University of Cincinnati Law Review

Volume 86 | Issue 1 Article 9

Social Media and Federal Prosecution: A Circuit Split on Cybercrime and the Interpretation of the Computer Fraud and Abuse Act

Melissa Anne Springer
springms@mail.uc.edu

SOCIAL MEDIA AND FEDERAL PROSECUTION: A CIRCUIT SPLIT ON CYBERCRIME AND THE INTERPRETATION OF THE COMPUTER FRAUD AND ABUSE ACT

Melissa Anne Springer[*]

I. INTRODUCTION

It is nine o'clock on a Monday morning. With a hot cup of coffee in your hand, you sit down at your computer. You use your company-provided credentials to log into the computer and then the company intranet. However, before you can even open the privileged document you were assigned last week, you receive a text from a friend cryptically praising a photo he saw of you from the weekend. Unsure whether it is a picture of you and your newborn nephew cuddling on the couch, or a not-so-flattering picture of you from Saturday night, you log into Facebook on your work computer. Although the company handbook strictly forbids personal use of a company computer, you must check this picture immediately. Plus, other colleagues check social media while at work. You never do and, you think, what harm could possibly come from just this one time?

Facebook loads; you check the recent posts you were tagged in; and a picture of you and your nephew appears. You are about to respond to your friend's text when your supervisor turns the corner, glances at your screen, and asks you to accompany him to his office. He fires you on the spot for violating provisions of the company handbook. You pack up your things and leave the office.

A month later, someone knocks on your door, confirms your name, and hands you a package. Before he walks away, he says, "You've been served." Bewildered, you call an attorney and review the complaint. Apparently, the company who fired you for checking Facebook is now suing you for "intentionally access[ing] a computer without authorization or exceed[ing] authorization."[1]

Although alleged violations involve various relationships, the overwhelming majority of Computer Fraud and Abuse Act (the "CFAA") claims, like the hypothetical presented above, arise out of an employer-employee relationship or the following relationships: 162 filings (50%) as employees, consultants, or contractors; 97 filings (30%) as competitors; 42 filings (13%) as technology service providers; 29 filings (9%) as derivative businesses; 24 filings (7%) as business

* Associate Member, 2016-2017 *University of Cincinnati Law Review*.

1. 18 U.S.C. § 1030(e) (2016).

partners; 22 filings (7%) as unnamed positions; 16 filings (5%) claiming no substantial relationships; 8 filings (2%) as customers or users; and 6 filings (2%) as employers.[2]

Even though the scenario above may not have transpired under the various circuit court interpretations of the CFAA, it illustrates the CFAA's broad application. The majority of CFAA allegations do not involve "hacking" but, instead, are "construed broadly" to contain any of the following allegations: 170 filings (52%) for misappropriation of information; 71 filings (22%) for editing or deleting information; 41 filings (13%) for invasion of privacy; 40 filings (12%) for accessing another person's account; 26 filings (8%) for financial misfeasance and/or hijacking another person's account; 20 filings (6%) for impersonation; 18 filings (6%) for misappropriating a computer system; 16 filings (5%) for unlocking mobile phones; 14 filings (4%) for software disruptions of computer systems; 11 filings (3%) for credential sharing and/or harassment; 9 filings (3%) for an unrelated website; 8 filings (3%) for copyright trolling; 7 filings (2%) for spam calls or emails; 6 filings (2%) for malware and/or reverse engineering; and 5 filings (2%) for physical disruptions of computer systems and/or automated website interactions and/or modifications to enterprise software.[3] The circuit courts are split on whether the CFAA affords a broad application of the civil actions arising out of various alleged cyber infractions or whether application of CFAA requires the rule of lenity, wherein courts should narrowly apply the statute.

This Article first provides a general overview of the CFAA and then analyzes the current circuit split. The Second, Fourth, and Ninth Circuits apply a narrow definition under the rule of lenity. The First, Fifth, Seventh, and Eleventh Circuits advocate a broader application. After the circuit split analysis, this Article argues that the narrow approach and the rule of lenity should be applied when analyzing CFAA violations in order to give effect to Congress's intentions and to protect ordinary and innocent citizens from federal prosecution. This Article then proceeds to discuss pending district court cases and concludes that those district courts, or their respective circuit courts if the case is appealed, should apply the narrow definition of "unauthorized access" and "exceeds authorized access."

2. Jonathan Mayer, *Article: Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1480-81 (2016) (hereinafter Mayer, *Cyber Litigation*) (further noting that "[t]he overwhelming majority of private cybercrime claims arise in business disputes (238, 73%), and of those, most follow from previous employment (168, 52%)").

3. *Id.* at 1482.

II. BACKGROUND ON THE COMPUTER FRAUD AND ABUSE ACT

"Everything has a computer in it nowadays."[4] Although a single computer originally filled an entire room,[5] computers today are so innovative that we can wear them on our wrists.[6] We use computers to research case law, to check the daily news, to make phone or video calls, to help monitor our health, to store credit card numbers and make payments, and more. In essence, "[c]omputers now dominate nearly every aspect of our lives."[7] Because of their prevalence and dominance in our lives, more than half of the world's population has been the victims of cybercrime[8] and about 65% of businesses "reported some form of unauthorized use of their computer system."[9] Through a congressional act to prevent future damage to computers, individuals, or businesses, these cybercrimes are classified as both federal crimes[10] and fraudulent acts subject to civil remedies.[11]

Although originally enacted by Congress in 1984[12] to prosecute hackers,[13] the CFAA now provides a private right of action for various

4. Shawn E. Tuma, *What Does CFAA Mean and Why Should I Care? – A Primer on the Computer Fraud and Abuse Act for Civil Litigation*, 63 S.C. L. REV. 141, 144 (2011) [hereinafter Tuma, *Why Should I Care?*] (quoting United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011) (quoting Mark Milian, *Apple's Steve Wozniak: "We've Lost A Lot of Control*," CNN, (Dec. 8, 2010, 12:16 PM), http://www.cnn.com/2010/TECH/innovation/12/08/steve.wozniak.computers)).

5. *See* John Kopplin, *An Illustrated History of Computers Part 4* (2002), http://www.computersciencelab.com/ComputerHistory/HistoryPt4.htm (last visited Jan. 24, 2017).

6. Such computers and innovative technology has led to "smartwatches," a compact computer device. *See e.g.* Scott Stein, Apple Watch Review – Apple Watch One Year In: My (Kinda Sorta) Everyday Companion, CNET, (May 3, 2016), https://www.cnet.com/products/apple-watch.

7. Tuma, *Why Should I Care?*, *supra* note 4, at 144.

8. *Id*. at 146.

9. *Id*.

10. *Id*. (citing Amber L. Leaders, Note, *Gimme a Brekka!: Deciphering "Authorization" Under the CFAA and How Employers Can Protect Their Data*, 6 WASH. J. L., TECH. & ARTS 285, 288 (2011) (quoting 18 U.S.C. § 1030(a)(2) (2006) ("The CFAA states in relevant part that whoever 'intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information contained in a financial record of a financial institution, or of a card issuer . . . or contained in a file of a consumer reporting agency on a consumer' commits a federal crime")).

11. *Id*. at 146-147 (citing Hanger Prosthetics & Orthotics v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal 2008) (explaining that, as used in 18 U.S.C. § 1030(a)(4), the term "'defraud' . . . simply means wrongdoing")).

12. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012) (explaining how Congress first passed the Counterfeit Access Devise and Computer Fraud and Abuse Act in 1984 and then revised and expanded the CFAA in 1986, naming it the Computer Fraud and Abuse Act of 1986).

13. Congress enacted the CFAA to "enhance the government's ability to prosecute computer crimes" and originally "target[ed] hackers who accessed computer to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives . . . .'" LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009) (quoting H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)).

cyber infractions.[14] "The CFAA prohibits (1) the unauthorized accessing (2) of a 'protected' computer (3) with the intent either (a) to obtain information, (b) to further a fraud, *or* (c) to damage the computer or its data."[15] However, to receive compensatory damages, injunctive relief, or other equitable relief under the CFAA, the injured party must meet the qualifying $5,000 loss in a one-year period.[16]

A "protected" computer is any computer "that is used in a manner that affects interstate or foreign commerce or communication of the United States."[17] The injured party may file a claim against anyone who "intentionally accesses a computer without authorization or exceeds authorized access . . . ."[18] However, the extent of an employee's authorized access may be difficult to determine because "unauthorized access" may depend upon the company's procedures and policies, the employee's employment period, or the explicit authorized or unauthorized permission of any single employee.[19] Furthermore, the time at which the alleged "unauthorized access" occurred is also pertinent.[20]

To satisfy the third prong of the statute, the offender's intent is broadly construed.[21] However, "anything of value" does provide a slight limitation on the otherwise broad definition of obtaining information.[22] Similarly, the CFAA does not fully define the element of fraud. The case law provides that CFAA fraud is not the same as common law fraud.[23] Common law fraud requires actual knowledge,[24] while CFAA

14. John DiGiacomo, *Civil Actions Under the Computer Fraud and Abuse Act*, REVISION/LEGAL (February 4, 2015), ¶ 1, https://revisionlegal.com/internet-lawyer/civil-actions-computer-fraud-abuse-act [hereafter DiGiacomo, *Civil Actions*]; *see also Brekka*, 581 F.3d at 1132 (providing a five-part test as applicable to that case: "(1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that [the defendant] (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was a loss to one or more persons during any one-year period aggregating at least $5,000 in value.").

15. DiGiacomo, *Civil Actions*, *supra* note 14, at ¶ 1.

16. *See* 18 U.S.C. § 1030(g) (2016).

17. A "protected" computer includes any computer that is used in interstate or foreign commerce, including computers physically "located outside the United States that [are] used in a manner that affects intestate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2) (2016).

18. 18 U.S.C. § 1030(a)(2) (2016).

19. DiGiacomo, *Civil Actions*, *supra* note 14, at ¶ 4 ("determining an employee's level of authorized access can be tricky . . . [and] the timeline of employment is important . . . .").

20. *See id.*

21. An injured party may have a claim against "whoever . . . knowingly . . . accesses a protected computer without authorization, or exceeds authorized access, and . . . obtains anything of value . . . ." 18 U.S.C. 1030(a)(4) (2016).

22. DiGiacomo, *Civil Actions*, *supra* note 14, at ¶ 7 ("the language 'anything of value' has limited it somewhat").

23. *Id.* at ¶ 8 (*citing* eBay Inc. v, Digital Point Solutions, Inc., 608 F.Supp.2d 1156 (N.D. Cal. 2009) (CFAA fraud claim requires a demonstration of unlawful access but not the elements of common

fraud is a "wrongful action,"[25] requiring constructive knowledge. Courts have determined that "unlawful access" may establish an intent to defraud.[26] In stark contrast to both the intent to obtain and the intent to defraud, the intent to cause loss or damage is more significantly defined within the CFAA.[27]

The penalties associated with a CFAA violation depend upon the severity of the offense and the harm caused.[28] Once a court determines a violation has occurred, "[a] court may award successful plaintiffs compensatory damages, injunctive relief, and other equitable relief."[29] However, plaintiffs claiming a minimum aggregate loss of "$5,000 can only receive monetary damages."[30] Finally, the statute of limitations on a CFAA claim begins to run two years from "when the damage resulting from the alleged unauthorized access is discovered."[31]

III. CIRCUIT DECISION SPLIT ON APPLYING THE CFAA

Since the CFAA's enactment in 1984, the computer industry has grown and evolved and computer use has seen an exponential increase in all aspects of business and social life.[32] Although Congress originally intended the CFAA to prosecute hackers' unauthorized access,[33] hundreds of complaints under the CFAA have been brought by businesses,[34] resulting in a circuit split on whether the CFAA applies to non-hacker claims alleging current or former employees exceeded their "authorized access" of a "protected" computer.

---

law fraud)).

24. *See id.* (*citing* Multiven, Inc. v. Cisco Systems, Inc., 725 F.Supp 2d. 887, 994 (N.D. Cal. 2010) (holding no reason for former employee to believe employer granted him unlimited access to secure website when provided with an employee login and password because employee knew of employer's computer network policy restricting such access by a non-employee and therefore acted with "intent to defraud")).

25. *Id.* (*citing* Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp. 2d 1121, 1126 (W.D. Wash. 2000)).

26. *Id.* (*citing eBay*, 608 F.Supp.2d at 1164).

27. The CFAA defines damages as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8) (2016). Loss is defined as "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." 18 U.S.C. § 1030(e)(11) (2016).

28. 4-84 Cipes, Bernstein & Hall, Andrew Grosso, Criminal Defense Techniques § 84.04(2)(a) (Matthew Bender, Rev. Ed.) (2016).

29. DiGiacomo, *Civil Actions*, *supra* note 14, at ¶ 10 (citing 18 U.S.C. § 1030(g) (2016)).

30. *Id.* (internal quotations omitted).

31. *Id.* (citing 18 U.S.C. § 1030(g) (2016)).

32. *See* Tuma, *Why Should I Care?*, *supra* note 4, at 144.

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

34. Mayer, *Cyber Litigation*, *supra* note 2.

A. Circuit Split: The Broad Application

The broad reading of the CFAA's "unauthorized access" [35] essentially extends CFAA liability to any and all employees—both current and former—and "punish[es] anyone who uses a computer wrongly."[36] For former employees, an employer may file suit for unauthorized access of a protected computer upon an employee's termination if that employee accessed an employer's computer after termination.[37] Furthermore, a current employee may be liable under the CFAA for obtaining personal information for non-business reasons.[38] Such a broad application may be justified via contract theory and agency theory.[39] By applying contract theory, "the law punishes persons who use a computer in a way that violates a contract or terms of service."[40] Similarly, agency law "punishes any employee who acts contrary to the interests of the employer."[41]

In 2006, the Seventh Circuit broadly applied the CFAA when, after receiving a laptop from his employer to use for work purposes, the employee quit and deleted all the data from the laptop by transmitting an erase program to the computer.[42] The court applied common law agency principals and concluded that, because the employee breached his duty of loyalty to his employer,[43] the employee's relationship with the employer was terminated.[44] Thus, the Seventh Circuit held that an employee's authority to access information was immediately rescinded upon termination of employment.[45] Therefore, if a former employee accesses a computer after termination, his access is not authorized and

35. 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) (2016).

36. Michael C. Mikulic, *The Unconstitutionality of The Computer Fraud and Abuse Act*, 30 NOTRE DAME J. L. ETHICS & PUB. POL'Y 175, 176 (2016) (hereinafter Mikulic, *CFAA Unconstitutional*).

37. *See generally* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

38. *See generally* United States v. Valle, 807 F.3d 508 (2nd Cir. 2015).

39. Mikulic, *CFAA Unconstitutional*, *supra* note 36, at 176.

40. *Id*.

41. *Id*.

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

43. *Id*. at 420 (The employee breached his duty of loyalty "when, having already engaged in misconduct and decided to quit [the company] in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee").

44. *Id.* at 421 ("Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, [the employee-defendant] acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal").

45. *Id*. (The defendant's "breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop").

he is in violation of the CFAA.[46]

Four years later, the Eleventh[47] and Fifth[48] Circuits followed a similar path as the Seventh Circuit and broadly interpreted "exceeds authorized access." In *United States v. Rodriguez*, an employee worked for the Social Security Administration and used his credentials and login information to obtain personal information of seventeen people the employee knew for non-business purposes.[49] This action fell under the Eleventh Circuit's definition of "exceeds authorized access."[50] Similarly, in *United States v. John*, an employee accessed confidential customer account information and used that information to defraud those customers and her employer.[51] The Fifth Circuit added a mens rea element when applying a similarly broad definition of "exceeds authorized access." This criminalized any unauthorized access, including limits on the use of information "when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetuate a crime."[52]

Finally, the First Circuit broadly applied the CFAA when the defendant worked for the employer but decided to open his own competing business.[53] In doing so, the employee hired a computer consultant to create a program that would compile information from the former employer's website so that the defendant could undercut prices.[54] The First Circuit held that the broad confidentiality agreement between the employee and the employer, which was also signed by the defendant, meant that the defendant "exceeded authorized access" because authorized access did not include obtaining proprietary information.[55]

B. Circuit Split: The Narrow Application

In contrast to the broad application of the CFAA's "exceeds authorized access," wherein essentially any action taken by an employee

46. *Id*. at 420-421.

47. *See* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

48. *See* United States v. John, 597 F.3d 263 (5th Cir. 2010).

49. *Rodriguez*, 628 F.3d at 1260.

50. *Rodriguez*, 628 F.3d at 1263 (the defendant "exceeded his authorized access and violated the [CFAA] when he obtained personal information for a nonbusiness reason").

51. *John*, 597 F.3d at 269.

52. *Id*. at 271.

53. *See generally* EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2011).

54. *Id*. at 578.

55. *Id*. at 581 ("because of the broad confidentiality agreement[,] appellants' actions 'exceeded authorized access'").

that is considered outside the realm of employment may be considered a violation, the narrow application applies the rule of lenity, looking to Congress' intended purpose behind the CFAA: to prevent hackers from wreaking havoc on corporate mainframes and gaining access to proprietary information.[56]

The Fourth[57] and Ninth[58] Circuits first delved into the true purpose intended by Congress in 2012. In *WEC Carolina Energy Solutions LLC v. Miller*, the employee was provided with a laptop, a cellphone, and the authority to access the company's intranet and computer services.[59] Upon resignation, the employee presented his new employer with his former employer's proprietary business information taken from the laptop with which the previous employer had supplied him.[60] Although the facts of *Miller* are similar to those facts analyzed by the First Circuit[61], the Fourth Circuit did not apply a broad definition of "exceeds authorized access." Instead, the Fourth Circuit interpreted the CFAA literally and narrowly: "'without authorization' and 'exceeds authorized access' . . . apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access."[62]

In *United States v. Nosal*, the defendant, after resigning from the company, asked current employees to download client lists and client contact information from the company's confidential database and send it to the defendant.[63] The Ninth Circuit took a literal and narrow approach; however, it went a step further by focusing solely on the word "access" within the CFAA's "exceeds authorized access."[64] The court noted that the CFAA does not mention "exceeds authorized use;" it only mentions "exceeds authorized access."[65] Thus, the Ninth Circuit held

56. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009) ("The act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to access and control high technology processes vital to our everyday lives . . . .'").

57. *See generally* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201-207 (4th Cir. 2012).

58. *See generally* United States v. Nosal, 676 F.3d 854, 856-864 (9th Cir. 2012).

59. *WEC Carolina Energy*, 687 F.3d at 202.

60. *Id.* at 201.

61. Similar to the facts in *WEC Carolina Energy*, the pertinent facts of the First Circuit case included a former employer using a former employer's proprietary business information to help a new, current employer succeed. EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577, 578-80 (1st Cir. 2011).

62. *WEC Carolina Energy*, 687 F.3d at 206.

63. *Nosal*, 676 F.3d at 856.

64. *Id.* at 863 ("[T]he phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions.").

65. *Id.* at 857 (The government's argument—CFAA "language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the

"exceeds authorized access" extends only to violations of restrictions on access to information; it does not extend to restrictions on the information's use.[66]

After the 2012 decisions by the Fourth and Ninth Circuits, the circuit courts did not analyze CFAA claims under the narrow approach until 2015. In *United States v. Valle,* the defendant was a police officer and an active member of an Internet fetish community.[67] As a member of the Internet community, he vividly discussed what he desired to do to his friends and family with numerous other users.[68] The defendant also used his login credentials to access information he was authorized to access but accessed that information for personal use, something that was prohibited under the police department's rules.[69] As the most recent Circuit Court case speaking to Congress' intent for CFAA claims, the Second Circuit applied the rule of lenity and read the statute narrowly.[70] However, unlike the Ninth and Fourth Circuits, the Second Circuit acknowledged that the CFAA might take both a broad and a narrow interpretation.[71] As such, the Second Circuit claimed to be required to "apply the rule of lenity and adopt the latter construction."[72] In so doing, the court stated that it would narrowly construe the CFAA in order to ensure that Congress writes the law and the courts interpret the law.[73] A broader decision could (and would) affect not only the defendant in this case but also any person who stumbles upon information on a computer he or she is not authorized to see, although he or she is authorized to access the computer.[74]

The Second, Fourth, and Ninth Circuit's narrow construction of the CFAA and refusal to "uphold a highly problematic interpretation of a statute," demonstrates their desire to protect the millions of ordinary and

information"—"is a poor fit with the statutory language." Therefore, "'[e]xceeds authorized access' would refer to data or files on a computer that one is not authorized to access.").

66. *Id.* at 863-864 ("we hold that 'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*) (emphasis in original).

67. United States v. Valle, 807 F.3d 508, 512 (2nd Cir. 2015).

68. *Id.*

69. *Id.* at 512-513.

70. *Id*. at 523 ("The rule of lenity ensures that criminal statutes will provide fair warning of what constitutes criminal conduct, minimizes the risk of selective or arbitrary enforcement, and strikes the appropriate balance between the legislature and the court in defining criminal liability").

71. *Id*. at 512 ("the CFAA permit[s] both interpretations").

72. *Id.*

73. *Id.* at 528 ("[T]he rule of lenity requires that Congress, not the courts or the prosecutors, must decide whether conduct is criminal").

74. *See id.* at 528 ("We, on the other hand, are obligated to 'construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals.'") (quoting United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012)).

innocent citizens of the United States.[75]

IV. ARGUMENT

As the Second Circuit acknowledged, the meaning of "exceeds authorized access" and "unauthorized access" may be construed both broadly and narrowly.[76] Although the broad definition and application in each specific case appears logical, these circuit courts looked only to the defendant's culpability and failed to consider the impact such decisions would render on other citizens.[77] In contrast, the narrow definition and application protects the millions of unsuspecting citizens from criminal and civil liability. Courts should continue refusing to "uphold a highly problematic interpretation of a statute."[78] Thus, going forward, courts should embrace the narrow application for numerous reasons. First, "exceeds authorized access" and "without authorization" should be defined in the narrowest sense to protect Congress's intention to prosecute "hackers," not individuals acting within their authorized scope but for unapproved uses. Second, the CFAA applies to the authorized or unauthorized access of protected computers, not both the unauthorized access and unauthorized use of materials obtained during either authorized or unauthorized access.

A. Promises Are Not Worth Their Weight: Prosecuting Ordinary Citizens

"Exceeds authorized access" and "without authorization" should be defined in the narrowest sense to protect Congress's intent to prosecute "hackers," not individuals acting within their authorized scope but for unapproved uses. Simply, "the broad interpretation approach is unfair to the American people."[79]

As computers became more prevalent and abundant in everyday life, Congress responded by enacting the CFAA; its goal was to prosecute hackers and other illegal, unauthorized access of protected computers in order to safeguard proprietary information stored on computer mainframes across the United States.[80] Although Congress's intention

75. *Id*.

76. *Id.* at 512.

77. *Id*. at 527 ("[C]ourts that have adopted the broader construction looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeded authorized access.'") (internal quotations omitted).

78. *Id*. at 528.

79. *See* Mikulic, *CFAA Unconstitutional*, *supra* note 36, at 188.

80. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009) ("The act was

may have been well intended in 1984,[81] certain circuit courts broadly apply the CFAA—specifically "unauthorized access" and "exceeds authorized access"—in order to ensure punishment of anyone who violates the CFAA.[82]

In *Rodriguez*, the Eleventh Circuit explicitly mentioned that, under the CFAA, it was a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any department or agency of the United States."[83] Furthermore, the Eleventh Circuit acknowledged that the CFAA defined "exceeds authorized access" as "to *access* a computer with authorized access and to use such access to *obtain* or *alter* information in the computer that the accessor is *not entitled* to obtain or alter."[84] From this point, however, the court went amiss in its analysis. By holding Rodriguez liable under the CFAA because "the Administration told [him] that he was not authorized to obtain personal information for nonbusiness reasons,"[85] the Eleventh Circuit allowed individuals, businesses, and courts to broadly construe and criminalize restrictions privately placed on an individual's duties and responsibilities while at work.[86] Therefore, not only may an employee face termination from a position, but she may also face federal prosecution for actions as mundane as accessing Facebook during work to check a photo in which she was tagged.[87] "We think, and therefore we Google,"[88] Facebook, tweet, Instragram, and Snapchat. Thus, "[c]ourts should not lightly conclude that visiting an unwelcome URL should subject a person to

originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday live . . . .'").

81. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012).

82. The Circuit Courts broadly applying the CFAA include the First Circuit, the Fifth Circuit, the Seventh Circuit, and the Eleventh Circuit, as noted above. *See generally* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); and EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2011).

83. *Rodriguez*, 628 F.3d at1263 (quoting 18 U.S.C. § 1030(a)(2)(B)) (internal quotations omitted).

84. *Id*. (quoting 18 U.S.C. § 1030(e)(6)) (internal quotations omitted) (emphasis added).

85. *Id*.

86. In *Rodriguez,* the Administration's policy—regarding employee use of its databases—authorized access only to the extent that the employee obtained personal information for business purposes. Although Rodriguez conceded that he had obtained information without a business purpose, he had general authorization to access the information he obtained. *See id*. at 1260.

87. United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) ("Under the government's proposed interpretation of the CFAA, posting for sale an item prohibited by Craigslist's policy . . . will earn you a handsome orange jumpsuit.").

88. Olin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1165 (2016).

arrest by federal agents and the potential for jail time."[89]

Contrast the factual circumstances in *Rodriguez* with those in *Valle*: Valle used his law enforcement credentials to access and search for individuals without a "law enforcement purpose."[90] In both cases, the defendants were granted access to personal information of other individuals and both defendants abused that power. However, the rulings in *Rodriguez*[91] and in *Valle*[92] are contradictory to one another. Any possible scenario criminalizing one individual's access while not criminalizing another's seems contrary to Congress's initial intent within the CFAA: to prosecute hackers and protect information stored within computers.[93]

By broadly applying "unauthorized access" or "exceeds authorized access," the First, Fifth, Seventh, and Eleventh Circuit Courts looked only to the defendant's culpability and failed to consider the impact such decisions would render on other citizens. However, the remedy available that protects "millions of ordinary citizens"[94] is for the courts to apply to rule of lenity[95] under the CFAA because

> [18 U.S.C. §] 1030(a)(2)(B) is ambiguous and where, as here, the Government and the defense both posit plausible interpretations of a criminal stature, the rule of lenity requires [courts] to adopt the defendant's construction . . . . When a reasonable doubt persists about a statute's intended scope even *after* resort to the language and structure, legislative history, and motivating policies of the statute, [the courts] resolve the doubt in favor of the defendant rather than imputing to Congress an undeclared will to criminalize conduct.[96]

Thus, the narrow view should be applied in CFAA cases involving "unauthorized access" or "exceeds authorized access" in order to protect ordinary citizens.

---

89. *Id.*

90. United States v. Valle, 807 F.3d 508, 513 (2nd Cir. 2015).

91. The Eleventh Circuit held that "[the defendant] exceeded his authorized access and violated the [CFAA] when he obtained personal information for a nonbusiness purpose." *Rodriguez*, 628 F.3d at 1263.

92. The Second Circuit ruled in favor of Valle, applying "the rule of lenity to adopt the interpretation that favors the defendant," because a broad constructive of the CFAA could find culpable behavior in "millions of ordinary citizens." *Valle*, 807 F.3d at 526-528.

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

94. *Valle*, 807 F.3d at 527.

95. The rule of lenity "ensures that criminal statutes will provide fair warning of what constitutes criminal conduct, minimizes the risk of selective or arbitrary enforcement, and strikes the appropriate balance between the legislature and the court in determining criminal liability." *Id.* at 523.

96. *Id.* (internal citations omitted) (emphasis in original).

The Second Circuit acknowledged that, while a broad application would prosecute individuals "who improperly access information from a government computer—a result that some readers might find palatable," their "construction of the statute impacts many more people than [the defendant]."[97] As explained in *Nosal*, "[b]ecause 'protected computer' is defined as a computer affected by or involved in interstate commerce—effectively all computers with Internet access—the government's interpretation of 'exceeds authorized access' makes every violation of a private computer use policy a federal crime."[98]

Although there may be merits in imposing criminal liability in one specific case, the courts "must construe the statute knowing that our interpretation of 'exceeds authorized access' [and 'unauthorized access'] will govern many other situations."[99] Despite promises by the Government or other organizations that they "would not prosecute an individual for checking Facebook at work,"[100] the courts should not "take prosecutors at their word in such matters. A court should not uphold a highly problematic interpretation of a statute merely because the Government *promises* to use it responsibly."[101]

Regardless of any Government or organizational promise, "exceeds authorization" and "without authorization" should be defined in the narrowest sense to protect Congress's intention to prosecute "hackers," not individuals acting within their authorized scope but for unapproved uses.

B. Promises Are Not Worth Their Weight: Differences Between "Access" and "Use"

How to apply the CFAA boils down to two words: access and use. Generally, the CFAA applies to the authorized or unauthorized access of protected computers and not both the unauthorized access and unauthorized use of materials obtained during authorized access. If courts were to construe the CFAA to include both access and use of materials, then this broad application could become a powerful tool, creating a sharp increase in CFAA civil litigation claims that alleged computer authorization violations.[102]

---

97. *Id.* at 528.

98. United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012).

99. *Valle*, 807 F.3d at 528.

100. *Id.*

101. *Id.* (emphasis added).

102. *See* Mayer, *Cyber Litigation*, *supra* note 2, at 1462, 1472-1474 ("Civil cybercrime litigation has unambiguously exploded . . . . [D]istrict court opinions surged by over an order of magnitude. The federal appellate courts have also been reviewing civil CFAA disputes at an increasing rate . . . . Private cybercrime claims are on the rise in federal district courts and in every regional court of appeals, with

The Second Circuit explained that the Senate Committee Report issued regarding the 1986 amendments "specifically described exceeds authorized access in terms of trespassing into computer systems or files."[103] The Second Circuit further noted that the Committee

> did not want to hold liable those who inadvertently stumble into someone else's computer file or computer data, which was particularly true in those cases where an individual is authorized to sign onto an use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer or data file that happens to be accessible from the same terminal.[104]

The Senate Committee also noted that "section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer."[105]

Generally, an employee has authorized access when "his employer approves or sanctions his admission to that computer . . . [and he] accesses a computer 'without authorization' when he gains admission to a computer without approval."[106] Furthermore, the Fourth Circuit defined "exceeds authorized access" as when an employee "has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access."[107] Thus, neither of these definitions applies to an employee's "improper *use* of information validly accessed."[108] In sum, the CFAA looks solely to how an alleged violator *accessed* the information; it does not look to how the alleged violator *used* the information so long as he had authorization. If the CFAA considered how an employee or former employee used the information, "[e]mployers also would be equipped with a powerful civil cudgel against their former employees, enabling retaliation for exercising legal rights or whistleblowing."[109] Such a powerful tool could create (and has already created) a sharp increase in CFAA civil litigation claims alleging computer authorization violations.[110]

Although "Congress may have intended to open the federal

---

the sole exception of the D.C. Circuit. . . . This sudden surge in civil cybercrime litigation suggests that cases are motivated by shifts in litigation strategy . . . .").

103. *Valle*, 807 F.3d. at 525 (internal quotations omitted).

104. *Id*. (internal quotations omitted).

105. *Id.* at 525.

106. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012).

107. *Id*.

108. *Id*. (emphasis in original).

109. Mayer, *Cyber Litigation*, *supra* note 2, at 1465.

110. *Id.* at 1462, 1472.

courthouse door—just a crack—to claims involving routine or unsophisticated computer misconduct," "Congress did not intend to fling the door wide open, for so much run-of-the-mill commercial litigation."[111] For example, the number of CFAA civil litigation claims has increased significantly from 1994 to 2013: between 1994 and 2005, the number of CFAA claims were below 25 each year; however, beginning in 2006, the number of claims sky-rocketed, increasing to almost 150 claims each year in 2011 and 2013.[112] This extreme increase over a relatively short period of time indicates not only that computer use has increased significantly over the last 20 years but also "that cases are motivated by shifts in litigation strategy, rather than shifts in the underlying cybercrime problem."[113] Similarly, federal criminal allegations and convictions pertaining to CFAA violations have increased significantly over the years: the number of criminal prosecutions of the CFAA jumped from about 30 in 1990, to almost 130 in 2002, slowly leveling off at around 100 each year thereafter.[114]

By looking only at the access of an alleged CFAA violator, courts can guarantee that the scope of the statute does not extend into innocuous "unauthorized uses" of computers while at work.[115] The courts can further curtail the jump in CFAA violation cases that pertain more so to commercial litigation as "motivated by shifts in litigation strategy, rather than shifts in the underlying cybercrime problem."[116] Although the Government has previously promised to only prosecute those violations truly measuring to the degree Congress intended under the CFAA, the courts should not "take prosecutors at their word in such matters. A court should not uphold a highly problematic interpretation of a statute merely because the Government *promises* to use it responsibly."[117]

V. COUNTER-ARGUMENTS AGAINST THE RULE OF LENITY AND APPLYING THE NARROW APPLICATION AND DEFINITION

Concerned for the integrity of their personal computers, business computers, and the computers nationwide that contain a plethora of

111. *Id.* at 1503-1504.

112. *Id.* at 1473.

113. *Id.* at 1474.

114. Mayer, *Cyber Litigation*, *supra* note 2, at 1476.

115. *See id.* at 1506 ("Today, of course, computer systems are pervasive, have myriad of functions, can be shared by million of users, and are used for everyday activities . . . . Plaintiffs and prosecutors can craft a colorable cybercrime claim from myriad modern fact patterns, dragging the courts into doctrinal quagmires and chilling socially beneficial activities. . . . [However,] cybercrime law is an exceedingly limited mechanism for addressing online misconduct.").

116. *Id.* at 1474, 1506.

117. United States v. Valle, 807 F.3d 508, 528 (2nd Cir. 2015) (emphasis added).

sensitive information, citizens may ask, so what if Congress or the courts criminalize "unauthorized access" or access that "exceeds authorized access"? This is one of many possible counter arguments as to why a broader application of the CFAA should be used rather than a narrower interpretation. However, such an argument is without merit because it overlooks the "[v]agueness doctrine [as] an outgrowth . . . of the Due Process Clause of the Fifth Amendment."[118]

The Due Process Clause of the Fifth Amendment requires that a person "be informed as to what the State commands or forbids."[119] Furthermore, "[t]he vagueness doctrine states a statute violates due process if it 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.'"[120] Thus, a court must apply two separate tests to determine voidness. A statute is unconstitutionally void "if (a) it does not provide fair notice of what action violates the law, or (b) it leads to discriminatory police enforcement of the law."[121] However, the second test is more important than the first because "[w]here the legislature fails to provide such minimal guidelines, a criminal statute may permit a standardless sweep that allows policemen, prosecutors, and juries to pursue their personal predilections."[122]

Although as a best practice, it is best to avoid checking Facebook at work, an application so broad as to criminalize checking Facebook at work should not be permitted because it violates an individual's Due Process rights to fair notice and non-discriminatory enforcement of the law.[123] First, judges in the circuit courts disagree as to what interpretation Congress intended through "unauthorized access" or "exceeds authorized access."[124] If federal circuit court judges cannot cohesively determine a proper application of the phrases, how will ordinary "men of common intelligence" know the meanings? They cannot and will not know because (1) "the plain language of the statute

118. Mikulic, *CFAA Unconstitutional*, *supra* note 36, at 189 (quoting United States v. Williams, 553 U.S. 285, 304 (2008)) (internal quotations omitted).

119. *Id.* (quoting Lanzetta v. New Jersey, 306 U.S. 451, 453 (1939)).

120. *Id.* (quoting *Williams*, 553 U.S. at 305).

121. *Id.* at 189-190.

122. *Id.* at 191 (quoting Kolender v. Lawson, 461 U.S. 352, 358 (1983)) (internal quotations omitted).

123. *Id.* at 194 (The CFAA "fails to provide a person of ordinary intelligence fair notice of what conduct is prohibited under the statute" and it "is also so standardless that it leads to discriminatory law enforcement").

124. *See id.*

is vague";[125] (2) "the CFA does not explicitly inform ordinary men or women that a violation of a contract will result in criminal penalties";[126] (3) "the CFAA never explicitly specifies that acting contrary to an employer's interests will result in criminal penalties";[127] (4) "when the statute actually does provide a definition of the phrase 'exceeds authorized access,' the definition fixes nothing [because] [t]he question still remains over what kind of restriction it implements";[128] and (5) "the legislative history of the statute is ambiguous."[129]

Thus, "[a] court should not uphold a highly problematic interpretation of a statute merely because the Government *promises* to use it responsibly"[130] and "lenity might constrain police and prosecutors by denying them the opportunity to augment their power by accidents [in] artful legislative drafting."[131] As such, regardless of any Government or organizational promise, "exceeds authorization" and "without authorization" should be defined in the narrowest sense to protect Congress's intention to prosecute "hackers," not individuals acting within their authorized scope but for unapproved uses.

VI. CFAA CONSTRUCTION IN DISTRICT COURTS

Regarding "authorized access" and "exceeds authorized access," all but three circuits[132] have determined whether they apply a broad definition and application or whether they apply a narrow definition and application. This next section analyzes the various district court decisions within these silent circuit courts, suggesting that a narrow definition should be applied.

A. Districts for the Third Circuit: Courts Apply the Narrow Application

Although the Third Circuit has not yet ruled on the ever-growing circuit split, like many of its sister courts,[133] the Middle District of

125. *Id.*

126. *Id*. at 195. Earlier in the article, Mikulic discussed the differences between contract theory and agency theory, noting that both "underlie the contours of a use restriction." *Id*. at 188.

127. *Id.* at 195.

128. *Id*.

129. *See id*.

130. United States v. Valle, 807 F.3d 508, 528 (2nd Cir. 2015) (emphasis added).

131. Richard H. McAdams, *Close Enough For Government Work? Heien's Less-Than-Reasonable Mistake of the Rule of Law,* U. of Chicago Pub. Law & Legal Theory Working Papers, No. 572 at 14 (2016).

132. The Sixth Circuit decision has not yet been discussed; however, it does appear later in this article. *See infra*, notes 152, 153, and 154.

133. Although the main case in focus is a case from the Middle District of Pennsylvania (*see infra*, note 134), both the Eastern District and the Western District have also adopted the narrow

Pennsylvania adopted the narrow application of both "authorized access" and "exceeds authorized access."

In *Advanced Fluid Sys. v. Huber*, the defendant-employee was an employee who had access to confidential information and to the company's component and labor costs and project quotes.[134] After the defendant-employee's resignation, his former employer searched the defendant's computer to ensure the company's confidential information was protected.[135] Furthermore, the former employer, upon restoring erased computer and phone data, discovered that the defendant-employee communicated with a competing company while a full-time employee for the former employer.[136] The former employer further alleged that the defendant-employee had "conspired to gain access to [] confidential information . . . and to use that confidential information for the purpose of diverting [away] business . . . ."[137]

Through its narrow application, the court noted that rulings under the CFAA should be "based upon the plain language of the statute, congressional intent, and a fair and balanced evaluation of circuit court opinion."[138] Thus, the CFAA prohibits only "unauthorized *access* to information rather than unauthorized use of such information."[139]

B. Districts for the Eighth Circuit: Courts Apply the Narrow Application

Although not nearly exhaustive for all districts within the Eighth Circuit, Minnesota applied the narrow interpretation of the CFAA, declining "to open the doorway to federal court so expansively when this reach is not apparent from the plain language of the CFAA."[140] In *Condux Int'l, Inc. v. Haugum*, the former employee alleged that the

application for CFAA allegations. *See* Carnegie Strategic Design Eng'rs, LLC v. Cloherty, No. 13-1112, 2014 U.S Dist. LEXIS 28654, at *30 (W.D. Pa. Mar. 6, 2014) ("The scope of the CFAA does not extend to employees who were authorized to access the data in question, but did so in bad faith or to the future detriment of his former employer because [the court] interprets the term 'authorization' narrowly and finds that it does not extend to the improper use of information validly accessed."); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 U.S. Dist. LEXIS 50833, at *9-10 (E.D. Pa. July 13, 2007) (wherein in the court rejected plaintiff's argument that an access of protected computer was unauthorized or exceeded authorized access because the CFAA pertains to the "unauthorized procurement or alteration of information, not [an employee's] misuse or misappropriation").

134. Advanced Fluid Sys. v. Huber, 28 F. Supp. 3d 306, 313-314 (M.D. Pa. 2014).

135. *Id.* at 314.

136. *Id*.

137. *Id*.

138. *Id*. at 329.

139. *Huber*, 28 F. Supp. 3d at 329 (emphasis in original).

140. Condux Int'l, Inc. v. Haugum, D.Minn. No. 08-4824 ADM/JSM, 2008 U.S. Dist. LEXIS 100949, at * 17 (Dec. 15, 2008).

defendant-employee had "misappropriated the confidential business information for his own benefit in competition with [the plaintiff]."[141]

The court adopted the narrow interpretation of the CFAA because (1) "[w]hen a court is confronted with two rational readings of a criminal statute, it is required to construe the statute in favor of the defendant"; and (2) "[t]his rule of lenity applies to civil statutes that have criminal applications because courts are required to interpret such statutes consistently, regardless of whether the court encounters the statute in a criminal or noncriminal context."[142] The court further refused to apply the broad interpretation because it "would create a federal cause of action for an employer" in any situation wherein the employee has authorized access to information but used that information "in a manner adverse to the employer's interests or in violation of a duty of loyalty."[143]

C. Districts for the Tenth Circuit: Courts Apply the Narrow Application[144]

The Tenth Circuit, to this date, has not expressed its views as to the circuit split between a broad and narrow definition. However, the District of Colorado, a district for the Tenth Circuit, has decided at least one case alleging CFAA violations, siding with narrow interpretation.

In *Cloudpath Networks v. Securew2 B.V.*, the employer provided services that "enable[d] secure network access on devices brought from outside the organization."[145] One employee worked as a "non-employee sales agent," executed a non-disclosure agreement, received access to trade secrets, and also worked for another business. This other business, Securew2 B.V., did not compete with Cloudpath at the time.[146] However, the defendant, while working for Cloudpath, "allegedly began conspiring to steal Cloudpath's trade secrets and thereby develop a

141. *Id.* at *3.

142. *Id.* at *16-17.

143. *Id.* at *17.

144. The *Cloudpath* case (*see infra*, note 145) discussed within the text is not the only district court to apply and follow the narrow definition and application. The District Court of Kansas also followed the narrow approach. The important facts of the case are that the defendant terminated his employment but took confidential work from his previous employer to a new employer; however, because of a computer malfunction, confidential information was made public for a short period of time, during which the defendant accessed the alleged confidential information. In applying the narrow application, the court held, "[w]hen an employee has been granted general authority to access a particular area of a computer or server, . . . the fact that his employer had an unexpressed desire or intent to limit his access to a portion of that area does not establish unauthorized access within the meaning of [the CFAA]." *See generally*, Tank Connection, LLC v. Haight, 161 F. Supp. 3d 957 (D. Kan. 2016).

145. Cloudpath Networks v. Securew2 B.V., 157 F. Supp. 3d 961, 966 (D. Colo. 2016).

146. *Id.*

competing product."[147]

To resolve the apparent conflict between the broad and narrow applications of the CFAA, the court stated that "the Second, Fourth, and Ninth Circuits reject any inquiry into an individual's purposes for accessing information, instead asking only whether the individual had any sort of permission to access whatever information he or she accessed."[148] In contrast, the court noted "the First, Fifth, Seventh, and Eleventh Circuits [] hold that an improper purpose may cause someone to lose permission even if he or she would retain such permission for proper purposes."[149] In its analysis, the court sided with the narrow application because "exceeds authorized access" "does not impose criminal liability on individuals who are authorized to access company data but do so for disloyal purposes."[150] Instead, "exceeds authorized access" applies "only to individuals who are allowed to access a company computer and use that access to obtain data they are not allowed to see for *any* purpose."[151]

D. The Sixth Circuit Is Yet to Decide the Issue

Although the Sixth Circuit has not yet considered a CFAA allegation pertaining to computers, in 2011, the Sixth Circuit considered whether an onslaught of automated calls and emails constituted a violation of the CFAA.[152] Through its analysis, the court relied upon *LVRC Holdings LLC v. Brekka* and found that "without authorization" and "exceeds authorized access" were separate and distinct.[153] Thus, although the Sixth Circuit briefly reviewed the applicability of a CFAA allegation, the court did not conclude, one way or another, whether the narrow or broad application and interpretation of both phrases should control going forward; the Sixth Circuit merely repeated *Brekka's* holding—"without authorization" should be narrowly applied—without discussing how to apply "exceeds authorized access."[154]

147. *Id.* at 966-967 (wherein the defendant terminated his relationship with Cloudpath but continued to allow Securew2 B.V to utilize his login information for Cloudpath. Defendant also convinced two current Cloudpath employees to join the conspiracy and to transmit information from Cloudpath's systems or sabotage Cloudpath's software systems).

148. *Id.* at 980.

149. *Id.*

150. *Id.*

151. *Id.* at 983 (emphasis added).

152. *See* Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 301 (6th Cir. 2011).

153. *Id.* at 304.

154. *Id.*

VII. CONCLUSION

Like many of the circuit courts which adopt the narrow application of the CFAA's "authorized access" and "exceeds authorized access," numerous district courts are also adopting such a narrow stance of statutory interpretation. Henceforth, if any of those district court cases are appealed, the applicable circuit court should follow the Second Circuit's narrow application in *Valle*, protecting millions of ordinary citizens by narrowly interpreting the statute to give effect to the plain meaning, as Congress intended.

Remember the example in the introduction, wherein you were fired for accessing Facebook while at work. Would you—as an attorney or layperson—place the outcome of a possible CFAA allegation in the hands of the government who *promises* not to extend liability to you, an innocent person who checked Facebook? The answer is absolutely no.

If the facts changed slightly, would you still place your faith in the Government's promises? Assume that you have authorized access to use the computer and access certain files stored but, unbeknownst to you, you were not authorized to view the employee pay-rate sheets, accessing them inadvertently when you were pulling up other documents. The answer is still absolutely no.[155]

Although the CFAA may be read both broadly and narrowly, only a narrow reading should apply because (1) "exceeds authorization" and "without authorization" should be defined in the most narrow sense to protect Congress's intention to prosecute "hackers," not individuals acting within their authorized scope but for unapproved uses; and (2) the CFAA applies to the authorized or unauthorized access of protected computers, not both the unauthorized access and unauthorized use of materials obtained during either authorized or unauthorized access.

155. Similarly, quoting Judge Kozinski in *United States v. Nosal*, Jonathan Mayer states "ordinary consumers would have to live at the mercy of [their] local prosecutor" and "posting for sale an item prohibited by Craigslist's policy, or describing yourself as 'tall, dark, and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit." *See* Mayer, *Cyber Litigation*, *supra* note 2, at 1464.