Science and Technology Law Review

Volume 20

2017

Is Your Roommate a Felon? Considering the Effect of Criminalizing Password Sharing in *Nosal* II

London Ryyanen England
Southern Methodist University, lryynaneneng@smu.edu

Is Your Roommate a Felon? Considering the Effect of Criminalizing Password Sharing in *Nosal II*

*London Ryynanen England**

In *United States v. Nosal* (*Nosal II*), the Ninth Circuit interprets key terms in the Computer Fraud and Abuse Act (CFAA), delineating actions considered criminal when taken "without authorization."[1] The majority opinion creates the unintended consequence of broadly criminalizing the common and usually innocent practice of password sharing.[2] This note compares the different definitions the majority and dissenting justices assign to the term "without authorization" within the meaning of the CFAA, specifically 18 U.S.C. § 1030(a)(4). The note suggests expanding the requisite authorization to include authorization from authorized individuals instead of just authorization from system owners. Doing so will narrow the application of the law to prevent criminalizing innocent password sharing, making the statute workable for both prosecutors and the public.

I. BACKGROUND OF THE CFAA, *NOSAL I*, AND *NOSAL II*

The CFAA was originally enacted in 1984, targeting hackers who access "computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the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.'"[3] The CFAA was passed before the Internet was fully publicly accessible, but Congress still recognized that computer crime posed serious threats to financial and life-altering technologies.[4] Today, the CFAA grants jurisdiction where the crime involves accessing "protected computers," meaning a computer "exclusively for the use of a financial institution or the United States Government . . . or which is used in or affecting interstate or foreign commerce or communication. . . ."[5]

---

* London Ryynanen England is a 2018 candidate for a Juris Doctor from SMU Dedman School of Law. She received a Bachelor of Arts in Business Administration from the University of Washington in 2008. She would like to thank Brad and Rudolf Ryynanen for their support during law school.

1. *See* United States v. Nosal, 844 F.3d 1024, 1050 (9th Cir. 2016) [hereinafter *Nosal II*].

2. *Id.* at 1036.

3. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009) (citing H.R. Rep. 98J894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)).

4. *See* S. Rep. 99–432, 1–22, 1986 U.S.C.C.A.N. 2479, *2–3 (citing an incident in 1983 in which an adolescent gang hacked the computer system at Memorial Sloan-Kettering Cancer Center, gaining access to radiation treatment records and the ability to alter radiation treatment for 6,000 past and present cancer patients).

5. 18 U.S.C.A. § 1030(e)(2)(A)–(B).

In considering the term "without authorization," courts have grappled with the challenges of employers and online work since the early days of the law.[6] The legislation provides no guidance for what satisfies "authorization."[7] In *United States v. Morris*, a Cornell University graduate student named Morris had "explicit authorization to use computers at Cornell" and to use the Internet connection between several research universities.[8] Morris developed a "worm" or "virus" to demonstrate the inadequate security of computer networks.[9] Morris used his authorized Cornell account to release the virus at Massachusetts Institute of Technology, where he held no access credentials.[10] The virus crashed computers at universities, military sites, and medical research facilities.[11]

Morris was the first case brought under the CFAA, and the Second Circuit looked to legislative intent to determine whether Morris acted "without authorization."[12] The court found that Congress intended to punish intentional trespasses both by those who are "outsiders" to the organization and those with some form of "insider" access.[13] Under the Second Circuit's reading of the CFAA, Morris was convicted despite having "insider" access.[14]

Recently, the Ninth Circuit analyzed the plain language of the CFAA to determine congressional intent for the definition of "without authorization."[15] The court relied on a dictionary definition for "authorization" as "permission or power granted by an authority" and held that, "for the purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations."[16] In other words, the court wanted to avoid criminalizing misuse of computers by otherwise authorized individuals.

---

6. *See generally* Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (discussing the expectation of privacy by an employee in relation to the contents of an office computer).

7. "The CFAA defines 'exceeds authorized access,' [the alternate criminal behavior for conviction under the CFAA], as 'access to a computer with authorization and using such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Nosal II*, *supra* note 1, at 1033.

8. United States v. Morris, 928 F.2d 504, 505–06 (2d Cir. 1991).

9. *Id.* at 505.

10. *Id.* at 506–10.

11. *Id.* at 506.

12. *Id.* at 509–11.

13. *Id.* at 511.

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

15. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132–33 (9th Cir. 2009).

16. *Id.* at 1133.

A. *Nosal I*

Nosal was a regional director for Korn/Ferry International (KFI), an executive search firm specializing in identifying and recommending candidates for executive-level corporate positions.[17] KFI used a proprietary internal software program to locate candidates. The software included data on more than one million executives (including contact information, employment history, salaries, biographies, and more), culled from a variety of public and proprietary sources.[18] KFI implemented security measures to protect the confidentiality of the system's information. This included giving each associate a unique username and password and requiring new associates to sign a confidentiality agreement that specifically prohibited password sharing.[19] Also, when each search was run, the computer program displayed a warning: "[t]his product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only."[20]

Nosal's employment contract included a non-compete agreement.[21] But Nosal left KFI to start a competing firm and negotiated his retention with KFI to finish his open searches subject to continuing his non-competition agreement.[22] According to Nosal, KFI paid him "a lot of money" to "stay out of the market."[23] Nosal did not stay out of the market.[24] Instead, he and three other KFI employees began a competing firm, Christian & Associates, from which Nosal earned eighty percent of the revenue.[25] Before leaving KFI, the Christian & Associates team downloaded information and source lists from the KFI database.[26] These downloads violated KFI's computer use policy.[27] In order for Christian & Associates team members to run executive searches within the KFI database, Nosal's former assistant continued her employment with KFI and shared her password with the Christian & Associates team.[28] More than a year after Nosal signed his non-compete agreement, an unidenti-

17. *Nosal II*, 844 F.3d 1024, 1030 (9th Cir. 2016).

18. *Id.*

19. *Id.* at 1031.

20. *Id.*

21. *Id.*

22. *Id.* at 1030.

23. *Nosal II*, 844 F.3d at 1030.

24. *Id.*

25. *Id.*

26. *Id.* at 1031.

27. *Id.* The downloading of KFI proprietary information while Nosal and his associates were still employed by KFI became the basis for five of the claims originally brought under the CFAA and addressed in *Nosal I*. *See* United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) [hereinafter *Nosal I*].

28. *Nosal II*, 844 F.3d at 1031.

fied person reported the access violations.[29] This report resulted in the termination of all access to Christian & Associates team members.[30]

In *Nosal I*, the court examined the misuse of log-in credentials during the time Christian & Associates staff were still partially employed by KFI.[31] The court held that the key term "'without authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all), and 'exceeds authoriz[ed] access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)."[32] For the five claims addressed in *Nosal I*, Nosal's work as an insider, with complete, unlimited access to KFI computers and data, placed him outside the scope of criminal charges under the CFAA, because the statute was not intended to address mere use violations.[33] The court held that despite KFI's internal policy against sharing passwords and information, because all parties were authorized by KFI to use the computers and the data as part of their employment, their conduct was not "without authorization."[34]

B. Claims in *Nosal II*

Initially, Nosal was charged with twenty criminal counts,[35] including eight under the CFAA, two trade secrets counts under the Economic Espionage Act, and one count of conspiracy.[36] Five of the eight CFAA claims were based on use violations by current employees, and were dismissed in *Nosal I*.[37] The government filed a second superseding indictment with three CFAA claims, two trade secrets claims, and one conspiracy claim.[38] The new CFAA claims were different from those in *Nosal I*, because former employees, with no access whatsoever, took and used a current employee's log-in credentials

29. *Id.*

30. *Id.*

31. *Nosal I*, 676 F.3d at 858.

32. *Nosal II*, 844 F.3d at 1034.

33. *Id.*

34. *Nosal I*, 676 F.3d at 864.

35. This Note does not seek to address the Economic Espionage Act, conspiracy charges, accomplice liability, or the court's back-and-forth regarding appropriate measures of restitution or attorney's fees. *See Nosal II*, 844 F.3d at 1031. Additionally, this note does not address in detail the appropriate language for jury instructions on "without authorization," instead focusing on the methods of interpretation. *See id.* at 1038–39.

36. *See Nosal II*, 844 F.3d at 1031.

37. *Nosal I*, 676 F.3d at 864.

38. *Nosal II*, 844 F.3d at 1031.

to run proprietary searches.[39] For this, prosecutors charged Nosal with violations of the CFAA under 18 U.S.C.A. § 1030(a)(4):

> Whoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such is not more than $5,000 in any 1-year period . . . shall be punished.[40]

The Federal District Court for the Northern District of California noted that these grounds were distinct from the claims in *Nosal I* and fell within the umbrella of hacking because Nosal attempted to circumvent the clear policy against use of the database.[41] Nosal was convicted on all counts.[42] He was sentenced to one year and one day in prison plus three years of supervised release, a $60,000 fine, $600 special assessment, and $828,000 in restitution to KFI.[43]

II. *NOSAL II* ANALYSIS

The Ninth Circuit examined "without authorization," and found that it is an unambiguous, non-technical term with a plain meaning.[44] The majority claims that "the interpretive fireworks" under 18 U.S.C. § 1030(a)(4) are reserved for the second prong, the meaning of "exceeds authorized access," as was discussed in *Nosal I*.[45] "[T]here has been no division among the circuits on the straightforward 'without authorization' prong of this section."[46] Interestingly, the majority opinion fails to address the stinging dissent on the meaning of that term. Regarding the implications of *Nosal II*, this Note addresses (1) the reasoning behind the majority's interpretation;[47] (2) the dissent's interpretation that "[t]his case is about password sharing";[48] and (3) supports the view put forth by the dissent that the majority has criminalized

39. *Id.* at 1031–32.

40. 18 U.S.C.A. § 1030(a)(4) (2016).

41. United States v. Nosal, 930 F. Supp. 2d 1051, 1060 (N.D. Cal. 2013).

42. *Nosal II*, 844 F.3d at 1032.

43. *Id.*

44. *Id.* at 1028.

45. *Id.* at 1033.

46. *Id.*

47. *See id.* at 1033–38.

48. *Nosal II*, 844 F.3d at 1048–58.

much of ordinary computer usage by not taking a realistic view of computer and pasword use.[49]

A. The Majority's Straight-Forward Approach

The majority focused on two Ninth Circuit cases to bind their interpretation, *Brekka* and *Nosal I*, before looking at case law from sister circuits supporting the approach that "without authorization" is "an unambiguous term that should be given its ordinary meaning."[50] In *Brekka*, the court analyzed the meanings of "without authorization" and "exceeds authorization" under §§ 1030(a)(2) and (a)(4).[51] "Because the CFAA does not define the term 'authorization,' we look[ ] to the ordinary, contemporaneous meaning of the term: permission or power granted by an authority."[52] In *Brekka*, as with *Nosal I* and *II*, the court distinguished actions taken by an employee while employed (and therefore authorized to use a computer) and actions taken *after* termination of employment (when acting "without authorization").[53] Following this reasoning, these courts held that "the plain language of the CFAA targets the unauthorized procurement or alternation of information, not its misuse or misappropriation."[54]

The majority used "classic statutory interpretation" to consider the plain and ordinary meaning of the term "without authorization."[55] Pulling definitions from Random House Unabridged Dictionary, Black's Law Dictionary, and the Oxford English Dictionary, the court summarized "authorization" to mean "permission or power granted by an authority."[56] The court found the use of a plain-language interpretation was clear because "the terms 'authorize, 'authorized' or 'authorization' are used without definition over 400 times in Title 18 of the United States Code," and therefore the term cannot be ambiguous.[57] This means that "someone, including an entity, can grant or revoke . . . permission.[58] Here, that entity was Korn/Ferry, and [Nosal's for-

49. *Nosal II* was remanded on the issues of attorney's fees and restitution, neither of which are the subject of this note. *See id.* at 1048.

50. *Id.* at 1028.

51. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009).

52. *Nosal II*, 844 F.3d at 1033 (quoting *Brekka*, 581 F.3d at 1132–36) (internal punctuation edited for clarity).

53. *Brekka*, 581 F.3d at 1133.

54. *Nosal II*, 844 F.3d at 1034 (quoting *Nosal I*, 676 F.3d 854, 863 (9th Cir. 2012)) (punctuation edited for clarity).

55. *Id.* at 1034.

56. *Id.* at 1035 (quoting RANDOM HOUSE WEBSTER'S UNABRIDGED DICTIONARY (6th ed. 2001), BLACK'S LAW DICTIONARY 159 (10th ed. 2014), and OXFORD ENGLISH DICTIONARY 107 (3d ed. 2014)).

57. *Id.*

58. *See id.*

mer secretary whose password was misused by Christian & Associates] did not have authority to give permission to former employees whose access had been categorically revoked by the company."[59] This supports the court's assessment that the CFAA does not target "insider" misuse of data because while the defendants used an insider's credentials, they had not been granted insider authority by KFI.[60]

The majority points out the consistency of this reasoning by reviewing interpretations of other appellate courts. The Second Circuit recognized that "'authorization' is a word 'of common usage, without any technical or ambiguous meaning.'"[61] Consistent with this interpretation, the Fourth Circuit held that an individual "accesses a computer 'without authorization' when he gains admission to a computer without approval. Similarly, . . . an employee 'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access."[62] Likewise, the Sixth Circuit held that "[c]ommonly understood . . . a defendant who accesses a computer 'without authorization' does so without sanction or permission."[63] In *Nosal II*, the Ninth Circuit acknowledged "that ill-defined terms may capture arguably innocuous conduct, such as password sharing among friends and family, inadvertently making criminals of large groups of people who would have little reason to suspect they are committing a federal crime," but ultimately found that "without authorization" is an unambiguous term.[64]

In essence, the majority created a clear and simple rule differentiating "without access" and "exceeds authorized access," and separating "insider" actions from crimes by "outsiders."[65] Plainly put, the rule from *Nosal II* is that an outside actor, without permission from a decision making authority, acts "without access" when he or she attempts to take or alter information on a protected computer.[66] The court held that the authority must be granted by a sanctioning power, either an individual or an entity, with proprietary ownership of the computer or data.[67]

59. *Id.*

60. *See Nosal II*, 844 F.3d at 1036.

61. *Id.* at 1050 (quoting United States v. Morris, 928 F.2d 504, 509–11 (2d Cir. 1991)).

62. *Id.* at 1052 (quoting WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (internal citations omitted)).

63. *Id.* (quoting Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 303–04 (6th Cir. 2011)).

64. *Id.* at 1038 (quoting *Nosal I*, 676 F.3d 854, 859 (9th Cir. 2012) (internal punctuation omitted)).

65. *See id.* at 1051–52.

66. *See Nosal II*, 844 F.3d at 1033–35.

67. *Id.* at 1037.

B. The Dissent's Practical Approach

The dissent fundamentally disagrees with the majority's interpretation in *Nosal II*. While the majority sees this as the work of outside hackers using fraudulent credentials, the dissent sees this as a case of password sharing among friends and former co-workers, in violation of an employer use policy.[68] The dissent characterizes the actions of Nosal and his compatriots in *Nosal II* as "only slightly different" from the insider actions dismissed in *Nosal I*.[69] The dissent argues that the majority's holding "jeopariz[es] most password sharing" by "los[ing] sight of the anti-hacking purpose of the CFAA, and despite our warning, threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens."[70] The dissent's analysis rejects the majority's definition of "without authorization," and substituted it with a definition where authorization to use a computer or data could be granted by *either* the system owner *or* an authorized user.[71] The dissent's definition works to narrow the reach of the statute only to malicious behavior.

Distilling the facts, the dissent argues that the actions by Christian & Associates staff to gain access to proprietary KFI search databases was done by borrowing the password of a present employee who was authorized to access the database.[72] Incongruously,

> [i]t would not have been a violation of the CFAA if they had simply given [the KFI employee] step-by-step directions, which she then followed. So the question is whether because [Christian & Associates] instead used [the employee's] password with her permission, they are criminally liable for access 'without authorization' under the Act.[73]

Unlike the majority, the dissent is not comfortable with this bright-line because simply failing to receive authorization from the owner of the proprietary information runs the risk of criminalizing large swaths of common behavior.

Applying that standard, the dissent found that the majority's "broader reading" of the CFAA results in a world in which "millions of unsuspecting individuals would find that they are engaging in criminal conduct. . . The majority does not provide, nor do I see, a workable line which separates the consensual password sharing in this case from the consensual password shar-

68. *See id.* at 1053–54.

69. *Id.* at 1049.

70. *Id.*

71. *See id.*

72. *Nosal II*, 844 F.3d at 1049.

73. *Id.*

ing of millions of legitimate account holders[.]"[74] Rejecting this result, the dissent argues that password sharing is not the type of "hacking" that the CFAA was enacted to penalize.[75]

As the majority did, the dissent notes that "without authorization" is used multiple times within the CFAA but is not defined.[76] The phrase appears in 18 U.S.C. §§ 1030(a)(2)(C) and (a)(4). A key difference between the majority and the dissent is whether "without authorization" should be read considering the entire statute, or specifically focused on (a)(4). Subsection (a)(2)(C) "is the broadest provision of the CFAA" focusing on "intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer."[77]

The dissent argues for a cautious definition of "without authorization" because it will not only apply to (a)(4) as in *Nosal II* but also to (a)(2)(C).[78] Section 1030(a)(2)(C) lacks the requirement of culpable intent, and broadly applies to "nearly all desktops, laptops, servers, smart-phones, . . . or any other Internet-enabled device, even some thermostats qualify as protected."[79] So by interpreting "without authorization" to "include[ ] common practices like password sharing, millions of our citizens would become potential federal criminals overnight."[80]

In a string of examples, the dissent illustrates the error in the majority's simplistic idea that acting "without authorization" occurs whenever the system *owner* does not consent to the use.[81] In each example, the dissent shows how "normal" and "acceptable" computer usage, like logging onto an account on behalf of a friend or spouse, should be considered criminal password sharing unauthorized by the system *owner's* terms of use.[82] Drawing a parallel to the earlier decision in *Nosal I*, this is exactly the type of behavior that the court attempted to *avoid* criminalizing but which ended up criminalized by the majority.[83]

To solve the over-criminalization problem created by the majority's broad reading, the dissent suggests that "the best reading of 'without authorization' in the CFAA is one that gives a narrow reach: a person accesses an

74. *Id.* (quoting *Nosal I*, 676 F.3d 854, 859 (9th Cir. 2012)).

75. *Id.*

76. *Id.* at 1050.

77. *Id.* (quoting 18 U.S.C. § 1030(a)(2)(C); also quoting *Nosal I*, 676 F.3d at 859) (internal punctuation omitted for clarity).

78. *Nosal II*, 844 F.3d at 1050 (quoting *Nosal I*, 676 F.3d at 861).

79. *Id.*

80. *Id.* at 1051.

81. *Id.*

82. *Id.*

83. *Id.*

account 'without authorization' if he does so without having the permission of *either* the system owner *or* a legitimate account holder."[84] Arguing that this fits the purposes of the CFAA more clearly (targeting hackers), the dissent posits that "the statute would cover only those whom we 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."[85] This, the dissent argues, makes particular sense because of Congress's focus on paralleling hacking with "breaking and entering."[86]

Finally, the dissent reasons that the an interpretation of "authorization" that includes authorization by either the system owner or a legitimate user, would serve the same purposes and legislative intent as the definition adopted by the majority while also working within the framework of judicial lenity.[87] Finding that the majority's decision creates ambiguity over *who* may grant authorization, the rule of lenity encourages adoption of the construction that prevents the criminalization of innocent behavior.[88] Therefore, the dissent argues for the narrower reading under the rule of lenity so that individual citizens will be on notice about which computer-related behaviors are potentially criminal.[89] The dissent examines behavior in which a friend or family member shares a password and "would most certainly believe—and with good reason—that his access had been 'authorized' by the account holder" but which *would* be criminal under the majority's position.[90] Under the majority rule, this sort of innocent behavior is not distinguished from Nosal's "unscrupulous" behavior, making both equally criminal.[91] Therefore, the dissent reasons, the "natural interpretation" of most computer users conflicts with the common-sense definition that the majority puts forth, and "[t]hat alone should defeat the majority's conclusion."[92]

Further, the dissent finds that the majority's position "would base criminal liability on system owners' access policies," an approach previously rejected in *Nosal I* because they are "lengthy, opaque, subject to change and

84. *Nosal II*, 844 F.3d at 1051.

85. *Id.*

86. *Id.* (quoting H.R. Rep. 98-894, 20, 1984 U.S.C.C.A.N. 3689, 3706).

87. *Id.* at 1053.

88. *Id.* (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001), which "concluded that the meaning of the term 'without authorization' in the CFAA 'has proven to be elusive' ").

89. *Id.*

90. *Nosal II*, 844 F.3d at 1054.

91. *See id.*

92. *Id.*

seldom read."[93] The dissent points out why this is problematic: private companies would essentially be capable of criminalizing access violations by refusing to authorize end users and writing access policies clearly forbidding password sharing.[94]

The "rule [of lenity] ensures that the clear (and public) words of Congress—not the obscure policies of system owners—delimit their scope."[95] Therefore, the dissent argues that "the majority opinion contains no limiting principle," because, while "the majority disavows the effects of its decision aside from dealing with former employees . . . the statute says nothing about employment," and may result in selective or arbitrary enforcement.[96] Even if the opinion only applied in employment cases, the dissent points out situations where password sharing between current and former employers may actually *benefit* the employer.[97] This inconsistency "is a recipe for giving large corporations undue power over their rivals, their employees, and ordinary citizens, as well as affording such indiscriminate power to the Justice Department."[98] The dissent points out, for example, that in *Nosal II*, a former employee with millions of dollars on the line was investigated by KFI with the help of ex-FBI agents while considering both the criminal and civil penalties under the CFAA and other laws.[99] Stopping short of accusing the employer of wrongdoing, the dissent shows that this interpretation of "without authorization," in unscrupulous and well-funded hands, could lead to improper prosecutorial motives and misapplication of the CFAA towards individuals most would not consider "hackers."[100]

C. Examining the *Nosal II* Implications in Modern Computing

The dissent presents a compelling argument that the majority's rule—that only the system owner may grant "authorization"—over-criminalizes common computer use and password sharing. Without going so far as to

93. *Id.* (quoting *Nosal I*, 676 F.3d 854, 860 (9th Cir. 2012)).

94. *Id.*

95. *Id.* It is worth noting here, that the dissent seems to imply that this concern would be minimized were the CFAA a purely civil statute, but because it is criminal it is particularly egregious.

96. *Nosal II*, 844 F.3d at 1055.

97. *Id.* at 1055–56. For example, consider a current employee calling a former employee for help accessing a rarely used file that the former employee remembers only roughly where to find it. Rather than spending a long time on the phone trying to help the current employee navigate the system, the former employee might use the current employee's login credentials to find the file and help the company.

98. *Id.* at 1056.

99. *Id.* at 1056–57.

100. *See id.* at 1057.

advocate for a complete rewrite of the CFAA, the definition of "without authorization" should be carefully examined because it inadvertently criminalizes a lot of perfectly "normal" computer activity. Defining "authorization" to mean that an end user may be authorized by *either* the system owner *or* an authorized user produces a narrow reading of the statute that avoids over-criminalizing.[101] This definition protects common use in the criminal context.

1. Almost All Americans Share Passwords for Systems They Do Not "Own"

The majority and dissent fundamentally disagree over whether this is a mere password sharing case.[102] However, on simplest version of the facts, Nosal and his partners at Christian & Associates borrowed an active, authorized KFI password and misused an existing employee's account in violation the KFI terms of use.[103] Computer users nationwide click rapidly past end-user license agreements and share passwords regularly, but the average American does not intend to commit a federal crime in doing so. The rule of lenity should protect citizens where the law clearly criminalizes commonplace behavior.

The dissent considers situations where an individual inadvertently breaks the law.[104] For example, consider a situation where an individual who is authorized to use a Netflix account, shares his or her log-in credentials with non-paying members. Or, a situation where a law student holds authorized student log-in credentials with LexisNexis or Westlaw, which allow unlimited free searches, and shares those log-in credentials with a friend who practices at a small firm on a pay-as-you-go plan. On their face, both of these maneuvers are unscrupulous and clearly designed to short the companies of revenue and skirt their end user license agreements. However, it is unlikely that either the Netflix user or law student would believe their behavior was criminal. In fact, a 2015 study revealed that prior to Netflix's new "multiple accounts" policy, two-thirds of all users shared their accounts with others, which violated the Netflix policy.[105] Those users may have believed that Netflix could cancel their account, charge them a fee, or potentially sue them. These users would be shocked to discover their case paralleled with *Nosal II*'s $828,000 restitution and jail time.[106] These examples are more intentional and include a small degree of moral objection that many of the dis-

101. *See id.* at 1051.

102. *Nosal II*, 844 F.3d at 1048.

103. *See id.* at 1030–31.

104. *Id.* at 1051.

105. Devin Coldewey, *Sharing Netflix Account with Friends? You're not the Only One*, NBC News (Oct. 28, 2016, 3:03 PM), http://www.nbcnews.com/tech/internet/two-thirds-netflix-users-share-access-others-n396671.

106. *Nosal II*, 844 F.3d at 1032. The restitution award was vacated in the amended opinion. *Id.* at 1048.

sent's examples lacked (like a wife accessing a husband's bank account at his request[107]), but do not facially appear *criminal* in nature.

2. Criminal Culpability under the CFAA Should Only Apply to Hackers

The definition of "without authorization" should allow either a system owner or an authorized user to grant permission for use. Not all sections of the CFAA require criminal culpability; therefore, a broad application risks capturing innocent conduct, contrary to congressional intent for the CFAA to target hackers.[108] For 18 U.S.C. § 1030(a)(2)(C), *no criminal culpability is required.*[109] While the majority attempts to draw bright lines, or narrow its holding to employment cases, the definition it supported for "without authorization" will apply equally to §§ (a)(2)(C) and (a)(4).[110] But § (a)(4) requires "knowingly or with intent to defraud," while § (a)(2)(C) requires no culpable intent.[111] Therefore, anyone who "accesses a computer without authorization [from the system *owner*], and thereby obtains . . . information from any protected computer . . . shall be punished."[112] Regardless of the application of "without authorization" to § (a)(4), this term will be applied equally throughout the CFAA and creates a situation where the law is no longer targeting hackers but general misuse. The interpretation runs completely contrary to the Ninth Circuit's opinion in *Nosal I*.[113]

Nationwide, courts have identified a conflict between the plain-language of the CFAA and the intent by Congress to target hackers, which will take more than a small definitional change to revise.[114] But weighing easy fixes to

107. *Id.* at 1055.

108. *See id.* at 1051.

109. 18 U.S.C. § 1030(a)(2)(C).

110. *Nosal II*, 844 F.3d at 1050.

111. *Compare* 18 U.S.C. § 1030(a)(4), *with* 18 U.S.C. § 1030(a)(2)(C).

112. 18 U.S.C. § 1030(a)(2)(C).

113. *See Nosal I*, 676 F.3d 854, 863 (9th Cir. 2012).

114. *See* iPhone Application Litig., 2011 U.S. Dist. LEXIS 106865, at *36–37 (citing Bose v. Interclick, Inc., No. 10 Civ. 9183 (DAB), 2011 U.S. Dist. LEXIS 93663, at *12–14 (S.D.N.Y. Aug. 17, 2011)) (the court dismissed the complaint but recognized tension between individual use-violations, end-user license agreements, the challenge to determine damages, and more); *see also* United States v. Rodriguez, 628 F.3d 1258, 1265 (11th Cir. 2010) (affirming the conviction of a Social Security Administration teleservices agent who accessed the SSA database to obtain information about women in whom he was romantically interested, and then pursued those women through disquieting phone calls or unannounced home visits); United States v. Ivanov, 175 F. Supp. 2d 367, 373–75 (D. Conn. 2001) (denying a motion to dismiss filed by the defendant, a Russian hacker, who allegedly violated the CFAA by stealing network passwords and attempting to extort money from the company in exchange

limit the scope of this law to behavior that is truly *intended* to circumvent policies (i.e., actual "hacking"), adopting a definition for "without authorization" that results in a narrow reach would protect all well-intentioned Netflix password sharers from *criminal* liability.

III. CONCLUSION

The Ninth Circuit clarified the CFAA by defining "without authorization," explaining that it is the grant of permission by a system owner.[115] The dissent argued that this definition criminalized common and innocent computer usage.[116] This definitional debate hinged on whether the party viewed Nosal and his compatriots as "hackers," or whether this was merely a case of password sharing.[117] Looking forward, the dissent provided an alternative definition for "without authorization," wherein a system owner *or* an authorized user could grant permission for computer-use.[118] Because not all crimes under the CFAA require criminal culpability, the majority's broad definition risks trapping people criminally who acted without criminal intent. Therefore, because the rule of lenity encourages interpreting statutes to provide citizens with notice of criminal acts, I advocate for a wide-spread adoption of the dissent's definition of "without authorization" that results in an appropriately narrow reach of the statute.

---

for making their network secure again); *see also* Andrew T. Hernacki, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U.L. REV. 1543, 1562–64 (2012) (citing the above cases to illustrate the problems with the present incarnation of the CFAA and offering proposed amendments to bring it back in line with the mission of targeting hackers).

115. *Nosal II*, 844 F.3d at 1035.

116. *See id.* at 1053–54.

117. *See id.*

118. *Id.*