AUTHORIZED: THE CASE FOR DUTY OF LOYALTY SUITS AGAINST FORMER EMPLOYEES UNDER THE COMPUTER FRAUD AND ABUSE ACT

Christopher Dodson[*]

ABSTRACT

The Computer Fraud and Abuse Act (CFAA) includes a provision for civil suits against anyone who engages in certain computer-based acts "without authorization." However, the statute leaves "authorization" conspicuously undefined. Agency law provides a legal framework for an employer to authorize an employee to act on its behalf. An employee owes a duty of loyalty to an employer under agency law. Breaching the duty of loyalty can cause an employee's authorization to be terminated. Some employers have filed suit under the CFAA against former employees who removed or deleted computer files after violating the duty of loyalty. The employers claim the breach of the duty of loyalty terminated the employee's authorization to use the employer's computer systems. The circuits are split over the issue of whether an employee's authorization under the CFAA terminates when the employee breaches the duty of loyalty. This Note reaches the conclusion that duty of loyalty violations do terminate an employee's authorization, and proposes a four-part analysis for determining whether an employee has accrued CFAA liability.

TABLE OF CONTENTS

[*] J.D. Candidate, 2013, Earle Mack School of Law at Drexel University; B.A., 1995, Fordham University. I would like to thank my wife, Rebecca, and daughter, Julia Violet, for their patience.

INTRODUCTION

The bluish light from a computer monitor reflects in his eyes as he begins to secretly copy the data. Byte after byte stream across the wire from the secured server through routers, switches, and cables before being reassembled as files on his computer. He moves the files immediately to a thumb drive, deleting the temporary copies from his computer to cover his tracks. He got in and out of the system without anyone noticing; the company's confidential data is his. Who is he? A hacker working for the Russian mob?[1] A hacktivist looking to expose the company's secrets online?[2] Actually, he is a trusted employee taking valuable proprietary information before he quits. And he will be long gone before anyone figures out he has the data.

A survey of computer security professionals found the average annual cost of responding to computer security incidents was nearly $290,000 per business.[3] One tool potentially available to businesses in combating security incidents is the Computer Fraud and Abuse Act (CFAA). The CFAA, while primarily a criminal statute, provides a civil cause of action,[4] which enables anyone who suffers a loss in excess of $5,000 due to a violation of its provisions to sue.[5]

In fact, some businesses have brought CFAA suits against former employees who either deleted data or copied valuable electronic information in the process of joining a competitor. These suits are controversial, in part because they do not involve situations where employees hacked into systems to which they did not have access, but,

1. *See, e.g.*, David Goldman, *The Cyber Mafia Has Already Hacked You*, CNN MONEY TECH. (Jul. 27, 2011, 9:45 AM), http://money.cnn.com/2011/07/27/technology/organized_cybercrime/index.htm ("The Russian Mafia are the most prolific cybercriminals in the world.").

2. *See, e.g.*, Loz Kaye, *'Anonymous' Hacktivists Expose the Intelligence Gap*, THE GUARDIAN (Jan. 9, 2012, 1:22 PM), http://www.guardian.co.uk/commentisfree/2012/jan/09/anonymous-hacktivist-expose-intelligence-gap; Damon Poeter, *50 Days of Mayhem: How LulzSec Changed Hacktivism Forever*, PC MAG. (June 28, 2011), http://www.pcmag.com/article2/0,2817,2387716,00.asp.

3. Robert Richardson, *2008 CSI Computer Crime & Security Survey*, COMPUTER SEC. INST. 16 (2008), http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf.

4. 18 U.S.C. § 1030(g) (2006).

5. *Id.* § 1030(c)(4)(A)(i)(I).

rather, they involve situations where the employees were authorized to use the systems to perform their duties.[6]

The basis for overcoming the employee's existing authorization is the subject of the controversy and this Note. Agency law creates the legal framework that allows an employee to act on behalf of an employer.[7] Under agency law, an employer authorizes an employee to act as its agent, and, in return, the employee has a duty to act loyally toward the employer.[8] An employee can breach the duty of loyalty by failing to notify his employer that he has agreed to aid a competitor while still employed.[9] When an employee violates the duty of loyalty, the agency relationship with his employer terminates.[10] Employers argue this termination removes the employee's authorization to access the employer's resources as a matter of law at the time the violation occurs.[11] According to the employers, if the employee then modifies or removes his employer's data on behalf of the competitor, he does so without authorization and is liable under the CFAA's civil cause of action.[12]

The agency approach has had mixed results in the courts and has resulted in a circuit split. The First, Fifth, and Seventh Circuits have ruled squarely in favor of using agency law to determine CFAA authorization;[13] however, the Ninth Circuit, along with District Courts in the Third, Fourth, Sixth, Tenth, and Eleventh Circuits have ruled against the use of agency law.[14] This Note takes the position that the use of agency law to terminate an employee's authorization is valid for purposes of the CFAA.

In Part I, Section A of this Note examines the text of the CFAA, focusing on the provisions defining violations and the civil cause of action. Part I, Section B explores the legislative history of the CFAA, in particular the Senate reports accompanying the 1986 and 1996 amendments. Part I, Section C examines the duty of loyalty as articulated in the Restatement (Third) of Agency, along with non-CFAA

6. *See, e.g.*, LVRC Holdings, L.L.C. v. Brekka, 581 F.3d 1127, 1128 (9th Cir. 2009); Deloitte & Touche, LLP v. Carlson, No. 11C327, 2011 WL 2923865, at *4 (N.D. Ill. Jul. 18, 2011).

7. *See* RESTATEMENT (THIRD) OF AGENCY § 1.01 (2006).

8. *Id.* § 8.01.

9. *See id.* §§ 8.01, 8.04, 8.11; *infra* Part I.C.

10. *See* RESTATEMENT (THIRD) OF AGENCY § 3.09; *infra* Part I.C.

11. *See infra* Part I.C.

12. *See infra* Part I.C.

13. Obiajulu Okuh, *When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access*, 21 ALB. L.J. SCI. & TECH. 637, 674 (2011).

14. *Id.*

duty of loyalty cases. Part I, Section D discusses other law review articles on this topic. Part I, Section E reviews CFAA cases where courts have ruled both for and against the use of agency law. Drawing on the common comparison of the CFAA to physical trespass, Part I, Section F looks at trespass cases where permission to enter was impliedly revoked based on a person's actions after entering. Part II analyzes the appropriateness of the duty of loyalty in the context of the CFAA and reaches the conclusion that it is valid to use the duty of loyalty under the CFAA. Finally, this Note proposes a four-part analysis for determining whether an employee has liability under the CFAA.

I. RELEVANT SOURCES OF LAW

A. The Computer Fraud and Abuse Act

To understand the CFAA's application in the context of lawsuits by employers, this section walks through the activities proscribed by the CFAA and introduces some important terminology. It then discusses the CFAA's cause of action and what constitutes damage and loss under the Act.

The CFAA defines three violations with direct relevance to employers' suits. The first provides that anyone who accesses a computer "without authorization" or who "exceeds authorized access"[15] and obtains information from a "protected computer"[16] has violated the statute.[17] This provision prohibits merely obtaining information from a protected computer; deleting or modifying data is not within its scope. To trigger a violation, a user must simply read or copy data without appropriate permission. The CFAA neither provides a definition of "without authorization," nor does it offer guidance on how authorization is to be granted or revoked.[18]

15. The CFAA defines "exceeds authorized access" as "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." 18 U.S.C. § 1030(e)(6) (2006).

16. The Act defines "protected computer" as one that is "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *Id.* § 1030(e)(2)(B). Protected means only that a computer is in scope for the CFAA. The statute has no requirement that a computer be "protected" in the sense of being secured by password or other security tool.

17. This violation occurs when one "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." *Id.* § 1030(a)(2)(C).

18. *See id.* § 1030.

The second relevant violation creates liability for anyone who intentionally causes damage to a protected computer without authorization by transmitting a command or program.[19] This involves such actions as deleting or modifying data. Under the language of this provision ("causes damage without authorization"), it is the *action* that must be unauthorized, not the access.[20] Users can delete or modify data as long as it is within the scope of their authorization. Merely accessing or copying data is not sufficient to produce a violation under this provision.

The third violation creates liability for anyone who causes damage and loss (whether intentionally or not) as a result of intentional, unauthorized access of a protected computer.[21] Unlike the previous violation, this provision requires that the access itself be unauthorized, regardless of the subsequent actions by the violator. Because this provision requires only that damage and loss occur subsequent to unauthorized access, it is somewhat analogous to a traditional trespass or burglary violation.[22] Under this provision, the harm can be the actual deletion or modification of data or economic losses resulting from system disruptions or the information technology (IT) response to the discovery of unauthorized access, regardless of whether the violator actually deleted or modified data.

The civil cause of action allows any person,[23] government, or private entity that suffers loss or damage due to a violation of the statute to sue for damages or equitable relief.[24] The cause of action is limited to several factors,[25] of which only one is applicable to employer suits. This provision requires an aggregate loss of $5,000 over a one-year period.[26]

19. Liability attaches when one "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." *Id.* § 1030(a)(5)(A).

20. *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419–20 (7th Cir. 2006) (distinguishing the requirements of the first two provisions).

21. 18 U.S.C. § 1030(a)(5)(C) ("Whoever intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss shall be punished as provided in subsection (c) of this section.").

22. *See infra* Part I, Section F.

23. 18 U.S.C. § 1030(e)(12) ("[T]he term 'person' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.").

24. *Id.* § 1030(g).

25. *Id.* ("A civil action . . . may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).").

26. *Id.* § 1030(c)(4)(A)(i)(I) (requiring "loss to 1 or more persons during any 1-year period . . aggregating at least $5,000 in value").

To put the $5,000 requirement in perspective, consider a scenario where the only cost to the employer was network support staff time in analyzing and responding to the situation. The national median cost of salary and benefits for a network administrator with four to six years of experience is nearly $105,000.[27] At this cost, an employer would have to dedicate nearly 100 employee-hours (almost 2.5 employee-weeks) to reach the $5,000 minimum loss required by the CFAA.[28]

Under the CFAA, damage is "any impairment to the integrity or availability of data, a program, a system, or information."[29] Impairment can be understood as interference with the ability to use a program or system. Interference can occur when a user inappropriately modifies or deletes data or the underlying software. But interference with the use of a system does not necessarily require the modification of software or data.[30] The statute's broad language of "any impairment" encompasses changes to user behavior that may result from the loss of trust in a system or its data, even if the impairment is only temporary while the IT staff investigates the incident. This impairment may impact end users of the system or its administrators.

The statute's approach to loss focuses on allowing victims to recover the IT costs associated with a violation of the statute. Loss is "any reasonable cost," including costs associated with the response to and assessment of the violation and restoration of data.[31] This might involve staff time for investigating the violation, such as reviewing log entries, disabling access, determining what network resources were available to the violator, or restoring historic data if a sufficient length of time had elapsed. It would also include the cost of an outside forensic analysis.

The statute makes lost revenues and consequential damages unavailable to the employer unless there was an interruption of ser-

27. *Network Administrator III*, SALARY.COM, http://swz.salary.com/SalaryWizard/Network-Administrator-III-Salary-Details.aspx (last visited Oct. 20, 2012).

28. *See infra* Appendix: Employee-Hours Calculations.

29. 18 U.S.C. § 1030(e)(8).

30. For example, a structured query language (SQL) injection attack can be used remotely against vulnerable systems to exfiltrate data from a database without any modification to data or code on the system.

31. 18 U.S.C. § 1030(e)(11) ("[T]he term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service . . . .").

vice.[32] It is not clear whether the interruption of service must be the direct result of the violator's actions or whether it can be the result of the efforts to investigate and respond to the violation. Regardless, unless a system was offline for a reason related to the violation, an employer cannot receive consequential damages.

The statute includes neither a definition for authorization nor requirements for granting or terminating it. The absence of any requirements for authorization leaves the door open for other areas of law appropriate to a particular situation to define authorization. For purposes of employment-related situations, that may include agency law. It is reasonable to ask, however, whether Congress ever intended the CFAA to apply to employees. The legislative history provides the likely answer.

B. Legislative History

Because the text of the CFAA does not address the issue of granting or revoking authorization, it is useful to look to the legislative history for guidance. The Senate Judiciary Committee Report on the 1986 CFAA amendments provides some indications of the concerns Congress attempted to address, including the CFAA's potential impact on employees.[33] The report describes computer crime as one of the most serious white-collar offenses.[34] Black's Law Dictionary defines white-collar crime as a "nonviolent crime usually involving cheating or dishonesty in commercial matters."[35] White-collar crime occurs in both government and the private sector and is often related to the scope of employment.[36]

In discussing a provision protecting federal government computers,[37] the report states a goal of not creating criminal liability for government employees whose actions "while technically wrong, should not rise to the level of criminal conduct."[38] To accomplish this goal, the 1986 amendments raised the scienter requirement for

32. *Id.*

33. *See* S. REP. NO. 99-432, at 36 (1986).

34. *Id.* at 2.

35. BLACK'S LAW DICTIONARY 1734 (9th ed. 2009).

36. *White-Collar Crime*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/white_collar/whitecollarcrime (last visited Oct. 20, 2012) ("White-collar crime in a nutshell . . . is now synonymous with the full range of frauds committed by business and government professionals.").

37. *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (2006)).

38. S. REP. NO. 99-432, at 7.

violations from "knowingly" to "intentionally."[39] This requirement would avoid ensnaring government employees who simply exceeded authorized access[40] or those who were acting as whistleblowers.[41] The committee preferred to address such incidents through administrative sanctions.[42] This was in contrast to situations where the employee accessed a computer belonging to another department of the government, a situation that the committee compared to trespass.[43]

When the report discusses non-government computers,[44] it specifically notes that the scienter requirement, "intentional," was the same as for other provisions where it prevented liability for certain behaviors by government employees.[45] The committee provides no indication that it did not expect the provisions to apply to private sector employees in the same way they applied to government employees. Nor did the committee give any indication that Congress intended the CFAA to preempt the normal operation of other laws relating to employees that might be implicated.

While the report provides no information about how the authors expect authorization to be created, communicated, or enforced, the authors provide an example of a situation they wanted to exclude from criminal prosecution, which is instructive. The report describes a situation where a government employee signs onto a computer but mistakenly accesses another user's files without authorization.[46] Because the user is not blocked by technical means from accessing the other user's files but the action is nonetheless unauthorized, it indicates that authorization may take more than one form, including technical restriction and employer policy.

The report also discusses Congress's approach to calculating loss. Loss was not to be limited to direct repairs to a computer, but was to include other expenses, such as loss of use, programming changes, restoration of data, and even losses caused by reliance on modified

39. *Id.* at 5–6.

40. *Id.* at 7.

41. *Id.* at 8.

42. *Id.* at 7–8.

43. *Id.* at 7.

44. *Id.* at 10.

45. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (2006)).

46. S. REP. NO. 99-432, at 6.

data.[47] The focus was on the cost of IT resources allocated by a victim in response to a violation.

The Senate Judiciary Committee Report accompanying the 1996 amendments provides additional insight.[48] It did not view the CFAA as an alternative to other legal theories. Rather, Congress intended the CFAA to work in concert with other federal and state laws.[49] In fact, a violation committed in the context of a violation of other laws was subject to the CFAA's "harshest penalties."[50] It is only a misdemeanor to commit the basic offense of improperly using a computer to obtain information.[51] The violation, however, becomes a felony when a user takes the information to gain a commercial advantage, to gain a private financial benefit, or to commit another crime or tort.[52] The seriousness of the violation depends on "what is planned for the information after it is obtained."[53]

The report uses new terminology that does not appear in the text of the statute but is useful for understanding Congress's intent regarding authorization. An "outsider" is anyone who accesses a computer without authorization,[54] while an "insider" is anyone with authorization.[55] The use of insider blends together people who have access by virtue of being employees and people who are authorized as users of a company's services. Both outsiders and insiders are considered to have committed violations when they intentionally cause damage.[56] But only outsiders face liability for damage caused by reckless or negligent actions.[57] Because unauthorized access by outsiders is an "intentional act of trespass," the threshold for liability is lower.[58] Insiders, however, are protected from inadvertent mistakes and are only liable for deliberately causing damage.

The legislative history shows Congress recognized the potential applicability of the CFAA to employment settings and that the CFAA was to work along with existing laws. Agency law is the area

47. *Id.* at 11–12.
48. S. REP. NO. 104-357 (1996).
49. *Id.* at 8.
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.* at 9.
55. *Id.* at 6.
56. *Id.* at 10.
57. *Id.* at 11.
58. *Id.*

of law by which one party, such as an employer, authorizes another to act on its behalf. Given the lack of detail in the CFAA around authorization, it is not surprising that issues concerning agency law might arise. The next issue to address is the role of the duty of loyalty in agency law and what effect a violation of it would have.

C. Agency Law and the Duty of Loyalty

An agent is anyone empowered to act on behalf of another, including an employee who acts on behalf of an employer.[59] Agency law governs interactions between a principal (the employer) and an agent (the employee), as well as interactions between an agent and a third party when the agent is acting on behalf of the principal.[60] The Restatement (Third) of Agency provides guidance in understanding the current approach to agency law and is often cited by courts.[61] It includes two components that are relevant to the issue of authorization under the CFAA.[62] First, the Restatement defines the contours of the duty of loyalty and how it can be violated. Second, it provides for how an agent's authority is terminated if he violates his duty. When an agent violates the duty of loyalty, his authorization to act on behalf of the principal terminates under agency law.[63] Currently, the circuits are split over the issue of whether a duty of loyalty violation terminates an employee's authorization for purposes of the CFAA.

The duty of loyalty requires that an agent act loyally and for the benefit of the principal in any matter within the scope of the agency relationship.[64] An agent must put the interests of the principal ahead of his own.[65] He may not compete with the principal or assist the principal's competitors.[66] An agent may make preparations to compete following termination of the agency relationship, as long as the

59. RESTATEMENT (THIRD) OF AGENCY § 1.01 (2006); D. GORDON SMITH & CYNTHIA A. WILLIAMS, BUSINESS ORGANIZATIONS 1 (2d ed. 2008).

60. RESTATEMENT (THIRD) OF AGENCY § 1.01; SMITH & WILLIAMS, *supra* note 59, at 1.

61. SMITH & WILLIAMS, *supra* note 59, at 2.

62. The Restatement (Third) of Agency was published in 2006 and will be considered here because it represents the current state of legal thought on agency. The Restatement (Second) of Agency was the active version when Congress passed the CFAA and its relevant amendments.

63. RESTATEMENT (THIRD) OF AGENCY § 3.09.

64. *Id.* § 8.01.

65. *Id.* § 8.01 cmt. b.

66. *Id.* § 8.04.

actions are not otherwise wrongful.[67] But if an agent actually competes with the principal or assists a competitor, he acquires an adverse interest and violates his duty of loyalty.[68] Additionally, an agent cannot use the principal's property in ways that are adverse to the principal's interests.[69] An agent may only use the principal's property on the principal's behalf—not to benefit the agent or a competitor.[70]

The duty of loyalty also sets guidelines for how an agent should use information. An agent may not use the principal's confidential information on his own behalf or that of a competitor.[71] An agent violates the duty of loyalty if he uses the information against the principal's interests, even if the information is not actually revealed to a third party.[72]

The duty of loyalty requires that an agent notify the principal of information that he knows the principal would want to have, particularly when it is material to the agent's duties.[73] An agent need not, however, volunteer plans to compete with the principal after termination of the agency relationship.[74] But, where an agent acquires an actual adverse interest or believes that notifying the principal may negatively impact his adverse interest, he must notify the principal.[75] Thus, if an employee competes on his own against his employer, cooperates with a competitor, or misuses his employer's property or proprietary information in furtherance of a hostile interest and fails to notify his employer, he also violates the duty of loyalty.

The Restatement then addresses the termination of the agency relationship as a result of an agent's violation of the duty of loyalty. An agent's actual authority terminates when circumstances develop from which the agent should reasonably conclude that the principal

67. *Id.*

68. *Id.* § 8.04 cmt. b.

69. *Id.* § 8.05.

70. *Id.* § 8.05(1), cmt. b (explaining the limits on an agent's use of the principal's property).

71. *Id.* § 8.05(2).

72. *Id.* § 8.05 cmt. c.

73. *Id.* § 8.11.

74. *Id.* § 8.04 cmt. c ("In general, an employee or other agent who plans to compete with the principal does not have a duty to disclose this fact to the principal. . . . Nor does an agent's duty to provide facts to the principal as stated in § 8.11 require disclosure to the principal of an agent's competitive plans.").

75. *Id.* § 8.11 cmt. d.

would no longer want the agency relationship to continue.[76] The termination of authority occurs at the time the circumstances change, not when the principal discovers the change.[77] Because agency law terminates the agent's authority "upon the occurrence" of his breach of the duty of loyalty and the agent violates the duty of loyalty by failing to inform the principal, the termination of authority occurs silently without any action or knowledge by the principal.[78] Thus, the termination of the agent's authority lies dormant, with the principal unaware of the change in the legal relationship with its agent until something else occurs, whether it is the agent's actual severance from the principal or the principal discovers the changed circumstances. While the termination of the agent's authority may require later recognition by a court to be put into effect, it occurs as a matter of law at the time the duty of loyalty is violated.[79]

Outside of the CFAA context, courts have held that employees who actively compete against their employers violate the duty of loyalty. In *Stewart v. Kentucky Paving Co.*,[80] the Court of Appeals of Kentucky upheld a judgment against a defendant who used his employer's client list and leads to secure work on the side without his employer's knowledge.[81] The court noted that an employee could neither serve a hostile interest nor use his employer's information in opposition to his employer.[82] Failure to disclose such activities was itself a violation of the duty of loyalty.[83]

Courts have similarly found that employees who use their employer's confidential information on behalf of a competitor violate the duty of loyalty. In *Riggs Investment Management Corp. v. Columbia Partners L.L.C.*, an employee of the plaintiff provided a competitor with detailed information about clients and employees before re-

76. *Id.* § 3.09. An employee has actual authority when the employee "reasonably believes, in accordance with the [employer's] manifestations to the [employee], that the [employer] wishes the [employee] so to act." *Id.* § 2.01.

77. *Id.* § 3.09(2) ("An agent's actual authority terminates . . . upon the occurrence of [the] circumstances on the basis of which the agent should reasonably conclude that the principal no longer would assent to the agent's taking action on the principal's behalf.").

78. *Id.*

79. *See, e.g.*, Riggs Inv. Mgmt. Corp. v. Columbia Partners L.L.C., 966 F. Supp. 1250 (D.D.C. 1997) (ordering defendant to return compensation already received dating back to the beginning of the breach of the duty of loyalty).

80. 557 S.W.2d 435 (Ky. Ct. App. 1977).

81. *Id.* at 436.

82. *Id.* at 438.

83. *Id.*

signing to join the defendant firm.[84] The competitor then used the information to recruit clients and employees away from the plaintiff.[85] The court found that the employee violated his duty of loyalty by failing to act for the sole benefit of his employer in matters related to his employment and acquiring an adverse interest.[86] It noted that employees may make future plans to compete provided they do not engage in unfair acts.[87] By providing confidential information about clients and employees and soliciting employees to join him, the employee violated his duty of loyalty.[88] The court held that the former employee must forfeit all compensation he received from the plaintiff from the date he breached his duty by removing the confidential information until his actual departure from the company.[89] Importantly, the court thus determined that the employee's duty of loyalty violation severed his relationship with his employer as a matter of law at the time of the violation, not when he actually left the company.

An employee also violates the duty of loyalty by providing services to his employer's competitors. In *Cameco, Inc. v. Gedicke*, the defendant was a transportation manager who arranged shipments of his employer's goods on common carriers.[90] He also arranged shipments for a logistics company on the side to supplement his income.[91] This company did not compete with his employer; however, it did provide shipping services for his employer's competitors, and the goods from both companies were commingled during shipment.[92] In upholding the lower court's denial of dismissal, the court observed that duty of loyalty claims require attention to fairness because the underlying facts are so unpredictable.[93] Although the defendant may have violated the duty in a slight and indirect manner, he nonetheless violated it.[94]

Agency law provides for granting and revoking the authorization of one person to act on behalf of another. Authorization can be ter-

84. 966 F. Supp. 1250, 1255 (D.D.C. 1997).
85. *Id.* at 1254.
86. *Id.* at 1264.
87. *Id.* at 1265.
88. *Id.*
89. *Id.* at 1266.
90. 724 A.2d 783, 786 (N.J. 1999).
91. *Id.*
92. *Id.* at 786–88.
93. *Id.* at 789.
94. *Id.*

minated silently if an agent violates the duty of loyalty. While the effects of duty of loyalty violations are well established in other areas of law, some commentators object to this use of agency law under the CFAA.

D. Articles on Terminating Authorization Through Agency Law Under the CFAA

Observers often see the CFAA as bringing the laws of trespass and burglary to computers.[95] Orin Kerr makes this argument in *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, where he traces some of the history leading up to the enactment of the CFAA.[96] He notes that, although variations exist between jurisdictions, the basic contours of common crimes in the physical world are broadly agreed upon.[97] The nature and scope of computer crimes, however, has proven more elusive.[98] While trespassing and burglary are readily understood, the lack of physical demarcations and ambiguity of authorization on a network make it difficult to apply existing statutes to computers.

Prosecutors initially relied on existing property laws, such as trespass and burglary.[99] This proved problematic, however, because the statutes were clearly limited to the physical world and did not cover cyberspace.[100] There was simply no getting around the fact that existing laws required a physical presence.[101] Instead, prosecutors turned to theft laws, which proved to have their own problems when applied to computers.[102] Theft laws require an identifiable piece of property of which the owner has been deprived.[103] Although the property interest in electronic data was clear enough,[104] the issue of deprivation became a problem in many cases.[105] It was

95. *See, e.g.*, Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 935–36 (W.D. Tenn. 2008) (quoting Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 79 N.Y.U. L. REV. 1596, 1617 (2003) and examining the legislative history of the CFAA).

96. Kerr, *supra* note 95, at 1602–17.

97. *Id.* at 1597.

98. *Id.*

99. *Id.* at 1605.

100. *Id.* at 1605–06.

101. *Id.* at 1606–07.

102. *Id.* at 1607–13.

103. *Id.* at 1609.

104. *Id.* at 1610.

105. *Id.*

difficult to identify how an owner was deprived of property in cases where computer files were viewed or copies made.[106] The difficulty and unpredictability of prosecuting computer misuse under existing laws led to sustained calls for statutes designed to address the unique issues presented by cyberspace.[107] One of the laws coming out of this movement was the CFAA.[108]

In *When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access*, Obiajulu Okuh questions whether the CFAA is the appropriate vehicle to address employee information theft or sabotage, asserting that Congress did not intend for the statute to reach employees.[109] According to Okuh, Congress intended for the CFAA to target traditional hacking[110] rather than cases where an employee caused no damage to an employer's electronic system, no harm to a computer's circuitry, and no interruption of service.[111]

While other criminal activities may involve computers,[112] they are not properly within the CFAA's scope.[113] Indeed, Okuh argues that employers should be limited to using other, more traditional tools, such as state trade secret statutes, to reach such activities.[114] Because Congress intended the CFAA to apply the legal concepts of trespass to computers, the necessary inquiry, he argues, is whether the employer granted permission to the employee to enter the virtual confines of a network and its computers, not the nature of the conduct of the employee while in the virtual property.[115]

Okuh offers additional criticisms of the agency-based approach. Congress, Okuh asserts, did not intend access by an authorized user to be actionable merely because his intentions were adverse to the

106. *Id.* (citing United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978)).

107. *Id.* at 1613–16 (citing 18 U.S.C. § 1030 (2006)).

108. *Id.* at 1616.

109. Okuh, *supra* note 13, at 637–38.

110. *Id.* at 645–46 ("Hacking 'includes . . . breaking passwords; creating 'logic bombs;' e-mail bombs; denial of service attacks; writing and releasing viruses and worms; viewing restricted, electronically-stored information owned by others; URL redirection; adulterating Web sites; or any other behavior that involves accessing a computing system without appropriate authorization.'" (emphasis omitted)).

111. *Id.* at 643.

112. *Id.* at 646 ("The Act was not intended to combat traditional torts such as fraud schemes perpetrated by means of the internet, internet gambling, online distribution of prohibited paraphernalia, cyberstalking, or harms caused by other methods other than unauthorized access") (footnote omitted).

113. *Id.*

114. *Id.* at 648.

115. *Id.*

employer.[116] He also criticizes the need to evaluate the subjective intent of the employee to determine whether his authority remained valid.[117] Furthermore, he suggests there is no deterrent value because employees do not fully understand the nature of their agency-based relationship with their employer.[118] Because the situations most likely to produce CFAA suits by employers are analogous to trade secret misappropriation, allowing the suits could also upend existing trade secret jurisprudence by giving employers "recourse to essentially similar relief under a much lower pleading standard."[119] Finally, Okuh questions whether an employee who "view[s] his employer's information in the course of performing his duties on Monday and then develop[s] an anti-competitive intent to use that information on Tuesday" should be subject to a suit under the CFAA.[120]

Having explored the text of the CFAA, the CFAA's legislative history, the nature of the duty of loyalty, this duty's effect on authorization for employees, and objections to terminating authorization under the CFAA subsequent to duty of loyalty violations, this Note next examines the application of the duty of loyalty under the CFAA by the courts.

E. CFAA Cases

Some courts have directly held that violating the duty of loyalty results in an employee's authorization being revoked under the CFAA.[121] The Seventh Circuit, for example, has adopted this approach. In *International Airport Centers, L.L.C. v. Citrin*, the plaintiff sued a former employee who, before resigning to go into business for himself as a direct competitor, deleted all the data on his computer.[122] He used a secure erase program to ensure his employer could not recover the data, which was not backed up.[123] The Seventh Circuit found that the employee likely violated the CFAA despite

116. *Id.* at 647–48.

117. *Id.* at 657.

118. *Id.* at 661.

119. *Id.* at 662.

120. *Id.* at 657.

121. Some cases apply the version of the CFAA that was in effect from November 2, 2002, through September 25, 2008. The current version, which went into effect on September 26, 2008, has no changes relevant to this analysis.

122. 440 F.3d 418, 419 (7th Cir. 2006).

123. *Id.*

appearing to be authorized to use the computer.[124] His authorization, the court noted, terminated as a matter of law when, after engaging in misconduct, he violated the duty of loyalty by destroying the incriminating files and the files belonging to his employer.[125] Under agency law, the authority of an agent is terminated if "he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty."[126]

In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, the court used agency law similarly when an employer sued a competitor under the CFAA after an employee of the plaintiff emailed confidential files to the competitor prior to going to work for it.[127] Relying on the Restatement (Second) of Agency, the court held that the employee lost authorization to access the employer's proprietary information when he became the competitor's agent.[128] The court also pointed to the CFAA's legislative history as an indication that Congress intended for losses from the cost of IT resources to be incorporated in the consideration of damage caused by proscribed conduct.[129] Even where other areas of law, such as copyright, offer protection to victims whose information was stolen, the court found that the CFAA still applies because it focuses on the use of a computer to acquire the information.[130] The court further found that CFAA liability accrues for someone who abuses his or her authority in the use of a computer to obtain confidential information for purposes of gaining a commercial advantage.[131]

Other courts, however, have found that using the duty of loyalty to revoke authorization is inconsistent with the requirements of the CFAA. In *ReMedPar, Inc. v. AllParts Medical, L.L.C.*, an employer filed suit after discovering that a former employee had given a competitor a copy of a proprietary software system.[132] The trial court dismissed the suit on a 12(b)(6) motion, primarily on the grounds that there was no evidence that the former employee accessed the source code without authorization or that the access exceeded au-

124. *Id.* at 420–21.

125. *Id.*

126. *Id.* at 421 (quoting RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).

127. *Id.* at 1125.

128. *Id.*

129. 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (quoting S. REP. NO. 104-357, at 11 (1996)).

130. *Id.* at 1128–29 (quoting S. REP. NO. 104-357, at 7–8).

131. *Id.* at 1128 (quoting S. REP. NO. 104-357, at 7–8).

132. 683 F. Supp. 2d 605, 607–08 (M.D. Tenn. 2010).

thorization.[133] It reasoned that Congress did not intend to apply the CFAA to situations where "access was technically authorized but the particular use of the information was not."[134] Other statutes provided a means of adjudication for the misuse of such information.[135] The court also criticized the focus on the employee's motive, arguing that it had no basis in the text of the statute.[136] Furthermore, the employer suits attempted to stretch the meaning of "without authorization" to cover access that "exceeds authorized access," which was not consistent with the intent of Congress.[137]

The Ninth Circuit also rejected the use of agency law with the CFAA, particularly criticizing the focus on the employee's intentions. In *LVRC Holdings, L.L.C. v. Brekka*, an employee opened a competing business and took copies of electronic files prior to leaving the company.[138] In upholding the suit's dismissal, the Ninth Circuit held that the text of the CFAA did not support the argument that "authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest."[139] If an employee had authorization to use a computer subject to certain limitations, the court reasoned, the authorization remains intact even if the employee violates the limitations.[140] A simple change of mental state from loyal employee to disloyal competitor did not remove authorization.[141] The split among the courts is therefore clear and direct. In some jurisdictions, a violation of the duty of loyalty can result in liability under the CFAA. In others, it cannot.

F. Physical Trespass Cases

Courts and commentators note that Congress envisioned the CFAA as bringing the laws of trespass and burglary to cyber-

133. *Id.* at 616.

134. *Id.* at 613 (citing Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 935–36 (W.D. Tenn. 2008)).

135. *Id.* at 612 (quoting *Black & Decker, Inc.*, 568 F. Supp. 2d at 934–35).

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

137. *Id.* (quoting Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580, 2006 WL 2683058, at *6 (M.D. Fla. Aug. 1, 2006)).

138. 581 F.3d 1127, 1129–30 (9th Cir. 2009).

139. *Id.* at 1133.

140. *Id.*

141. *Id.* at 1134.

space.[142] Scholars often use this rationale as the basis for arguing that employing agency law under the CFAA is inappropriate because employees have the equivalent of permission to enter.[143]

Yet, the criminal laws of several states, including Washington and California, recognize that a person's license to enter is impliedly revoked if the person enters with criminal intent, leaving the person exposed to penalties for unauthorized entry. In *State v. Collins*, the defendant arrived at the wrong house and was invited inside by an elderly resident to use the phone.[144] After making a phone call, the defendant sexually assaulted the elderly resident.[145] Despite receiving the resident's permission to enter, the defendant was convicted of first-degree burglary, which, under Washington law, occurs when a person "with intent to commit a crime . . . enters or remains unlawfully . . . [and] assaults any person therein."[146] The Supreme Court of Washington upheld the conviction, stating that while criminal intent does not always make a defendant's presence unlawful, there may be an implied limitation or revocation of his privilege to enter that does make his presence unlawful.[147] Revocation of the authorization to enter could properly be inferred from the circumstances of the case.[148]

A court can recognize that an employee's permission to enter was impliedly revoked based on the employee's actions on the premises. In *People v. Deptula*, the defendant managed a bowling alley and had access to the safe as part of his duties.[149] The defendant confessed to killing an employee in the workplace in an attempt to cover up the theft of cash from the safe.[150] The trial court found the defendant guilty of burglary despite the fact that, as the manager, he was authorized to be in the place of business.[151] Because the defendant committed the killing during a burglary, the court found him guilty of first-degree murder.[152] The Supreme Court of California upheld

142. *See, e.g.*, ReMedPar, Inc. v. AllParts Med., L.L.C., 683 F. Supp. 2d 605, 613 (M.D. Tenn. 2010) (using the comparison to trespass and burglary as an explanation for not applying the duty of loyalty theory).

143. *See supra* text accompanying notes 95–108.

144. 751 P.2d 837, 838 (Wash. 1988).

145. *Id.*

146. *Id.* (quoting WASH. REV. CODE § 9A.52.020 (1975)).

147. *Id.* at 839–40.

148. *Id.* at 841.

149. 373 P.2d 430, 431 (Cal. 1962).

150. *Id.*

151. *Id.*

152. *Id.*

the convictions and noted that the statute defined burglary as occurring when someone "enters any . . . building. . . with intent to commit grand or petit larceny or any felony."[153] The court noted it was settled law that anyone entering a building with criminal intent is guilty of burglary, even when he received express permission to enter.[154] Thus, the manager no longer had permission to enter as a matter of law because he planned to engage in criminal activity on the premises.

Indeed, implied revocation of authorization to enter property is not a new legal concept, as the 1892 case of *People v. Barry* demonstrates.[155] The trial court convicted the defendant of burglary after entering a grocery store during business hours and taking money from the cash drawer.[156] An appellate court overturned the defendant's conviction on the basis of a faulty jury instruction.[157] The Supreme Court of California, however, directly rejected the defendant's contention that burglary was not possible because, as a member of the general public, he had an invitation to enter the store during business hours.[158] The court stated that someone "who enters with the intention to commit a felony enters without an invitation."[159]

II. DUTY OF LOYALTY VIOLATIONS CAUSE AN EMPLOYEE'S AUTHORIZATION TO BE TERMINATED UNDER THE CFAA

The circuits have split on the issue of whether a duty of loyalty violation by an employee causes the termination of his authorization to use his employer's computer systems under the CFAA. This section argues that a duty of loyalty violation can be used to terminate an employee's authorization under the CFAA.

First, I seek to demonstrate that Congress anticipated the use of the CFAA within the context of employment and did not act to preempt the operation of agency law. Next, I provide a framework for properly understanding the operation of agency law as applied to the CFAA. Finally, I present and rebut several common arguments against the use of agency law under the CFAA.

153. *Id.* (quoting CAL. PENAL CODE § 459 (West 2012)).
154. *Id.* at 431–32.
155. *See* People v. Barry, 29 P. 1026, 1026–27 (Cal. 1892).
156. *Id.* at 1026.
157. *Id.* at 1027.
158. *Id.* at 1026–27.
159. *Id.* at 1027.

Despite some assertions to the contrary,[160] the legislative history indicates that Congress was aware the CFAA could be used against employees and took no actions to exempt them. The 1986 report begins by acknowledging the seriousness of white-collar crime, a term commonly used in an employment setting.[161] It expressly admits that government employees who accessed government computers without authorization were potentially liable.[162] The report also described Congress's efforts to limit the CFAA's reach to serious offenses by employees.[163] In discussing private-sector computers, the report mentions steps taken to prevent liability for employees of telecommunications companies when making repairs.[164] The 1996 report does not expressly refer to employees, but instead distinguishes between insiders and outsiders.[165] The existence of authorization determines whether a person is an insider regardless of whether he is an employee or a user of a company's services.[166]

Congress was aware the CFAA could reach employees, but, rather than exempting employment-related activity entirely, Congress took steps to protect employees who made innocent mistakes, had minor indiscretions, or acted as whistleblowers from being subject to serious penalties.[167] One way Congress did this was to require a person to act "intentionally" in provisions potentially affecting employees,[168] thereby removing liability for employees who merely act recklessly or negligently.[169] Another step Congress took was to use the term "without authorization" rather than "exceeds authorized access" for provisions that could reach employees.[170] This choice turned the violations into something resembling trespass and precluded liability for employees who slightly exceeded their privileges.[171]

160. *See, e.g.*, Okuh, *supra* note 13, at 638.

161. S. REP. NO. 99-432, at 2 (1986); *see also White-Collar Crime*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/white_collar/whitecollarcrime (last visited Sept. 7, 2012) ("White-collar crime in a nutshell . . . is now synonymous with the full range of frauds committed by business and government professionals.").

162. S. REP. NO. 99-432, at 7 (1986).

163. *Id.* at 7–9.

164. *Id.* at 12.

165. S. REP. NO. 104-357, at 9–10 (1996).

166. *Id.* at 11.

167. S. REP. NO. 99-432, at 8.

168. *Id.* at 5–6.

169. S. REP. NO. 104-357, at 11.

170. S. REP. NO. 99-432, at 7.

171. *Id.* at 7–8; S. REP. NO. 104-357, at 11.

The legislative history demonstrates that Congress intended the CFAA to work in conjunction with other areas of law.[172] Because the CFAA does not define or impose requirements for authorization, the contours of authorization are, out of necessity, defined by sources outside of the CFAA. Authorization under the CFAA is therefore a fact-specific problem with much depending on the context of the situation. In employment settings, agency law provides the basic framework that enables an employee to act on behalf of an employer.[173] It provides a means for the creation and termination, both express and implied, of authority and is always in the background when employees act as agents of their employers. Courts routinely apply agency law to similar situations that do not implicate the CFAA.[174] Furthermore, Congress has done nothing to preempt agency law in the context of the CFAA. When the facts of a situation implicate agency law, it is an appropriate source for determining CFAA authorization.

Having established that employees are within the scope of the CFAA, I propose a four-part analysis for determining whether an employee is liable under the CFAA. An employee who, in the process of violating the duty of loyalty, removes or modifies data on his employer's computers exposes himself to potential liability under the CFAA when his employer expends significant resources in response to the employee's actions. For a CFAA suit by a former employer to succeed under this theory, four distinct events must occur *in sequence*. First, the employee must acquire an interest that is hostile to his employer.[175] Second, he must fail to inform his employer.[176] Third, he must delete, inappropriately modify, or copy data from his employer's computers in furtherance of the hostile interest.[177] Fourth, his employer must incur losses of over $5,000 in responding to the employee's actions.[178] The first three elements constitute the duty of loyalty violation. The third also serves to bring

172. S. REP. NO. 104-357, at 8. The CFAA increases penalties when a person commits the offense for "commercial advantage or private financial gain," or "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 1030(c)(2)(B) (2006).

173. This is not to imply that agency law is limited to employment situations; any person acting on behalf of another person implicates agency law. *See, e.g.*, RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. c (2006).

174. *See supra* text accompanying notes 78–94.

175. *See* RESTATEMENT (THIRD) OF AGENCY § 8.04.

176. *See id.* § 8.11.

177. *See id.* § 8.05.

178. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I).

the employee's actions into the context of the CFAA while the fourth is the loss threshold required by the CFAA.

The first step toward violating the CFAA occurs when an employee acquires an interest that is hostile to his employer. A hostile interest includes working on behalf of a competitor or acting as a competitor himself.[179] An employee may lay the groundwork for joining a competitor or even becoming one himself.[180] Neither formulating plans for future competition, nor accepting a job with a competitor trigger a duty of loyalty violation without further action by an employee. To breach the duty of loyalty, the employee must agree to affirmatively act on behalf of a competitor against the interests of his current employer while still employed.[181] But this alone is not sufficient to constitute a violation of the duty of loyalty because the employee still has an opportunity to notify his employer.

The second step occurs when the employee fails to inform his employer of his newly acquired competitive interest. Agency law does not obligate an employee to inform an employer of plans to compete in the future, whether by joining a competing firm or by creating a new firm.[182] But, when an employee withholds the existence of an actual competitive interest from his employer, he violates the duty of loyalty.[183] The failure to inform denies his employer the option of determining whether he can be trusted with continued access to company resources. At this point, the employee has violated the duty of loyalty, but not the CFAA.

The third step requires that the employee access or modify his employer's data in furtherance of the competitive interest. An employee cannot use his employer's property or confidential information against his employer's interests.[184] In the CFAA context, an employee violates this rule in two ways. First, he uses his employer's computers (at a minimum, the computer where the data resides) on behalf of a competitor.[185] Second, he accesses or modifies the data

179. RESTATEMENT (THIRD) OF AGENCY § 8.04.

180. *Id.* § 8.04.

181. *Id.* § 8.04, cmt. b; *see also* Shurgard Storage Ctrs., Inc. v. SafeGuard SelfStorage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (reviewing a case where an employee emailed files to his new employer before resigning).

182. RESTATEMENT (THIRD) OF AGENCY § 8.04 cmt. c.

183. *Id.* § 8.11 cmt. d.

184. *Id.* § 8.05.

185. *Id.* § 8.05(1). Accessing the computer itself without authorization is a violation of 18 U.S.C. § 1030(a)(2)(C) (2006), regardless of whether data is copied or modified.

on behalf of a competitor.[186] The information need not be revealed to the competitor, just used in furtherance of the competitor's interests.[187] At this point, the employee has committed both an additional duty of loyalty violation and a CFAA violation by removing or modifying information in support of an adverse interest.

The fourth event required for employee liability is that the employer must incur the CFAA-mandated $5,000 in losses as a result of the employee's actions.[188] The losses include the employer's costs of responding to the incident, including analysis, data restoration, system changes, or any other reasonable, IT-related cost.[189] It is only at this point that the necessary elements are in place for employee liability. The employee has violated both the duty of loyalty and the CFAA, and the employer has incurred the necessary IT costs. Thus, the employee has accrued liability under the CFAA.

If the events occur out of sequence or if even one event is absent, then either the employee's authority is intact or he has violated the CFAA but is nonetheless not liable for his employer's losses.[190] For example, if an employee acquires a competitive interest (step one) but notifies his employer (step two is absent) and then removes data (step three), the employee has not violated the CFAA because, by notifying his employer, he fulfilled his obligations as an agent and has not violated the duty of loyalty. Similarly, if an employee removes data (step three) before acquiring a competitive interest (step one occurs later), the employee has not violated the CFAA because the data was not removed as part of a duty of loyalty violation and the employee's authority remains undisturbed. Finally, if steps one through three are present and occur in order but the employer does not suffer the minimum $5,000 loss, then the employee has violated the CFAA but is not liable for the employer's losses. In each case, the employee might be liable for subsequent misuse of the data under

186. RESTATEMENT (THIRD) OF AGENCY § 8.05(2). If the employee only accesses and removes data without modifying it following a duty of loyalty violation, the employee violates the two provisions of the CFAA that merely require unauthorized access, 18 U.S.C. § 1030(a)(2)(C) and 18 U.S.C. § 1030(a)(5)(C). If the employee modifies or deletes data following a duty of loyalty violation, the employee violates the provision of the CFAA requiring transmission of a command and intentionally causing damage. 18 U.S.C. § 1030(a)(5)(A).

187. RESTATEMENT (THIRD) OF AGENCY § 8.05 cmt. c.

188. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

189. 18 U.S.C. § 1030(e)(11); S. REP. NO. 99-432, at 11–12 (1986).

190. *But see, e.g.*, Okuh, *supra* note 13, at 657 (criticizing the agency law theory because an employee might be liable if he accesses data on Monday while performing his duties and then acquires a competitive interest on Tuesday).

other theories of law (such as trade secrets), but he is not liable under the CFAA.

The timing of the termination of an employee's authority due to a breach of the duty of loyalty is important under the CFAA. While the third event required for CFAA liability, removing or modifying data, acts as the trigger that brings the duty of loyalty violation in-scope for the CFAA, this is not the point in time at which the employee's authority terminates as a matter of law. Rather, the termination occurs before that, at the point when the employee should have reasonably inferred that his employer, if informed, would no longer provide him with access to data.[191] As demonstrated in *Riggs*, the termination occurs at the earliest point where the conditions for a breach of the duty of loyalty are fulfilled.[192] In *Riggs,* the court ordered the defendant to forfeit his compensation from the date the violation began until he actually left the company.[193] Under the CFAA, an employee's compensation is not at issue, but the legally effective termination of his agency relationship is. The employee's agency relationship in general, and authorization to use his employer's computers in particular, terminates at the point in time when the employee acquires the hostile interest (step one) and fails to notify his employer (step two).

That the Restatement specifies an agent's "actual authority terminates" when he violates the duty of loyalty further demonstrates the timing of the termination.[194] By specifying actual authority, the Restatement leaves room for apparent authority to operate and recognizes there are situations where those involved may not be aware that an agent's authority has terminated.[195] This provides protection for third parties when the agent's actual authority has been terminated but apparent authority still exists. For example, if an employee signs a contract with an innocent third party after the employee's actual authority has been silently terminated due to a duty of loyalty violation, the contract remains valid because of the agent's apparent

191. RESTATEMENT (THIRD) OF AGENCY § 3.09.

192. Riggs Inv. Mgmt. Corp. v. Columbia Partners L.L.C., 966 F. Supp. 1250, 1266 (D.D.C. 1997).

193. *Id.*

194. RESTATEMENT (THIRD) OF AGENCY § 3.09 ("An agent's actual authority terminates . . . upon the occurrence of [certain] circumstances. . . .").

195. *See id.* § 2.03 ("Apparent authority is the power held by an agent or other actor to affect a principal's legal relations with third parties when a third party reasonably believes the actor has authority to act on behalf of the principal and that belief is traceable to the principal's manifestations.").

authority.[196] By terminating actual authority independent of apparent authority, the Restatement protects innocent third parties while anticipating that an employee's agency relationship with his employer can terminate before the employee leaves the company. This latent termination of the legal relationship leaves the employee open to liability under the CFAA.

Scholars and courts generally have four criticisms of the use of agency law in employer-initiated suits. First, they argue that such suits try to stretch the CFAA to apply "without authorization" provisions to situations where the "exceeds authorized access" provisions would be more appropriate.[197] Second, critics contend that Congress intended for the relevant provisions to target outsiders of an organization, not insiders.[198] Third, they claim that, because Congress intended the CFAA to be analogous to trespass law, employees have the equivalent of a license to enter and therefore cannot commit a trespass-like offense.[199] Fourth, they criticize the need to examine the intent behind an employee's actions.[200]

The first criticism, that the suits try to stretch the "without authorization" provisions to cover employees who actually had authorization, misconstrues the duty of loyalty argument. If the suits relied on semantics and word games to manipulate "without authorization" into a functional equivalent of "exceeds authorized access," this criticism would be valid. Instead, the suits apply the well-known duty of loyalty to establish that the employee did not have authorization at all, despite appearing to have it. Employers do not seek to create novel liability for innocent employees who mistakenly found themselves in an area of the network they should not have been.[201] Instead, they essentially seek reimbursement for losses caused by former employees whose actions severed the legal relationship between the parties and caused a significant loss to the employer.[202] The legislative history demonstrates Congress's awareness that the CFAA could reach employees and agency law is an integral

196. *See* SMITH & WILLIAMS, *supra* note 59, at 21–25.

197. *See, e.g.*, ReMedPar, Inc. v. AllParts Med., L.L.C., 683 F. Supp. 2d 605, 612 (M.D. Tenn. 2010).

198. *See, e.g.*, Okuh, *supra* note 13, at 647.

199. *See, e.g.*, *ReMedPar, Inc.*, 683 F. Supp. 2d at 613.

200. *See, e.g.*, Okuh, *supra* note 13, at 657.

201. *See* LVRC Holdings, L.L.C. v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (cautioning against interpreting the statute "in such an unexpected manner").

202. *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) (reviewing a case where an employee started a competing business then used a secure-erase program to ensure no data from his laptop could be recovered).

part of employment.[203] There is nothing in the text of the CFAA or the legislative history indicating that Congress intended to preempt agency law when it drafted the CFAA.

The second argument, that the "without authorization" provisions only apply to outsiders, ignores the text of the CFAA. The insiders-outsiders language is in the legislative history, not the statute itself.[204] Instead, the relevant provisions only refer to the state of authorization. Congress knew that the statute could impact employees. Yet, Congress added no language to the statute excluding employees, defining authorization, or preempting agency law despite the fact that agency law establishes a precedent for terminating an employee's authorization that otherwise appears intact.

The third criticism is based on Congress's intention to make the CFAA analogous to trespass law.[205] Trespass does not occur when a person has permission to enter. An employee's authorization to use computer resources, the argument goes, is equivalent to permission to enter a building. Unauthorized computer access, like trespass, cannot occur when a person has received permission. It is correct that Congress drew parallels to trespassing.[206] However, it is well established that authorization to enter property is subject to implied revocation.[207] Multiple states' supreme courts have held that even express permission to enter is revoked as a matter of law when a person intends to commit a crime on the premises.[208] Indeed, the Supreme Court of California specifically held this in a case involving an employee who entered the premises of a business to steal.[209] The court found the employee's express permission to enter terminated as of the time he entered because he planned to engage in criminal activity on the premises.[210] The trespass analogy does not help the case against use of agency law under the CFAA. Both permission to enter a physical building and authorization to use an employer's computer system are vulnerable to implied revocation based on a person's actions.

203. *See supra* Part I.B.

204. *See, e.g.*, S. REP. NO. 104-357, at 10 (1996).

205. *See, e.g.*, Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 935 (W.D. Tenn. 2008) (quoting Kerr, *supra* note 95, at 1617).

206. *See, e.g.*, S. REP. NO. 99-432, at 7 (1986).

207. *See supra* Part I.F.

208. *See* cases cited *supra* notes 144, 149, 155.

209. People v. Deptula, 373 P.2d 430, 431–32 (Cal. 1962).

210. *Id.*

Finally, though some scholars argue against the use of the duty of loyalty on the grounds that courts must delve into the subjective intentions of an employee to adjudicate these disputes,[211] Congress has already recognized this need.[212] The legislative history includes several illustrative examples of situations where intent was a factor in determining whether a person should be liable under the CFAA. One example involved a user who "inadvertently 'stumble[s] into'" something he is not authorized to access on the network.[213] Another example describes a user who only briefly "peruses data" he is not supposed to look at.[214] Congress also took actions to protect whistleblowers, who, by definition, act with good intentions.[215] Finally, penalties under the CFAA are more severe depending on "what is planned for the information after it is obtained."[216] The examples in the legislative history demonstrate that Congress recognized the relevance of intent to potential CFAA violations. Each expressly or implicitly accounts for the employee's intentions in accessing the data and bad intentions are a factor in meeting the threshold for liability or a more severe penalty.

CONCLUSION

There is currently a circuit split on the issue of whether, under the Computer Fraud and Abuse Act, a duty of loyalty violation terminates an employee's otherwise existing authorization to use his employer's computer systems and exposes him to CFAA liability. This Note has argued that when an employee violates the duty of loyalty then removes or modifies data for the benefit of a competitive interest, the employee's authorization terminates and the employee may be liable under the CFAA.

Congress neither defined authorization in the CFAA, nor did it specify how it could be granted or terminated. Case law outside of the CFAA firmly establishes that, if an employee violates the duty of loyalty, the employee's agency relationship with the employer terminates, and, along with it, the employee's authorization to act on the employer's behalf. The legislative history of the CFAA demonstrates Congress's awareness that the statute would reach employ-

211. *See, e.g.*, Okuh, *supra* note 13, at 657.
212. S. REP. NO. 99-432, at 6 (1986).
213. *Id.*
214. *Id.* at 7.
215. *Id.* at 8.
216. S. REP. NO. 104-357, at 8 (1996).

ees. Yet, Congress did nothing to prevent the normal operation of the duty of loyalty in the context of the CFAA.

This Note proposed that four, distinct steps must occur in sequence for an employee to be liable under the CFAA. First, the employee must acquire an interest that is hostile to his employer. Second, he must fail to inform his employer of the hostile interest. Third, he must delete, modify, or copy data from his employer's computers in furtherance of the hostile interest. Fourth, his employer must incur losses of over $5,000 in responding to the events. Thus, if an employee becomes a competitor or agrees to act on behalf of a competitor and fails to provide notice to his employer, he violates the duty of loyalty. The breach of the duty of loyalty terminates the employee's authority under agency law. If he then removes or modifies data in support of the hostile interest and his employer suffers damages in excess of the CFAA's $5,000 threshold, he is liable under the "without authorization" provisions of the CFAA.

APPENDIX: EMPLOYEE-HOURS CALCULATIONS

Total Compensation:	$105,000
Statutory Loss:	$5000
Work Hours/Year:	2080 (40 hours x 52 weeks)
Hourly Rate:	$50.48 (Total Compensation / Work Hours/Year)
Employee Hours:	99 (Statutory Loss / Hourly Rate)
Employee Weeks:	2.5 (Employee Hours / 40-hour week)