4-1-2017

Comment: United States v. Nosal II

Futoshi Dean Takatsuki

COMMENT: *UNITED STATES V. NOSAL II*

*Futoshi Dean Takatsuki**

The Ninth Circuit in *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) ("*Nosal II*") ruled that sharing your Netflix password, for example, is a federal crime under the Computer Fraud and Abuse Act ("CFAA"). In *Nosal II*, the Ninth Circuit had to determine whether obtaining permission to use someone's login credentials constituted an access of "a protected computer without authorization" in violation of section 1030(a)(4) of the CFAA. Ultimately, the court broadly interpreted the statute and held that a person accesses a computer without authorization, in violation of the CFAA, if he or she accesses a computer after the system owner has revoked permission to access the computer.

The majority in *Nosal II* broadened violations of the CFAA to include, for example, Netflix password sharing along with grievous transgressions like stealing trade secrets. In *Nosal II*, the majority incorrectly focused on defining "without authorization," rather than getting to the heart of the issue, which was *who* was entitled to give authorization. By concluding that the CFAA criminalizes access to computers by those without permission conferred by the system owner, the majority steps toward the consequences that the Ninth Circuit attempted to prevent in its en banc decision in *Nosal I*: (1) it expands the CFAA to potentially criminalize innocuous behavior in password sharing; and (2) it leaves citizens who engage in password sharing at the mercy of the system owner and local prosecutor. Instead, the Ninth Circuit in *Nosal II* should apply the rule of lenity to pressure Congress into reforming the CFAA to better meet computer use norms of present-day society.

* I would like to give special thanks to the following people: Professor Jennifer Kamita, Valerie Henderson, Tom, Neda, and the entire Loyola Law School Entertainment Law Review team. Without their help and sincere efforts, this Comment would forever be stuck on page one. I would also like to thank Mom, Dad, Ojiichan, Obaachan, Uncle Mark, Eiko, Kaori, Atsushi, Kazuhiro, Kent, Sarah, Christine, and my friends for their constant encouragement and inspiration to stay true to myself and to pursue my dreams. Thank you very much.

I. INTRODUCTION

Password sharing has become common "innocuous conduct," whether at work or at home.[1] For example, Netflix—the subscription-based Internet television network company—specializes in providing streaming media online.[2] In 2015, over 44.7 million Americans subscribed to Netflix's online multimedia streaming service.[3] Of those 44.7 million American Netflix subscribers, two-thirds shared their login credentials with at least one other person.[4] Netflix's service options seem to promote the practice of password sharing, at least within a household: its $7.99 "Basic" plan allows for one device to stream content at a time, its $9.99 "Standard" plan allows for two devices to stream at the same time, and its $11.99 "Premium" plan allows for four.[5] Moreover, Netflix's Terms of Use do not strictly prohibit password sharing between its users.[6] While Netflix does not officially encourage password sharing, at the Consumer Electronics Show in Las Vegas, Netflix CEO Reed Hastings stated that sharing account information was "a positive thing, not a negative thing."[7] Presently, it seems that individuals can continue using their parents', friends', siblings',

1. United States v. Nosal, 844 F.3d 1024, 1038 (9th Cir. 2016).

2. *See About Netflix*, NETFLIX MEDIA CENTER, http://media.netflix.com/en/about-netflix [http://perma.cc/E9SJ-ESVY].

3. Jitender Miglani, *Netflix 2015 Revenues, Profits, and Subscribers Growth Analysis*, REVENUES AND PROFITS (Jan. 20, 2016), http://revenuesandprofits.com/netflix-2015-revenues-profits-and-subscribers-growth-analysis [http://perma.cc/7QWP-8SHV].

4. Jason Mander, *Two Thirds of Netflixers Share Their Accounts*, GLOBALWEBINDEX (July 20, 2015), http://www.globalwebindex.net/blog/two-thirds-of-netflixers-share-their-accounts [http://perma.cc/X9D2-JH7P].

5. *See Choose the Plan That's Right for You*, NETFLIX, http://www.netflix.com/simple/planform [http://perma.cc/TC7X-Y9EB].

6. *See Netflix Terms of Use*, NETFLIX (Nov. 30, 2016), http://help.netflix.com/legal/termsofuse?local=en&docType=termsofuse [http://perma.cc/5FKX-CCWZ] ("The Account Owner's control is exercised through use of the Account Owner's password and therefore to maintain exclusive control, the Account Owner should not reveal the password to anyone.").

7. Sarah Perez, *Netflix CEO Says Account Sharing Is OK*, TECHCRUNCH (Jan. 11, 2016), http://techcrunch.com/2016/01/11/netflix-ceo-says-account-sharing-is-ok [http://perma.cc/SMY6-TZHS].

or acquaintances' Netflix accounts without fearing any penalty.[8] The Internet, however, has seen a flurry of disturbing news: sharing your Netflix password has apparently been decreed a federal crime under the Computer Fraud and Abuse Act ("CFAA"),[9] because of a ruling from the Ninth Circuit.[10] The case responsible for this alarming news is *United States v. Nosal*, 844 F.3d 1024, 1028 (9th Cir. 2016) ("*Nosal II*").[11]

In *Nosal II*, the Ninth Circuit was faced with determining whether using someone else's login credentials, with their permission, constituted an access of a protected computer "without authorization" in violation of section 1030(a)(4) of the CFAA.[12] Ultimately, the majority concluded that the conduct violated section 1030(a)(4) of the CFAA, which imposes criminal penalties on whoever "'knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . .'"[13] In doing so, the Ninth Circuit broadened CFAA violations to include innocuous password sharing of, for instance, a legitimately owned Netflix account along with grievous transgressions like stealing trade secrets.[14]

This Comment will explore the history of the CFAA and how the Ninth Circuit, in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) ("Nosal I"), interpreted the vague language of this statute to avoid the undesired consequence of criminalizing a broad category of common actions that nobody would expect to be federal crimes.[15] Next, this

---

8. *See generally* Ethan Wolff-Mann, *No, the FBI Won't Drag You Away for Sharing Your Netflix Password*, MONEY (July 12, 2016), http://time.com/money/4403154/netflix-password-sharing-federal-crime [http://perma.cc/FKF7-C36K].

9. 18 U.S.C. § 1030(a)(4) (2012) (effective Sept. 26, 2008).

10. Wolff-Mann, *supra* note 8.

11. *Nosal*, 844 F.3d at 1028.

12. *See id.* (quoting 18 U.S.C. § 1030(a)(4)).

13. *Id.* (emphasis omitted) (quoting 18 U.S.C. § 1030(a)(4)).

14. *See Nosal*, 844 F.3d at 1049 (Reinhardt J., dissenting).

15. *See* United States v. Nosal, 676 F.3d 854, 860–62 (9th Cir. 2012) (en banc) (refusing to interpret the "exceeds authorized access" prong of section 1030(a)(4) of the CFAA to extend to violations of a company's use restrictions because doing so would expand the CFAA's scope far beyond computer hacking to criminalize broad day-to-day activity).

Comment will critique the Ninth Circuit's interpretation of the CFAA in *Nosal II*, which seems to depart from its policy concerns in *Nosal I*.[16] Finally, this Comment will argue that courts should not attempt to fill the gaps of the CFAA, but rather, should apply pressure on Congress to clarify the statute's meaning and scope.

Part II of this Comment will first explore the history of the CFAA by discussing its originally limited purpose and then trace its growth over the past two decades to its current posture. Part III will examine how the Ninth Circuit has attempted to limit the scope of the CFAA through its decisions in *Nosal I* and *Nosal II*. Part IV will then discuss how the majority's decision in *Nosal II* will potentially expand CFAA liability to password sharing—a common, innocuous behavior. Part V will consider approaches to avoid expanding CFAA liability to common, innocuous behaviors and will conclude by proposing the use of the rule of lenity, while courts await the reformation of the CFAA, to better meet computer-use norms of present-day society.

II. THE HISTORY OF THE CFAA & ITS CURRENT STATUTORY FRAMEWORK

A. History of the CFAA

The CFAA traces its origins to the passing of the Comprehensive Crime Control Act ("CCCA") in 1984.[17] Narrow in scope, the CCCA established only three federal crimes: hacking into computers to obtain national security secrets, hacking into computers to obtain personal financial records, and hacking into government computers.[18] Thus, the law was "'[c]onsciously narrow in scope and aimed at hackers.'"[19] During the following two decades, however, Congress substantially expanded the CCCA, which began as a criminal statute, into a wide-reaching statute

16. *See Nosal*, 844 F.3d at 1028–30.

17. *See generally* Comprehensive Crime Control Act of 1984, Pub L. No. 98-473, 98 Stat. 1976 (1984).

18. Michael C. Mikulic, Note, *The Unconstitutionality of the Computer Fraud and Abuse Act*, 30 NOTRE DAME J.L. ETHICS & PUB POL'Y 175, 179 (2016); *see also* 18 U.S.C. § 1030(a)(1)–(3) (2012) (effective Sept. 26, 2008).

19. Mikulic, *supra* note 18, at 179 (alteration in original) (quoting Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 88 (2013)).

designed to address new challenges arising in the increasingly computerized world.[20]

In 1986, Congress passed a series of amendments to the CCCA, which resulted in the current statute name—the Computer Fraud and Abuse Act.[21] The amendments added three more federal crimes: section 1030(a)(4) prohibits the unauthorized access of a computer with intent to defraud;[22] section 1030(a)(5) prohibits accessing a computer without authorization and altering, damaging, or destroying information, thereby causing either $5,000 or more of aggregated loss or impairing a medical diagnosis, treatment, or care of one or more individuals;[23] and section 1030(a)(6) prohibits trafficking in computer passwords.[24] Then, in 1994, Congress expanded the CFAA through the Violent Crime Control and Law Enforcement Act,[25] which added a civil provision to the CFAA, allowing victims of computer crimes to recover civil damages against hackers.[26]

Up until the 1994 amendments, violations of the CFAA only protected "federal interest" computers "used either by the U.S. Government or financial institutions, or as part of a multistate computer network."[27] The 1996 amendments, however, changed this by expanding the statute to cover every computer connected to the Internet.[28] Those amendments replaced the category of "federal interest" computers with the new category of "protected computers," defined as any machine "used in interstate commerce."[29] Then, the category of "protected computer[s]" was further

---

20. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010) [hereinafter Kerr, *Vagueness Challenges*].

21. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986); Mikulic, *supra* note 18, at 179.

22. *See* 18 U.S.C. § 1030(a)(4).

23. *See Id.* § 1030(a)(5).

24. *See Id.* § 1030(a)(6).

25. *See generally* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (1994).

26. *See* 18 U.S.C. § 1030(g).

27. *See* Kerr, *Vagueness Challenges*, *supra* note 20, at 1565.

28. Mikulic, *supra* note 18, at 180.

29. 18 U.S.C. § 1030(e)(2)(B).

expanded to include international computers when Congress passed the USA Patriot Act of 2001.[30] Thus, by replacing the category of "federal interest" computers with "protected computer," Congress considerably expanded the scope of the CFAA.

The 2008 amendments continued the trend of expanding the realm of the CFAA.[31] First, the new amendments removed section 1030(a)(2)'s interstate communication requirement, which now makes "*any* unauthorized access to *any* protected computer that retrieves *any* information of *any* kind, interstate or intrastate . . . punishable by the statute" under section 1030(a)(2)(C).[32] Thus, a computer no longer needs to be connected to the Internet to be within the grasp of the CFAA.[33]

B. The CFAA Today

As a result of the various amendments and our increasing dependency on an Internet-connected world, "the CFAA [has become] one of the most far-reaching criminal laws in the United States Code."[34] Despite its broadened scope, the CFAA's objective has remained the same since its birth in 1984—to prohibit the unauthorized access to a computer.[35] Section 1030(a)(2) prohibits the intentional accessing of a computer without authorization or exceeding authorization to obtain financial information, information from any department or agency of the United States, or "information from any protected computer. . . ."[36] Section 1030(a)(4) is the federal computer fraud provision, which prohibits accessing a computer without authorization or exceeding authorization to defraud and obtain anything of value.[37]

---

30. *Id.*; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

31. *See* Kerr, *Vagueness Challenges*, *supra* note 20, at 1569.

32. *Id.*

33. Mikulic, *supra* note 18, at 181.

34. Kerr, *Vagueness Challenges*, *supra* note 20, at 1561.

35. *See id.*

36. *See* 18 U.S.C. § 1030(a)(2).

37. *See Id.* § 1030(a)(4).

"Most claims brought under the [CFAA] are for unauthorized access to a computer or for access beyond the user's authorization level."[38] Seventy-three percent of private CFAA claims arise in business disputes, and of those, fifty-two percent flow from previous employment.[39] Moreover, approximately fifty percent of civil CFAA filings involve a dispute where the plaintiff and defendant had an employee, consultant, or contractor relationship.[40] Thirty percent of civil CFAA filings were brought against a plaintiff's competitors.[41]

C. The Current Circuit Split

The CFAA seeks to punish those who access a computer without authorization or, although authorized, exceed their authorization.[42] For example, section 1030(a)(2) prohibits "intentionally access[ing] a computer *without authorization or exceed[ing] authorized access*, and thereby obtain[ing] . . . information from any protected computer. . . ."[43] Similarly, section 1030(a)(4) prohibits "knowingly and with intent to defraud, access[ing] a protected computer *without authorization, or exceed[ing] authorized access*, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value. . . ."[44] Regardless of whether sections 1030(a)(2) and 1030(a)(4) are brought as a civil or criminal charge, the outcome turns on whether a defendant accesses a computer "without authorization" or "exceeds authorized access."[45] Despite the numerous amendments made to the CFAA, however, the statute fails to define the term "without authorization."[46] In contrast, the statute does define the phrase "exceeds authorized access": "to access a computer with

38. Ryan E. Dosh, Comment, *The Computer Fraud and Abuse Act: As Conflict Rages on, the* United States v. Nosal *Ruling Provides Employers Clear Guidance*, 47 LOY. L.A. L. REV. 901, 904 (2014).

39. Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1481 (2016).

40. *Id.* at 1480.

41. *Id.*

42. *See* 18 U.S.C. § 1030(a)(2).

43. *Id.* (emphasis added).

44. *Id.* § 1030(a)(4) (2012) (emphasis added); *see also* Dosh, *supra* note 38, at 904.

45. *See Id.* § 1030(a)(2), (4).

46. *See Id.* § 1030.

authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter."[47]

The statute's broad reach, in conjunction with its failure to define "authorization," has created a widening split between circuit courts as to the scope and meaning of the CFAA, particularly over the interpretation of the CFAA's terms "without authorization" and "exceeds authorized access."[48] We can divide the approaches that courts have taken into three categories: a broad contract-based approach, an even broader agency-based approach, and a narrow approach.[49]

1. Broad Interpretation: Contract-Based Approach

The First, Fifth, and Eleventh Circuits take a broad approach, based in contract law, in interpreting "authorization."[50] Under this contract-based approach, courts "look[] beyond how the computer is accessed, and instead look[] to the purpose for which it was accessed."[51] If the user accesses a computer for a reason "different from, or in excess of, the purpose for which permission was granted," that user will be considered to be without authorization or to have exceeded authorized access.[52] Courts using this contract-based approach will look to whether the user's conduct was governed by an express or implied contract between the user and the party with the authority to grant access.[53] For courts that utilize this approach, an employment contract can establish the parameters of authorized access.[54]

47. 18 U.S.C. § 1030(e)(6).

48. *See* Dosh, *supra* note 38, at 906; *see also* Mikulic, *supra* note 18, at 184–88; *see also Circuit Splits*, 12 SETON HALL CIR. REV. 250, 265 (2016).

49. Matthew Gordon, Note, *A Hybrid Approach to Analyzing Authorization in the Computer Fraud and Abuse Act*, 21 B.U. J. SCI. & TECH. L. 357, 362 (2015).

50. *See* Dosh, *supra* note 38, at 907–09.

51. Gordon, *supra* note 49, at 366.

52. *Id.*; *see also* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

53. Gordon, *supra* note 49, at 366.

54. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–83 (1st Cir. 2001) (holding that an employee "exceeded authorized access" by attempting to "mine" his former employer's website in violation of a broad confidentiality agreement he signed as part of his employment).

Under this approach, courts may also recognize the existence of implied contracts in the form of widely known company policies.[55]

2. Broader Interpretation: Agency-Based Approach

The Seventh Circuit adopted the broadest approach in interpreting "authorization" by applying the CFAA to misuse.[56] "Under [this] 'agency-based' approach, employees are 'authorized' to use a computer in the interest of their employer, however this authorization ends when the employee uses the computer or information stored on it to serve an interest adverse to the employer's."[57] This approach extends the CFAA's reach the furthest because, in defining "authorization," it looks "more generally at the interest of the party authorizing the computer's use" rather than explicit or implicit grants of authority as recognized under the contract-based approach.[58]

3. Narrow Interpretation

In contrast to the First, Fifth, Seventh, and Eleventh Circuits, the Fourth and Ninth Circuits have adopted a narrow approach in interpreting the meaning of "authorization" as used in the CFAA.[59] Under this approach, courts have placed greater emphasis on the purpose of the CFAA, recognizing the importance of narrowly construing the statute to prevent the CFAA from transforming into an expansive misappropriation statute rather than an anti-hacking statute as originally intended.[60]

---

55. Gordon, *supra* note 49, at 366–67; *see also John*, 597 F.3d at 269–72 (holding that a manager's access of Citigroup's confidential information to assist in the perpetration of fraud was a violation of Citigroup's official policy, and thus was a violation of the CFAA).

56. *See* Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that an employee was no longer "authorized" to use a company's computer once the employee used the company computer to engage in improper conduct).

57. Gordon, *supra* note 49, at 368; *see also Citrin*, 440 F.3d at 420–21.

58. Gordon, *supra* note 49, at 369.

59. *See* Dosh, *supra* note 38, at 909–10; *see also* David J. Schmitt, *The Computer Fraud and Abuse Act Should Not Apply to the Misuse of Information Accessed with Permission*, 47 CREIGHTON L. REV. 423, 439 (2014).

60. *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (holding that the CFAA's provision of "exceeds authorized access" is limited to violations on "access" to information, and not restrictions on its "use"); *see also* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012) (defining the terms "without authorization" and

Consistent with the approach, the Fourth and Ninth Circuits have defined the word "authorization" as permission or power granted by an authority, and thus do not consider the terms of any employment contracts or policies.[61] Instead, the analysis under the narrow interpretation approach of the Fourth and Ninth Circuits turns on whether the defendant had permission to access the computer from one who had the authority to grant such permission.[62]

III. *UNITED STATES V. NOSAL*

The Ninth Circuit faced the task of interpreting the terms "exceeds authorized access" in *Nosal I*[63] and then "without authorization" in *Nosal II*.[64] In *Nosal I*, the Ninth Circuit was faced with the question of whether current employees "exceeded authorized access" when they used their passwords to download information and source lists for a developing competitor.[65] The court chose to adopt a narrow interpretation of the CFAA's phrase "exceeds authorized access," limiting the provision's application to the unauthorized access of a computer, and not to the misuse or misappropriation of its information.[66] Under this approach, a user violates the CFAA when the user does not have authority to access the computer in the first place—it does not matter how the user uses the

---

"exceeds authorized access" narrowly to 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, so as not to "transform a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy," especially where there are other remedies for such grievances).

61. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (holding "that an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer"); LRVC Holdings LLC v. Brekka, 581 F.3d 1127, 1129, 1133 (9th Cir. 2009) (defining the word "authorization" as "permission or power granted by an authority" and holding that an employee who was given a company password and used that password to access the company's website to obtain confidential company statistical data was "authorized" to access and use the information on the company's website).

62. *See Nosal*, 844 F.3d at 1028; *Brekka*, 581 F.3d at 1129, 1333.

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

64. *See* United States v. Nosal, 844 F.3d 1024, 1028 (9th Cir. 2016).

65. *See Nosal*, 676 F.3d at 856.

66. *Id.* at 863–64.

computer.[67] The court thereby eliminated the possibility of employers manipulating computer-use agreements and personnel policies turning such employee relationships into ones policed by criminal law.

Then, in *Nosal II*, the court was faced with the question of whether the CFAA's prohibition extended to a former employee whose computer access was rescinded, but who accessed the computer by using a current employee's login credentials with that employee's permission.[68] The court concluded that the phrase "'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[69] Thus, the court reasoned that the definition of "without authorization" "has a simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party."[70]

A. Facts

David Nosal was a high-level regional director at Korn/Ferry International, a global executive search firm headquartered in Los Angeles with offices in San Francisco and Redwood City, California.[71] Nosal "worked for Korn/Ferry from approximately April 1996 until October 2004."[72] "Korn/Ferry's bread and butter was identifying and recommending potential candidates for corporate" executives and other high-level positions.[73] "[A]fter being passed over for a promotion, Nosal announced his intention to leave Korn/Ferry."[74] Negotiations ensued and Nosal entered into a Separation and General Release Agreement and an Independent Contractor Agreement with Korn/Ferry.[75] In these

67. *See id.*

68. *See Nosal*, 844 F.3d at 1028–29.

69. *Nosal*, 844 F.3d at 1028.

70. *Id.*

71. *Id.* at 1030; United States v. Nosal, 930 F. Supp. 2d 1051, 1054 (N.D. Cal. 2013).

72. *Nosal*, 930 F. Supp. 2d at 1054.

73. *Nosal*, 844 F.3d at 1030; *see also Nosal*, 930 F. Supp. 2d at 1054.

74. *Nosal*, 844 F.3d at 1030.

75. *Id.*; *Nosal*, 930 F. Supp. 2d at 1054.

agreements, Nosal agreed to serve as an independent contractor to Korn/Ferry for roughly a year, and he "agreed not to perform executive search[es] or related services for any other entity during the term of his contract."[76] In return, as Nosal put it, Korn/Ferry gave him "'a lot of money' to 'stay out of the market.'"[77] During this period, however, Nosal secretly launched his own executive search firm with the assistance of three other current or former Korn/Ferry employees: Becky Christian ("Christian"), Mark Jacobson ("Jacobson"), and Jacqueline Froehlich-L'Heureaux ("FH").[78]

"Christian . . . was employed by Korn/Ferry from approximately September 1999 to January 2005."[79] "In January 2005, Christian left Korn/Ferry and, under instructions from Nosal, set up an executive search firm—Christian & Associates—from which" Christian retained twenty-percent of the revenues, while Nosal retained eighty-percent.[80] Jacobson then followed Christian a few months later and joined Christian & Associates.[81] While the three began work for clients, FH remained at Korn/Ferry.[82]

In its early stages, Nosal's start-up company lacked a key ingredient to become competitive in the executive search firm market—Korn/Ferry's "Searcher" database, a proprietary database of executives and companies.[83] Searcher was "an internal database of information on over one million executives" that Korn/Ferry collected over several years.[84] Such information included "contact information, employment history, salaries, biographies and resumes. . . ."[85] Searcher allowed for Korn/Ferry employees to efficiently compile a "source list" or candidate list for client

76. *Nosal*, 844 F.3d at 1030; *Nosal* 930 F. Supp. 2d at 1054.

77. *Nosal*, 844 F.3d at 1030.

78. *Id.*; *Nosal*, 930 F. Supp. 2d at 1054.

79. *Nosal*, 930 F. Supp. 2d at 1054.

80. *Nosal*, 844 F.3d at 1030.

81. *Id.*

82. *Id.* at 1030-31.

83. *Id.* at 1030; *Nosal*, 930 F. Supp. 2d at 1054.

84. *Nosal*, 844 F.3d at 1030.

85. *Id.*

companies looking to fill an open executive position by searching the database.[86] Needless to say, Searcher was necessary for Christian & Associates to remain competitive in their respective market.

The Searcher database, however, was hosted on Korn/Ferry's password-protected internal computer network.[87] "Korn/Ferry issued each employee a unique username and password to its computer system."[88] Without a password, no person could access Searcher.[89] "During the fourth quarter of 2004, just prior to leaving Korn/Ferry, Christian downloaded custom reports from the 'Searcher' database containing over 3,000 records. She took copies of these reports with her when she left the firm."[90]

After Christian and Jacobson left the company and Nosal became a contractor, Korn/Ferry revoked their credentials to "access Korn/Ferry's computer system."[91] Therefore, on three occasions, the three began enlisting the help of FH, who remained an employee at Korn/Ferry.[92] "In April 2005, Nosal instructed Christian to obtain some source lists from Searcher to expedite their work for [their start-up company's] new client."[93] Christian then asked FH for her login credentials, "which Christian . . . used to log in to Korn/Ferry's computer system and run queries in Searcher."[94] Christian sent the results of those queries to Nosal.[95] In July 2005, Christian again accessed Searcher from a computer in Korn/Ferry's San Francisco office using FH's account to download two source lists.[96] Then, later that month, Jacobson also used FH's credentials to log into the company's computer network "to download information on

86. *Id.*

87. *Id.*

88. *Id.* at 1031.

89. *See Nosal*, 844 at 1031.

90. *Nosal*, 930 F. Supp. 2d at 1055.

91. *Nosal*, 844 F.3d at 1031.

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.*

96. *Nosal*, 844 F.3d at 1031; *Nosal*, 930 F. Supp. 2d at 1056.

2,400 executives. None of these searches related to any open searches that fell under Nosal's independent contractor agreement.'"[97] In March 2005, Korn/Ferry received an e-mail from an unidentified person alerting Korn/Ferry "that Nosal was conducting his own business in violation of his non-compete agreement. The company launched an investigation and, in July 2005, contacted government authorities."[98]

B. Nosal I

On June 26, 2008, at a superseding indictment, Nosal was charged with twenty criminal counts, including trade secret theft, mail fraud, conspiracy, and eight counts under the CFAA (counts two through nine).[99] Counts two and four through seven alleged that, while employed at Korn/Ferry, Christian, and FH used their login credentials, downloaded proprietary information, and duplicated that information for Nosal's benefit, both without authorization and by exceeding authorized access.[100] On January 12, 2009, Nosal filed a motion to dismiss the CFAA counts, arguing that the CFAA only targets hackers, not individuals who access a computer with authorization and then misuse the information obtained through such access.[101] The district court denied Nosal's motion, holding that the CFAA covered the situations alleged in the complaint.[102]

Then, "[i]n September 2009, the Ninth Circuit decided *LVRC Holdings LLC v. Brekka*, which interpreted the CFAA's prohibition on accessing computers 'without authorization' or 'exceeding authorized access.'"[103] In light of *Brekka*, Nosal filed a motion to reconsider the district court's order refusing to dismiss the CFAA charges.[104] Applying the reasoning from *Brekka*, the district court dismissed counts two and four

97. *Nosal*, 844 F.3d at 1031.

98. *Id.*

99. United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *2 (N.D. Cal. Apr. 13, 2009).

100. *Id.* at 4.

101. *Nosal*, 930 F. Supp. 2d at 1056.

102. *Nosal*, 2009 WL 981336, at *7.

103. *Nosal*, 930 F. Supp. 2d at 1057 (discussing LRVC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)).

104. *Id.*

through seven.[105] The district court reasoned that access to Korn/Ferry's computers in all five of those instances did not violate section 1030(a)(4) because the individuals who allegedly accessed the computer were still Korn/Ferry employees with permission to access the company's database.[106] The government subsequently appealed the dismissals of counts two and four through seven.[107] Thereafter, a majority of the justices on the Ninth Circuit voted to rehear the case en banc.[108]

The Ninth Circuit, reviewing the case de novo, focused on the question of whether Nosal's accomplices had exceeded their authorization.[109] The court began with an analysis of the statutory definition of "exceeds authorized access"—"'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter.'"[110] The court stated that the language could be read in either of two ways: (1) "it could refer to someone who's authorized to access only certain data or files on a computer, but accesses unauthorized data or files," commonly referred to as "hacking"; or (2) it could refer to someone who has unrestricted access to information on a computer, but is limited in the manner the information can be put to use.[111]

The government argued that the statutory text could only support "exceeds authorized access" as meaning someone who has unrestricted physical access to a computer, but limited in the use to which he can put the information."[112] The government contended that "entitled" means "furnish[ed] with a right" and that "so" means "in that manner," referring to use restrictions.[113] In rejecting these arguments, the court observed that

---

105. United States v. Nosal, No. C 08-0237 MHP, 2010 WL 934257, at *8 (N.D. Cal. Jan. 6, 2010).

106. *Id.*

107. *Nosal*, 930 F. Supp. 2d at 1057.

108. United States v. Nosal, 661 F.3d 1180, 1180 (9th Cir. 2011) (mem.) (ordering rehearing en banc).

109. *Nosal*, 676 F.3d at 856–57.

110. *Nosal*, 676 F.3d at 856 (quoting 18 U.S.C. § 1030(e) (2012) (effective Sept. 26, 2008)).

111. *Id.* at 856–57.

112. *Id.*

113. *Id.*

"entitled" could more sensibly be read as a synonym for "authorized," and that Congress could have very well included the word "'so' as a connector or for emphasis."[114] Under the court's interpretation, "exceeds authorized access" refers to the accessing of information by individuals whose computer-access authorization does not cover that information, rather than to the information's use.[115]

The court rejected the government's interpretation on the grounds that it "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute."[116] Instead, the court agreed with Nosal's narrower interpretation that "exceeds authorization" refers to someone who is authorized to access certain files or data on a computer, but exceeds the scope of authorization by accessing unauthorized files or data.[117] The court noted that a narrower interpretation of the CFAA is "a more sensible reading of the text and legislative history of the statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere."[118] "'[W]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)."[119]

For the court, the government's construction of the statute posed dire consequences for a society that is becoming increasingly reliant on computers.[120] The court emphatically refused to turn violations of use restrictions imposed by employers or websites into crimes under the CFAA.[121] First, it noted that if employers could define "exceeding access" through access restrictions in employment contracts, this could criminalize

---

114. *Id.* at 858.

115. *Nosal*, 676 F.3d at 858.

116. *Id.* at 857.

117. *Id.* at 858.

118. *Id.* at 863.

119. *Id.* at 858 (emphases in original).

120. *See Nosal*, 676 F.3d at 860.

121. *See id.* at 862–63.

innocuous use.[122] As an example, the court noted that an employee could be prosecuted simply for watching Reason.TV on the employee's computer.[123] The court was also concerned that employers might increasingly threaten to report employees to the FBI as a pretext to rid themselves of certain employees.[124] Second, the court recognized that computer users often agree to terms of service without reading or understanding them.[125] Hence, basing criminal liability upon these agreements that are "lengthy, opaque, subject to change, and seldom read" would "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved."[126]

The court provided several examples of the dangers that flow from a broad definition.[127] First, as the court noted, although "Facebook makes it a violation of the terms of service to let anyone log into your account, . . . it's very common for people to let close friends and relatives check their e-mail or access their online accounts."[128] As another example, the court considered the effects of a broader interpretation on dating websites whose terms of use prohibit inaccurate or misleading information, stating that, "describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit."[129] Finally, the court recognized the danger of allowing website owners and companies to determine who is authorized access through use agreements where they may retain the right to change the terms of these use agreement at any time and without notice.[130] The danger in a broader approach is that it essentially allows website owners or companies to make "behavior that

122. *Id.* at 860.

123. *Id.*

124. *Id.*

125. *Nosal*, 676 F.3d at 860.

126. *Id.*

127. *See id.* at 861–62

128. *Id.* at 861.

129. *Id.* at 862.

130. *Nosal*, 676 F.3d at 862.

wasn't criminal yesterday . . . become criminal today without an act of Congress, and without any notice whatsoever."[131]

Concerned that a broad interpretation of the CFAA would criminalize a broad range of day-to-day activities, the court applied the doctrine of lenity, noting the long-standing principle that courts "must construe ambiguous criminal statutes narrowly . . . so that Congress will not unintentionally turn ordinary citizens into criminals."[132] Based on the above, the *Nosal I* court affirmed the district court's decision, holding that the CFAA, construed narrowly, does not cover misappropriation.[133]

C. Nosal II

1. Procedural History

After the Ninth Circuit's en banc decision in *Nosal I*, Nosal seized the opportunity and moved to dismiss the three remaining CFAA counts (counts three, eight, and nine) that were not addressed on the appeal.[134] Since the hearing on Nosal's motion to dismiss, however, the government secured a second superseding indictment adding additional factual detail to counts three and eight.[135] Count three now alleged that Christian, after terminating her employment with Korn/Ferry, had used FH's login credentials, and, without authorization and by exceeding authorized access, downloaded and duplicated proprietary information from Korn/Ferry's computer system.[136] Count eight now alleged that on July 12, 2005, an unidentified individual had used FH's login credentials to access Korn/Ferry's computer network and Christian ran queries to download two source lists from the Korn/Ferry system.[137] Count nine alleged that on or about July 29, 2005, "J.F." used Jacobson's computer in Korn/Ferry's offices to remotely log into the Korn/Ferry computer network with her

131. *Id.*

132. *Id.* at 862–63.

133. *Id.* at 863–64.

134. *Nosal*, 930 F. Supp. 2d at 1053.

135. *Id.* at 1053, 1055–56.

136. *See id.* at 1055.

137. *Id.* at 1056.

login credentials.[138] She then turned the computer over to Jacobson who used Searcher to download information from the database to his computer.[139] Under each count, Nosal was alleged to have been involved as a co-conspirator.[140]

Nosal brought forth three arguments to the district court: (1) that the remaining claims must be dismissed because they failed to allege that he or his co-conspirators "hacked" the Korn/Ferry computer system;[141] (2) that the CFAA does not cover situations of voluntary password sharing;[142] and (3) that in count nine, Jacobson did not "access" Korn/Ferry's computer system to give rise to a violation of the CFAA.[143] After the district court denied Nosal's motion to dismiss the three remaining CFAA counts, a jury convicted Nosal on all counts.[144] Nosal appealed.[145]

2. *Nosal II* Majority Opinion

The issue facing the court in *Nosal II* was distinguishable from the one addressed in *Nosal I*.[146] In *Nosal I*, "the Ninth Circuit addressed whether Nosal's coworkers, as current employees, exceeded authorized access" by using their own login credentials to access Korn/Ferry's computer network.[147] The question before the court in *Nosal II* was whether the CFAA's prohibition extended to former employees whose

138. *Id.*

139. *Nosal*, 930 F. Supp. 2d at 1056.

140. *Id.* at 1055.

141. *Id.* at 1060.

142. *Id.* at 1061–62.

143. *Id.* at 1062.

144. *Nosal*, 844 F.3d at 1031–32.

145. *Id.* at 1028.

146. *See id.* at 1029 (comparing the *Nosal I* court's addressing of whether current Korn/Ferry employees who downloaded proprietary information in violation of Korn/Ferry's confidentiality and computer policies "'exceed[ed] authorized access' with intent to defraud under the CFAA," with its (*Nosal II*'s) addressing of "whether the 'without authorization' prohibition of the CFAA extends to a former employee whose computer access credentials have been rescinded but who, disregarding the revocation, accesses the computer by other means").

147. *See Trade Secret Misappropriation/Employment Litigation*, 28 No. 11 BUS. TORTS REP. 269, 271 (2016).

computer access was rescinded, but who nonetheless accessed the company's computer by using a current employee's login credentials with that employee's permission.[148] Thus, the court had to decide whether Nosal and his accomplices' use of FH's login credentials to access Korn/Ferry's Searcher database after their login credentials were revoked violated section 1030(a)(4).[149]

Again, the court in *Nosal* II faced deciphering the meaning of the first prong of section 1030(a)(4) that was at issue in *Nosal I*: accessing a computer "without authorization" "knowingly and with intent to defraud."[150] The Ninth Circuit had already defined the term "without authorization" in the previous *Brekka* and *Nosal I* cases.[151] Reviewing precedent, the Ninth Circuit concluded: "'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[152] Employing the ordinary meaning of the word "authorization" found in Black's Law Dictionary as well as the Oxford Dictionary, the court reasoned that the plain and ordinary meaning of "'authorization' means 'permission or power granted by an authority.'"[153] Furthermore, the court held that this definition from *Brekka* "has a simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party. Unequivocal revocation of computer access closes both the front door and the back door."[154]

Thus, whether Nosal accessed Searcher "without authorization" in violation of section 1030(a)(4) of the CFAA turned on whether the

148. *Id.*

149. *See Nosal*, 844 F.3d at 1029 ("Put simply, we are asked to decide whether the 'without authorization' prohibition of the CFAA extends to a former employee whose computer access credentials have been rescinded but who, disregarding the revocation, accesses the computer by other means.").

150. *See id.* at 1028.

151. *See Nosal*, 676 F.3d at 858; *Brekk*a, 581 F.3d at 1135 (holding that "a person uses a computer 'without authorization'" under the CFAA "when the employer has rescinded permission to access the computer and the defendant uses the computer anyway").

152. *Nosal*, 844 F.3d at 1028.

153. *Id.* at 1035 (quoting *Brekka*, 581 F.3d at 1135).

154. *Id.*

authority to grant permission for such access rested with FH or with Korn/Ferry.[155] For the majority, there was no question that Korn/Ferry was the sole entity that had the exclusive authority to grant persons permission to access the Searcher database.[156] It therefore held that when FH obtained permission to use her login credentials to access Korn/Ferry's computers, it did not authorize Nosal and the others to access the company's computers because "while FH might have been wrangled into giving out her password, she and the others knew that she had no authority to control system access."[157] The majority reasoned that "Korn/Ferry owned and controlled access to its computers, including the Searcher database, and it retained exclusive discretion to issue or revoke access to the database."[158]

Accordingly, after Nosal and his accomplices' credentials were revoked, they became "outsiders" who were no longer authorized to access Korn/Ferry's computers.[159] Yet, Nosal and the others blatantly circumvented the revocation by using the login credentials of FH, the current employee of Korn/Ferry who *was* authorized to access the company's database.[160] The majority concluded that Nosal and his accomplices' conduct fell squarely within the CFAA's prohibition on access "without authorization" and affirmed his conviction under section 1030(a)(4).[161]While Nosal challenged the jury instruction given at the conclusion of his trial, arguing that the CFAA only criminalizes access if a party circumvents a technological barrier, the majority found no such requirement and concluded that the instruction was a fair and accurate characterization of the term "without authorization."[162]

155. *See id.* at 1030; *see also* 18 U.S.C. § 1030(a)(4).

156. *Nosal*, 844 F.3d at 1035–36.

157. *Id.* at 1035 n.7.

158. *See id.* at 1035–36.

159. *Id.* at 1036.

160. *See id.*

161. United States v. Nosal, 844 F.3d 1024, 1038 (9th Cir. 2016).

162. *Id.* at 1038-39.

IV. ARGUMENTS

A. The Court's Majority Improperly Concluded that a Person Necessarily Accesses a Computer Account "Without Authorization" if He Does so Without the Permission of the System Owner.

For the majority, the issue in *Nosal II* was straightforward: "whether the 'without authorization' prohibition of the CFAA extends to a former employee whose computer access credentials have been rescinded but who, disregarding the revocation, accesses the computer by other means."[163] The CFAA statute fails to define the terms "without authorization."[164] Nonetheless, per the majority, the *Brekka* opinion provided a proper definition: "'[A] person uses a computer "without authorization" . . . when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.'"[165] "'Without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[166]

In *Brekka*, the Ninth Circuit defined the word "authorization" as "'permission or power granted by an authority.'"[167] Hence, an individual exceeds authorization when the individual "is authorized to use a computer for certain purposes but goes beyond those limitations."[168] Further, "a person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question."[169] There, Brekka used his password, supplied by his employer, LVRC, to access LVRC's website to obtain confidential company data.[170] Brekka then e-mailed the data to the e-mail account he shared with his wife and proceeded to use it in his

163. *Nosal*, 844 F.3d at 1029.

164. *See* 18 U.S.C. § 1030(a)(4) (2012) (effective Sept. 26, 2008).

165. *Nosal*, 844 F.3d at 1029 (alteration in original) (quoting LRVC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009)).

166. *Id.* at 1028.

167. *Brekka*, 581 F.3d at 1133 (citation omitted).

168. *Id.*

169. *Id.*

170. *Id.* at 1129.

own consulting business.[171] The court reasoned that because LVRC provided Brekka with the passsword, LRVC authorized Brekka to access and use the information on LVRC's website, supporting the court's holding that he did not violate the CFAA.[172]

This Comment does not dispute the plain ordinary meaning that the Ninth Circuit attached to "without authorization." Rather, it argues that the majority in *Nosal II* failed to adequately clarify *who* is entitled to give authorization in circumstances where a computer system is accessed with the permission of a valid account holder.[173] After appealing to the "ordinary meaning" and multiple dictionaries to corroborate the definition of "authorization" supplied by *Brekka*, the majority concluded that the CFAA criminalizes access to computers by those who do not have permission from the system owner.[174] Thus, the majority concluded that Korn/Ferry, as owner and controller of access to its computers, had exclusive discretion to issue or revoke access to the Searcher database.[175]

The majority in *Nosal II* is incorrect to conclude that a person necessarily accesses a computer account "without authorization" if he or she does so without the permission of the system owner. Although a system owner's policies may prohibit access to third parties through password sharing, legitimate account holders commonly "authorize" access of their accounts to others by lending their login credentials.[176] In justifying its refusal to base criminal liability on violations of private computer use policies to avoid criminalizing "otherwise innocuous behavior," the *Nosal I* court pointed to password sharing in violation of Facebook's Terms of Service as an example.[177] It is a violation of Facebook's Terms of Service to allow outsiders to use one's login credentials.[178] Yet, as the court in *Nosal I* pointed out, it is "very common

171. *Id.* at 1129–30.

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

173. *See Nosal*, 844 F.3d at 1052 (Reinhardt, J., dissenting).

174. *See id.* at 1035–36.

175. *Id.*

176. *See* Orin S. Kerr, Essay, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1174, 1179 (2016); *see also Nosal*, 844 F.3d at 1051 (Reinhardt, J. dissenting).

177. United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012).

178. *See Statement of Rights and Responsibilities*, FACEBOOK (Jan. 30, 2015), http://www.facebook.com/terms [http://perma.cc/6S9U-CN5V]; *see also Nosal*, 676 F.3d at 861.

for people to let close friends and relatives check their e-mail or access their online accounts."[179]

Password sharing of Netflix accounts provides another example. In 2015, over 44.7 million Americans held legitimate Netflix accounts, of which two-thirds shared their login credentials with at least one other person.[180] In both the Facebook and Netflix examples, legitimate account holders commonly "authorize" third parties to access their accounts.[181] Those third parties then access computer systems owned by entities that grant access to the account holders.[182] While both the account holders and the third parties may be aware that, if discovered, they may lose access to their online accounts or face a monetary penalty, few would imagine that they would go to federal prison for doing so.[183]

Furthermore, the dictionary definitions and the cases cited by the majority do not support the conclusion that "authorization" necessarily comes from the system owner. The majority relied upon the definition of "authorization" put forth in *Brekka*, which defined "authorization" as "'permission or power granted by an authority.'"[184] There, the majority appealed to the ordinary meaning of the words "without authorization" and several dictionaries to corroborate this definition.[185] "Black's Law Dictionary defines 'authorization' as '[o]fficial permission to do something; sanction or warrant.' The Oxford English Dictionary defines it as . . . 'to give official permission for or approval to.'"[186]

---

179. *Nosal*, 676 F.3d at 861.

180. Jason Mander, *Two Thirds of Netflixers Share Their Accounts*, GLOBALWEBINDEX (July 20, 2015), http://www.globalwebindex.net/blog/two-thirds-of-netflixers-share-their-accounts [http://perma.cc/X9D2-JH7P]; Jitender Miglani, *Netflix 2015 Revenues, Profits, and Subscribers Growth Analysis*, REVENUES AND PROFITS (Jan. 20, 2016), http://revenuesandprofits.com/netflix-2015-revenues-profits-and-subscribers-growth-analysis [http://perma.cc/7QWP-8SHV].

181. *See Nosal*, 676 F.3d at 861; Mander, *supra* note 180.

182. *See Nosal*, 676 F.3d at 861; Mander, *supra* note 180.

183. *Nosal*, 676 F.3d at 861.

184. *Id.* at 856; *Brekka*, 581 F.3d at 1133 (citation omitted).

185. *See Nosal*, 844 at 1035.

186. *Id.* (alteration in original) (citations omitted).

To support its contention that "without authorization" deserves a dictionary definition, the majority cited to Fourth, Sixth, and Tenth Circuit cases that used dictionaries to give meaning to terms.[187] In *Pulte Homes, Inc. v. Laborer's International Union of North America*,[188] the Sixth Circuit held that it is "[c]ommonly understood . . . [that] a defendant who accesses a computer 'without authorization' does so without sanction or permission."[189] Similarly, in *WEC Carolina Energy Solutions LLC v. Miller*, the Fourth Circuit held that based on the common meaning of "authorization," an employee "accesses a computer 'without authorization' when he gains admission to a computer without approval."[190]

The dictionary definitions the majority cited, however, do not support the conclusion that the CFAA criminalizes access by those without the system owner's permission. The text of the CFAA statute does not explicitly require persons to obtain the permission of a system holder; it may also be properly read to criminalize computer access only by those without the permission of "either a legitimate account holder or the system owner."[191] While the dictionary defines "authorization" as receiving permission from a person with authority,[192] none of those definitions suggest that such permission cannot come from a valid account holder. At best, as the Second Circuit concluded in *United States v. Valle*, while citing the Random House Dictionary, the "common usage of 'authorization' suggests that one 'accesses a computer without authorization' if he accesses a computer without permission to do so at all."[193]

Additionally, the cases the majority cited do nothing to support the position that only the computer system owner can give authorization.[194] In *Pulte Homes, Inc.* and *Miller*, access to a computer system by a third party

187. *See id.* at 1052 (Reinhardt, J., dissenting).

188. *Id.* at 1037 (citing Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295 (6th Cir. 2011)).

189. *Pulte Homes, Inc.*, 648 F.3d at 304.

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

191. *See Nosal*, 844 F.3d at 1052 (Reinhardt J., dissenting).

192. *See, e.g.*, *id.* at 1035.

193. United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015).

194. *See Nosal*, 844 F.3d at 1037.

through a legitimate account holder was not at issue.[195] The majority also cited *United States v. Willis* as support.[196] But *Willis* is also factually distinguishable from *Nosal II*. There, the defendant, Willis, was an employee at a debt collection agency who was responsible for assigning employees usernames and passwords to access a financial services website.[197] In exchange for methamphetamine, Willis gave his drug dealer the login credentials of a co-worker's account, without that co-worker's permission, which was then used by others to perpetrate a fraud.[198] Therefore, unlike Nosal and his accomplices who accessed Korn/Ferry's system with the permission of a legitimate account holder,[199] the defendant in *Willis* aided third parties in perpetrating fraud by using a legitimate account holder's login credentials *without that account holder's permission*.[200]

B. The Majority's Interpretation Expands Criminal Culpability Under the CFAA to Common, Innocuous Behavior.

Congress enacted the CFAA in 1984 primarily to prevent computer hacking.[201] In *Nosal I*, the en banc Ninth Circuit took a narrow approach in interpreting the CFAA to maintain its focus as a federal anti-hacking statute, and nothing further.[202] There, the court expressed concern about

---

195. In *Miller*, former employees were accused of downloading their employer's proprietary information, on behalf of a competitor company, prior to resigning from their employment. *See Miller*, 687 F.3d at 202. *Pulte Homes, Inc.* was a CFAA suit brought by a homebuilder against a labor union and two of its officers, alleging that the defendants intentionally attempted to clog the builder's phone and e-mail systems with an onslaught of phone calls and e-mails. *See Pulte Homes, Inc.*, 648 F.3d at 298–99.

196. *Nosal*, 844 F.3d at 1037 (citing United States v. Willis, 476 F.3d 1121, 1124–27 (10th Cir. 2007)).

197. *Willis*, 476 F.3d at 1123.

198. *Id.* at 1123–24.

199. *Nosal*, 844 F.3d at 1031.

200. *Willis*, 476 F.3d at 1123–24.

201. *Nosal*, 676 F.3d at 858; *see also* David J. Schmitt, *The Computer Fraud and Abuse Act Should Not Apply to the Misuse of Information Accessed with Permission*, 47 CREIGHTON L. REV. 423, 429 (2014).

202. *See* Ryan E. Dosh, Comment, *The Computer Fraud and Abuse Act: As Conflict Rages on, the* United States v. Nosal *Ruling Provides Employers Clear Guidance*, 47 LOY. L.A. L. REV. 901, 909–10 (2014).

expanding the statute beyond computer hacking and held that liability for accessing a computer without authorization under the CFAA does not turn on use restrictions imposed by employers.[203] In refusing to adopt the contract- and agency-based approaches to interpreting the CFAA, the Ninth Circuit criticized the other circuit courts as looking "only at the culpable behavior of the defendants before them, and fail[ing] to consider the effect on millions of ordinary citizens . . . ."[204] The other circuits, "therefore failed to apply the long-standing principle that [courts] must construe ambiguous criminal statutes narrowly so as to avoid 'making criminal law in Congress's stead.'"[205]

The *Nosal II* majority attempted to distinguish *Nosal I* by interpreting it as only being applicable to construing the term "exceeds authorized access."[206] But the overarching public policy concerns in *Nosal I* also apply in the context of *Nosal II*. In *Nosal I*, the Ninth Circuit was weary of transforming "whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved."[207] For instance, the court refused to base CFAA liability upon a system owner's use restrictions, thereby criminalizing activities such as accessing a work computer to visit ESPN.com or visiting dailysudoku.com.[208] While system owners commonly prohibit such activities, violators are seldom disciplined.[209]

Indeed, the Ninth Circuit also specifically considered the effect of a broad interpretation of the CFAA on the innocuous, common behavior of password sharing.[210] In the face of this policy concern, the majority stated that *Nosal II* was not a case about password sharing.[211] The majority acknowledged the dangers noted in *Nosal I*—"that ill-defined terms [might

203. *See Nosal*, 676 F.3d at 859–63.

204. *Id.* at 862.

205. *Id.* at 862–63 (citation omitted).

206. *See Nosal*, 844 F.3d at 1029.

207. *Nosal*, 676 F.3d at 860.

208. *Id.*

209. *Id.*

210. *See id.* at 860.

211. *Nosal*, 844 F.3d at 1029.

criminalize] arguably innocuous conduct, such as password sharing among friends and family. . . ."[212] It reasoned, however, that the circumstances before the court—"former employees whose computer access was categorically revoked and who surreptitiously accessed data owned by their former employer"—bore little resemblance to common password sharing.[213] Because the system owner had revoked Nosal and his accomplices' authorization, and they knew that FH had no authority to control system access, they acted "without authorization" in violation of the CFAA when they used FH's login credentials to circumvent the revocation of access.[214] Yet, the Ninth Circuit's conclusion in *Nosal II* criminalizes those who access the computer system even with the legitimate account holder's login credentials.[215] As such, this interpretation undermines the invisible line the Ninth Circuit previously created that separates innocuous behavior from the criminal computer hacking that the CFAA was intended to prevent.

C. The Majority's Interpretation of Accessing a Computer "Without Authorization" Leaves Criminal Culpability in the Hands of Private Companies & the Local Prosecutor.

Despite the majority's efforts to avoid the criminalization of innocuous behavior by recognizing liability under the CFAA if authorization to access a computer is revoked, such an interpretation still runs afoul of two other public policy concerns the Ninth Circuit touched upon in *Nosal I*. First, in *Nosal I*, the Ninth Circuit warned about the dangers of having the public at large live at the mercy of companies and local prosecutors.[216] In the context of employer-employee relationships like Nosal and Korn/Ferry, broadly interpreting the CFAA allows private parties to manipulate their computer use and personnel policies so as to turn these relationships into ones policed by the criminal law.[217]

---

212. *Id.* at 1038.

213. *Id.*

214. *Id.* at 1035–36.

215. *See* United States v. Nosal, No. C 08-0237 MHP, 2010 WL 934257, at *9 (N.D. Cal. Jan. 6, 2010).

216. *Nosal*, 676 F.3d at 862.

217. *Id.*

"Significant notice problems arise if" criminal liability turns on private policies that are "lengthy, opaque, subject to change and seldom read."[218] Not only are such terms vague and unknown, however, system owners also typically retain the right to change terms at any time and without notice.[219]

For example, Netflix's Terms of Use states, "Netflix may, from time to time, change these Terms of Use, including the Privacy Statement and [End User License Agreement]. Such revisions shall be effective immediately; provided however, for existing members, such revisions shall, unless otherwise stated, be effective 30 days after posting." [220] Currently, Netflix does not prohibit third parties from accessing its content using a valid account holder's login credentials.[221] What, then, would occur if Netflix decided to change its Terms of Use to prohibit access through password sharing? Would access to Netflix be "revoked" to the millions who use their friends' or family members' Netflix accounts, and thus criminalize their actions overnight?

Answers to such questions are ambiguous because the majority fails to clarify what constitutes a "revocation" of authority that would give rise to CFAA liability for accessing a computer "without authorization."[222] On the one hand, in the above hypothetical, those who had accessed content on Netflix through the use of a valid account holder's login credentials may have had their access "revoked" at the moment Netflix changed its Terms of Use. On the other hand, "revocation" is more obvious if Netflix were to personally serve the person who accessed content through the use of a valid account holder's login credentials, for example, via a cease and desist letter. But in determining that Nosal and his accomplices acted without authorization when accessing Korn/Ferry's Searcher database, the majority pointed out that "[Korn/Ferry] revoked [Nosal's] authorization and, while

---

218. *Id.* at 860; *see also* Michael C. Mikulic, Note, *The Unconstitutionality of the Computer Fraud and Abuse Act*, 30 NOTRE DAME J.L. ETHICS & PUB POL'Y 175, 188–98 (2016).

219. *Nosa*l, 676 F.3d at 860.

220. *Netflix Terms of Use*, NETFLIX (Nov. 30, 2016), http://help.netflix.com/legal/termsofuse?local=en&docType=termsofuse [http://perma.cc/5FKX-CCWZ].

221. Netflix's Terms of Use states that an "Account Owner's control [over his or her account] is exercised through use of the Account Owner's password and therefore to maintain exclusive control, the Account Owner *should* not reveal the password to anyone." *Id.* While not revealing the passwords may be an effective means of maintaining exclusive control, Netflix does not specifically *prohibit* the sharing of that password. *See id.*

222. *See Nosal*, 844 F.3d at 1028.

FH might have been wrangled into giving out her password, she and the others knew that she had no authority to control system access."[223] Thus, based upon the majority's reasoning, with a simple change in Netflix's Terms of Use and perhaps an automated e-mail to the legitimate account holders, the legitimate account holders and third party non-subscribers alike may be assumed to know that the account holders have no authority to control system access.[224] Thus, any subsequent access by non-subscribers through password sharing would be accessing Netflix's computer system "without authorization" in violation of the CFAA.

In *Nosal I*, the government assured the court that "whatever the scope of the CFAA," the government would not prosecute such minor violations as those described above.[225] The Ninth Circuit, sitting en banc, however, refused to rely upon such a dangerous proposition, stating: "we shouldn't have to live at the mercy of our local prosecutor."[226] Indeed, the same policy concern applies in the context of password sharing. The act of accessing an online account, such as an e-mail account, with the account holder's permission is common in our society and often harmless.[227] Yet, under the majority's interpretation, citizens who engage in such mundane activities are criminals if the prosecutors and juries determine the specific action to be morally reprehensible. Granting such power to prosecutors invites discriminatory and arbitrary law enforcement.[228]

---

223. *Nosal*, 844 F.3d at 1035 n.7.

224. In a subsequent case, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062 (9th Cir. 2016), the Ninth Circuit held that a defendant accessed a computer "without authorization" when he accessed Facebook accounts with the permission of valid account holders, even after receiving a cease and desist letter from Facebook. There, the court held that the cease and desist letter constituted a "revocation" by the system owner, which the defendant subsequently attempted to circumvent. *Id.* at 1069. The *Nosal II* facts, however, do not indicate that Nosal or his accomplices received any similar notice.

225. *Nosal*, 676 F.3d at 862.

226. *Id.*

227. *See id.* at 861; *see also Nosal*, 844 F.3d at 1053–54 (Reinhardt J., dissenting).

228. To demonstrate how the CFAA can be used as a tool of the prosecutors to charge a person's online behavior as a crime, the Ninth Circuit in *Nosal I* cited United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009), where a woman was charged under the CFAA for violating MySpace's terms of service, which prohibited lying about identifying information, including age. *Nosal*, 676 F.3d at 862.

V. SEARCHING FOR A SOLUTION

A. The Dissent's Approach Would Create a Loophole for "Inside" Hackers.

Judge Stephen Reinhardt's dissent shares the major concerns addressed in this Comment.[229] For Judge Reinhardt, *Nosal II* was about password sharing—"ubiquitous, useful, and generally harmless conduct" that Congress did not intend to criminalize through the CFAA.[230] In his view, the court's majority failed to create "a workable line" between consensual password sharing of millions of legitimate account holders and grievous transgressions like stealing trade secrets.[231]

Judge Reinhardt was particularly critical of the majority's conclusion that a person necessarily accesses a computer account "without authorization" if he does so without the permission of the system owner.[232] Listing several examples, such as "the case of an office worker asking a friend to log onto his e-mail to print a boarding pass, in violation of the system owner's access policy," Judge Reinhardt argued that access may be "authorized" even without permission from the system owner.[233] Thus, the majority's construction expands the CFAA from an anti-hacking statute to one that criminalizes otherwise innocuous conduct just because a computer is involved.

To avoid this result, Judge Reinhardt proposed an alternative construction of "without authorization."[234] "[T]he best reading of 'without authorization' in the CFAA is a narrow one: a person accesses an account 'without authorization' if he does so without having the permission of *either* the system owner *or* a legitimate account holder."[235] "This narrower reading," Judge Reinhardt argued, "is more consistent with the purpose of the CFAA" because the statute would extend only to "those whom we

229. *See* United States v. Nosal, 844 F.3d 1024, 1048–58 (9th Cir. 2016) (Reinhardt J., dissenting).

230. *Id.* 1048 (Reinhardt J., dissenting).

231. *See id.* at 1049 (Reinhardt J., dissenting).

232. *Id.* at 1051 (Reinhardt J., dissenting).

233. *Id.* (Reinhardt J., dissenting).

234. *Nosal*, 844 F.3d at 1051 (Reinhardt J., dissenting).

235. *Id.* (Reinhardt J., dissenting).

would colloquially think of as hackers: individuals who steal or guess passwords or otherwise force their way into computers without the consent of an authorized user, not persons who are given the right of access by those who themselves possess that right."[236]

Although Judge Reinhardt's proposed construction of the CFAA was intended to narrowly target hackers while protecting civilians who engage in password sharing,[237] his narrow construction of the CFAA undermines the statute's purpose of preventing hackers from accessing protected computers. Construing "without authorization" to mean that a person accesses a computer account without permission from either the system owner *or* a legitimate account holder fails to consider the possibility of a hacker obtaining access to a computer with the permission of a valid account holder, and then proceeding to destroy an entire computer system from the inside out.[238] For instance, under Judge Reinhardt's proposed construction, a person would be criminally culpable for accessing a computer with the intent to destroy the entire network only if he or she does so with no permission at all. That same person, however, would *not* be criminally culpable if he had permission from an account holder to do so. The CFAA cannot adequately fulfill its anti-hacking purpose if such a loophole exists.

B. A Code-Based Approach Would Protect Against Criminalizing Password Sharing, But Would Undermine the Purpose of the CFAA.

Another proposed solution before the court in *Nosal II* was the "code-based" approach.[239] In its amicus brief in support of Nosal, the Electronic Frontier Foundation ("EFF")[240] argued that CFAA liability requires the circumvention of a technological barrier.[241] Similar to Judge Reinhardt's

236. *Id.* (Reinhardt J., dissenting).

237. *See id.* (Reinhardt J., dissenting).

238. *Id.* at 1037.

239. *See* Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant at 11, United States v. Nosal, Nos. 14-10037 & 14-10275 (9th Cir. Dec. 9, 2014) (arguing that "circumvention of a technological access barrier is necessary for the purposes of the CFAA").

240. *Id.* at 1 ("The Electronic Frontier Foundation ('EFF') is a non-profit, member-supported civil liberties organization working to protect digital rights.").

241. *Id.* at 11.

approach, EFF viewed *Brekka* and *Nosal I* as narrowing the interpretation of the CFAA to maintain its focus as a federal anti-hacking statute.[242] In its view, the *Brekka* decision to have "authorization" turn on an employer's explicit actions to grant or deny permission to use a computer was "simply another way of stating that circumvention of a technological access barrier is necessary" for CFAA liability.[243]

Under this "code-based" approach, a system owner indicates who is permitted and not permitted to access a computer system when the system owner erects a technological access barrier, such as a password requirement, to allow authorized persons in and keep unwanted persons out.[244] Thus, using an authorized user's login credentials, with the user's permission, is not circumventing a technological barrier because the third party acts as the authorized user's agent or proxy.[245]

This code-based construction of "without authorization," however, creates certain inconsistencies within the CFAA. First, as the *Nosal II* majority explained, a requirement that a party must circumvent a technological access barrier "make[s] little sense because some [section] 1030 offenses do not require access to a computer at all."[246] Second, similar to Judge Reinhardt's proposed construction in his dissent,[247] a code-based approach is too restrictive, and thus fails to protect against conduct that Congress intended the CFAA to prevent. As one scholar explained, a person commits a crime under section 1030(a)(5)(A) if the person "'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.'"[248] Under a code-based approach, therefore, a person would not be criminally culpable for intentionally destroying an entire computer system so long as that person

242. *Id.* at 7–8.

243. *Id.* at 11.

244. Brief of Amicus Curiae, *supra* note 239, at 11; *see also* Matthew Gordon, Note, *A Hybrid Approach to Analyzing Authorization in the Computer Fraud and Abuse Act*, 21 B.U. J. SCI. & TECH. L. 357, 362 (2015).

245. Brief of Amicus Curiae, *supra* note 239, at 13.

246. *Nosal*, 844 F.3d at 1039.

247. *Id.* at 1051 (Reinhardt J., dissenting).

248. Gordon, *supra* note 244, at 365 (quoting 18 U.S.C. § 1030(a)(5) (2012) (effective Sept. 26, 2008)).

did not circumvent a technological access barrier.[249] Although a code-based approach protects against the unintended consequence of criminalizing innocuous password sharing, it also undermines the CFAA's ability to prevent at least one form of hacking for which it was created to protect.

C. An Agency Approach Broadens the CFAA to Criminalize Password Sharing

Finally, at least one scholar has suggested that "authorization" in the digital world rests on trespass norms in the physical world.[250] When a physical lock and key limits access, whether entry into premises is physical trespass depends upon whether it falls within the zone of permission granted by the owner.[251] Similar to how a landlord may grant access to the landlord's land to a third party, a computer owner may grant access rights to a valid account holder. It would follow that under trespass norms, the account holder is authorized to access the account while others are not.[252]

When the account holder gives his or her login credentials to a third party, however, access by that third party is authorized only if the third party continues to act as the account holder's agent.[253] Under such a construction of the CFAA, if the third party accesses the account on the account holder's behalf, the third party acts in the place of the account holder and accesses the computer "with authorization."[254] If the third party uses the valid account holder's login credentials in pursuit of the third party's own ends, however, then the third party accesses the computer without authorization.[255]

---

249. *Id.* at 365; *see also* Trademotion, LLC v. Marketcliq, Inc., 857 F. Supp. 2d 1285, 1291 (M.D. Fla. 2012) (holding that the plaintiff's former employee did not violate the CFAA when he intentionally deleted files from the company's computers and inserted code into its software to divert e-mails from prospective customers to his current employer because he did not circumvent a technological barrier).

250. *See* Orin S. Kerr, Essay, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146 (2016).

251. *Id.* at 1153.

252. *Id.* at 1178.

253. *Id.*

254. *Id.* at 1178–79.

255. Kerr, *supra* note 250, at 1179.

An agency approach such as that described above broadens the CFAA to criminalize innocuous conduct such as shopping for personal items online, checking the news, or accessing an e-mail account.[256] For example, assume that a law student gives a colleague his school login credentials specifically to print certain criminal law outlines he has saved on his cloud account within the school's system. A strict adherence to the proposed agency approach might criminalize that colleague's conduct if that colleague chooses to check the weather or inadvertently accesses the wrong documents.

The problem escalates further when the "zone of permission" granted by the owner is unclear. In the context of employer-employee relationships, where the CFAA is most commonly raised, scholars have criticized the agency-based approach for failing to define "authorization" in a way that gives employees notice of prohibited computer activities.[257] Because "authorization" under an agency approach is a subjective inquiry, employees are left with no reliable or predictable way to determine if they have authorization to access a computer. The result is that liability will turn on when authorization terminated in the eyes of the principal, leading to inconsistent applications of the CFAA. As one scholar argued, "what one employer may tolerate—occasional non-business-related web browsing—another might find an outrageous and blatant misuse of company time and resources."[258]

D. Congress Must Reform the CFAA and Define the Terms "Without Authorization"

A construction of the CFAA's "without authorization" must be narrow enough to prevent the criminalization of innocuous, commonly utilized conduct such as password sharing. Such a construction must also be broad enough to allow the CFAA to prevent all forms of hacking as it was intended, which it cannot do in its current form. Courts, however, should not attempt to construct such meanings from scratch because it has led to inconsistent results among different jurisdictions.[259]

---

256. *See* Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 116 (2013).

257. Michael C. Mikulic, Note, *The Unconstitutionality of the Computer Fraud and Abuse Act*, 30 NOTRE DAME J.L. ETHICS & PUB POL'Y 175, 184–89, 194 (2016).

258. Jensen, *supra* note 256, at 116–17.

259. *See* United States v. Bass, 404 U.S. 336, 348 (1971) (explaining that "because criminal punishment usually represents the moral condemnation of the community, legislatures

Instead, the CFAA should be resolved in favor of the criminal defendant because its text is ambiguous.[260] The statute fails to define the terms "without authorization," and courts continue to struggle to provide a definition of their own.[261] Members of the public are therefore left to guess at the phrases' meanings and speculate as to whether their conduct violates the CFAA. Indeed, at least one scholar criticized the CFAA as being unconstitutional because it fails to adequately provide notice to the common person about whether that person's conduct is criminal.[262]

Thus, courts should not feel responsible for defining the scope of the CFAA. Rather, Congress must clarify the terms and scope of the statute and update the CFAA to meet the needs of an increasingly Internet-reliant society.[263] In the meantime, courts should apply the rule of lenity, which requires ambiguous criminal laws to be interpreted in favor of defendants.[264] The Ninth Circuit has already applied the rule of lenity in

---

and not courts should define criminal activity."); *see also* Mikulic, *supra* note 257, at 194–96 (explaining that because the CFAA is vague, it fails to provide "fair notice of what is prohibited under the statute").

260. Jensen, *supra* note 256, at 123; *see also* LRVC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) (applying the rule of lenity because "[t]he Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants").

261. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012) (declining to extend CFAA liability to violations of use-restrictions).

262. *See* Mikulic, *supra* note 257, at 189 (citing Lanzetta v. State of New Jersey, 306 U.S. 451, 453 (1939), for the proposition that the Fifth Amendment's "Due Process Clause requires that persons 'be informed as to what the State commands or forbids.'"); *see also* United States v. Williams, 553 U.S. 285, 304 (2008) ("A conviction fails to comport with due process if the statute under which it is obtained 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."). Therefore, because the CFAA does not define the meaning of "without authorization," it fails to provide a person of ordinary intelligence fair notice of what behavior is culpable. This problem is highlighted by the different ways circuit courts have defined the CFAA's key terms.

263. *See Nosal*, 844 F.3d at 1050–51 (Reinhardt J. dissenting).

264. United States v. Santos, 533 U.S. 507, 514 (2008); *see also Brekka*, 581 F.3d at 1134 (applying the rule of lenity because, "[t]he Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants"); *Bass*, 404 U.S. at 347–48 (holding that "'ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity'" because "criminal punishment usually represents the moral condemnation of the community," and so, "legislatures and not courts should define criminal activity"); Jensen, *supra* note 256, at 98–99 ("The rule of lenity embodies two important policies. First, citizens should be given fair warning in easily understood language of behavior that can

Nosal I when it refused to adopt the stricter construction of "exceeds authorization."[265] It should have done the same in *Nosal II*, by refusing to read "without authorization" broadly until Congress provides a clear definition of those terms and the Supreme Court finds the statute constitutional.

VI. CONCLUSION

Congress created the CFAA to criminalize computer hacking and the improper access of computer systems.[266] The ambiguous statutory text of the CFAA, however, has led to inconsistent constructions of its meaning and scope.[267] As a product of the 1980s, when computer systems were relatively rare and single-purposed, the CFAA has not kept up with a society where millions of users use computer systems for everyday activities.

In *Nosal II*, the Ninth Circuit attempted to apply the CFAA to conduct that perhaps Congress did not foresee as becoming common practice among family and friends and certainly did not intend to criminalize. Yet, by broadly interpreting the words "without authorization," the Ninth Circuit has placed those who access a friend or family member's Netflix, Facebook, or e-mail accounts, even with that account holder's permission, at the mercy of the system owners and the local prosecutor. Nevertheless, at least in the meantime, Netflix users should fear not; Netflix has not prohibited access to their system by those who engage in password sharing.[268] Yet, with a simple change in their Terms of Use and a revocation of access, Netflix may render over twenty-nine million Americans criminals overnight.

---

result in criminal sanctions." "Second, laws with criminal penalties are a reflection of society's condemnation and should be defined by legislatures, not courts.").

265. *See* United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012).

266. Michael C. Mikulic, Note, *The Unconstitutionality of the Computer Fraud and Abuse Act*, 30 NOTRE DAME J.L. ETHICS & PUB POL'Y 175, 179 (2016).

267. Ryan E. Dosh, Comment, *The Computer Fraud and Abuse Act: As Conflict Rages on, the* United States v. Nosal *Ruling Provides Employers Clear Guidance*, 47 LOY. L.A. L. REV. 901, 907–10 (2014).

268. *See Netflix Terms of Use*, NETFLIX (Nov. 30, 2016), http://help.netflix.com/legal/termsofuse?local=en&docType=termsofuse [http://perma.cc/5FKX-CCWZ].