely different theory of liability from Sections 2, 4, and 5B-C. More importantly, by removing the authorization language, the entire CFAA could be subjected to a code-based interpretation of authorization that will fulfill the remaining purposes of the statute. A code-based approach to the amended CFAA would limit expansive liability while still allowing for changes in technology, and would subject employees to liability for crimes of computer misuse without interfering with traditional state causes of action.[193] This result can be seen by applying the amended statute to some of the fact patterns that have already been discussed.

First, the amended CFAA would impose liability on an individual who used a computer for which he had been given log-in information to launch a computer virus infecting other computers. Such a user would be liable under Sections 5B-C, because the virus circumvents security protocols to infiltrate the additional computers, constituting

---

191. *See* 18 U.S.C. § 1030(a)(4) (2006) ("Whoever ... knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [shall be liable], unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.").

192. NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1062 (S.D. Iowa 2009). The court also referenced other equivalent interpretations of the statute applied in other cases. *Id.* The court went on to hold that an employee who used customer lists for his own personal gain violated Section 4. *Id.* at 1062-63.

193. *See supra* Part III.C.

access without authorization.[194] If the individual intended to infect the other computers, purposefully interfering with property rights, and damaged the computers, the person would also be liable under the amended Section 5A. This is the fact pattern from *United States v. Morris*, in which the Second Circuit upheld the defendant's conviction.[195] This result is important, as it is the only CFAA case for which there is confirmed congressional approval of the verdict.[196]

The amended CFAA would also impose liability on a defendant who, after deciding to quit his employment to work for a competitor, deleted from his laptop the only copies of company information, as well as deleting potential evidence of disloyalty. Liability would attach under the amended Section 5A, because the damage to information on the computer was carried out under an intentional plan to deny the company of its interest in the data and conceal potentially illicit activities of the employee. There would be no liability under Section 2C, Section 4, or Sections 5B-C, because the information existed on the employee's computer, to which he had full access without any coding restrictions.[197] This is the fact pattern from *International Airport Centers, L.L.C. v. Citrin*.[198]

The proposed language would not impose liability on a former employee accused of creating a computer program to glean pricing information from his employer's website for the purpose of undercutting those prices at a competing company, even if the employee violated a confidentiality agreement about sharing technical information with a competitor. The information was available on a public website and not protected by any coding, so no liability could arise under Section 2C, Section 4, or Sections 5B-C.[199] The program also

194. *See* 18 U.S.C. § 1030(a)(5)(B)-(C) (Supp. II 2008) ("[Holding liable] [w]hoever ... intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.").

195. 928 F.2d 504, 505 (2d Cir. 1991); *see also supra* notes 22-26 and accompanying text.

196. *See supra* note 95.

197. *See supra* notes 29-33 and accompanying text.

198. 440 F.3d 418, 419 (7th Cir. 2006); *supra* notes 43-46 and accompanying text. The result of applying the amended Section 5A differs in part from the Seventh Circuit's decision, which cited agency law. The Seventh Circuit held that the defendant could be charged under the current Section 5A as well as Sections 5B-C because the court determined the employee's access occurred without authorization. *Citrin*, 440 F.3d at 420-21.

199. *See supra* notes 29-33 and accompanying text.

did not cause any damage to the computer or data, preventing any liability under the amended Section 5A.[200] This conclusion directly contradicts the First Circuit's ruling in *EF Cultural Travel BV v. Explorica, Inc.*, a case decided based on a contractual approach.[201] This difference in result occurs not because of the amended Section 5A, but instead due to the shift from a contractual approach to a code-based interpretation of authorization throughout the rest of the statute.

Finally, the amended CFAA would not impose liability on a former employee who copies confidential information or trade secrets off of his computer or e-mails such information to a competitor. So long as the employee is using his own computer and is not prevented from accessing the information by security protections, there is no violation of Sections 2C, Section 4, or Sections 5B-C, because no access occurred without authorization nor in excess of authorization.[202] Likewise, no liability attaches under the amended Section 5A if there is no damage or destruction of the information when it is copied. This is the fact pattern seen in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, in which the court held that the plaintiff had stated a claim under an agency theory.[203] This is also the general fact pattern faced in *Lockheed Martin Corp. v. Speed*, in which the court rejected the agency approach in dismissing a similar claim.[204] This example again shows the narrowing of liability for former employees under a consistent code-based approach to interpreting authorization. Use of a computer to commit a traditional employment crime, such as disclosing trade secrets, would no longer impose vastly different liability depending on whether such information came from a computer or from a file drawer.

---

200. If the program caused the site to slow down, and the employee knew this would happen, liability could potentially arise for damages under the amended Section 5A. However, those allegations were not made in the *Explorica* case.

201. 274 F.3d 577, 583-84 (1st Cir. 2001); *see also supra* notes 52-54 and accompanying text.

202. *See supra* notes 29-33 and accompanying text.

203. 119 F. Supp. 2d 1121, 1127-29 (W.D. Wash. 2000); *supra* notes 40-42 and accompanying text.

204. 81 U.S.P.Q.2d (BNA) 1669, 1670-71 (M.D. Fla. 2006); *supra* notes 67-70 and accompanying text.

CONCLUSION

The scope of federal protection under the CFAA has expanded as computers become more common and indispensable in the home and in the workplace. Courts have struggled with interpreting the CFAA as employers have taken advantage of its protections to pursue civil charges against former employees who used their computer access to act against their employers' interests.[205] Courts have applied a variety of interpretations to the statute with extremely different consequences for defendants. These differences are especially important as the statute provides for criminal liability as well as civil remedies.[206]

The development of agency, contract, and code-based approaches to interpreting authorization under the CFAA may have resulted from imperfections in the language of the statute itself. As Part III demonstrated, none of the interpretations of authorization employed by the courts can consistently satisfy the basic purposes of the CFAA that this Note puts forth. A code-based interpretation comes closest, but it does not render Section 5A broad enough to reach all intentional damage to protected computers.[207] To allow for a consistent reading of the statute fulfilling all of these purposes, Section 5A should be amended to remove "without authorization" and focus on the intent of the person damaging a protected computer. Such a change would reflect the history of the statute and allow for a consistent code-based interpretation of the rest of the CFAA.

Employers would likely oppose the amendment and interpretation advanced by this Note, because employers benefit from a broad reading of the CFAA that often provides an easier path to recovery than traditional state remedies.[208] Critics may also legitimately argue that employing a code-based approach is too restrictive because it does not protect computerized property against trespass and other violations as strongly as real world concepts,[209] and it

205. *See supra* note 47 and accompanying text.
206. *See supra* notes 5-6 and accompanying text.
207. *See supra* Part III.C.6.
208. *See supra* note 47 and accompanying text.
209. *See* Winn, *supra* note 60, at 1419-22.

places the burden of protection on computer owners. These are certainly important considerations; however, they are likely less important in the given context of employer-employee relationships.

Employers' property is necessarily open and available to their employees, and employers are more likely to have the technological and financial resources to place restrictions on computerized access to information than typical computer owners. Employers are also not left without recourse for the misuse of their information; traditional causes of action, such as trade secret protections and the common law duty of loyalty,[210] will continue to provide remedies for resulting damages. Indeed, employers may receive ancillary benefits from further protecting their information, such as bolstering secrecy claims in trade secret litigation.[211]

As with any call for legislative action, the underlying problem will remain until Congress acts. The court in *Black & Decker, Inc. v. Smith* provided a well-reasoned example of how to deal with the present wording of the CFAA.[212] The court, citing the statute's plain meaning, refused to find liability based on actions of an employee subsequent to the computer access.[213] It also distinguished the causes of action relating to access without authorization from Section 5A, in which the court noted Congress intended to reach all intentional damage.[214] In this way, the court arrived at an end result in line with the purposes of the CFAA.[215] Courts can evaluate future cases similarly while waiting for congressional action. Of course, relying on courts to reach this result based on the "plain meaning" of the statute, rather than using a definitive interpretation such as the code-based approach, will likely lead to further inconsistency, as courts obviously continue to disagree about the statute's meaning. The *Black & Decker* court also necessarily ascribed different meanings to authorization throughout the statute

210. *See supra* note 146 and accompanying text.

211. As secrecy is one of the traditional elements of a trade secret, by placing information behind computerized security a corporation would also create evidence of this element. *See* Virginia Uniform Trade Secrets Act, VA. CODE ANN. § 59.1-336 (2006) (defining trade secrets to require, as a requisite element, "efforts that are reasonable under the circumstances to maintain [the information's] secrecy").

212. 568 F. Supp. 2d 929, 933-34 (W.D. Tenn. 2008).

213. *Id.* at 934-35.

214. *Id.* at 937.

215. *See supra* Part II.

to reach this result, seemingly contradicting the presence of a "plain meaning" and running contrary to general construction preferences.[216] Still, *Black & Decker* can provide a guide to interpreting the CFAA in employer-employee disputes until the statute is amended again.

Finally, it should be noted that the proposed amendment does not address all of the interpretive questions associated with the CFAA. There remain notable debates about the types of damages that are required under the statute, the meaning of access, and other terms and applications.[217] Employers and employees are not the only subjects of the statute, and although its application to hackers and other outsiders has been less controversial, hackers and outsiders remain the original focus of the legislation.[218] That being said, the modest changes in language and interpretation herein should not greatly affect the use of the CFAA in those situations and would lead to more consistent results better tailored to the statute's underlying purposes. Congressional inaction, on the other hand, will likely cede the issue to the Supreme Court in the coming years.

Garrett D. Urban[*]

216. *See supra* note 183.

217. *See, e.g.*, Boyer, *supra* note 28, at 691-702 (discussing different interpretations of damages and loss under the CFAA).

218. *See supra* note 101 and accompanying text.

* J.D. Candidate 2011, William & Mary School of Law; B.A. 2006, Duke University. Many thanks to Katherine Lunney and my family for their patience, and to Brandon Murrill and the rest of the Law Review staff for their efforts and expertise.