THE UNEXPECTED SCOPE OF THE CFAA: AND HOW NETFLIX USERS COULD BE COMMITTING A FEDERAL CRIME

By Michael Levy†

I. INTRODUCTION

Can allowing access to a personal account be a federal crime? Is a former Netflix subscriber banned from accessing Netflix on another account after deleting his/her account? The recent Ninth Circuit opinion has led to such a conclusion. In *United States v. Nosal (II)*, David Nosal was convicted on multiple counts of violating the Computer Fraud and Abuse Act (hereinafter CFAA) after his co-conspirators (Becky Christian and Mark Jacobson) accessed his former company's system using a

† Associate Editor, *International Comparative Policy and Ethics Law Review*; B.S. Northeastern University; J.D. Candidate 2018, Benjamin N. Cardozo School of Law. The author would like to thank his friends and family for their love and support. He would like to especially thank his faculty note advisor, Jessica Roth, for investing her valuable time and providing him with her esteemed insight. He would also like to express appreciation to his friend, Taylor Montanari, for motivating him to work hard and supporting him in his endeavors to reach his goalst

current employee's (Jacqueline Froehlich-L'Heureaux) credentials.[1] The Ninth Circuit held that "Nosal, a former employee whose computer access credentials were revoked by Korn/Ferry acted 'without authorization' in violation of the CFAA when he or his former employee co-conspirators used the login credentials of a current employee to gain access to computer data owned by the former employer and to circumvent the revocation of access."[2]

The Computer Fraud and Abuse Act was passed in 1984 as an "anti-hacking" law.[3] The House Report explains the purpose of the bill, stating that the criminal justice system is left powerless to the emergence of technology related crimes. The report goes on stating, "Compounding this is the advent of the activities of so-called 'hackers' who have been able to access (trespass into) both private and public computer systems, sometimes with potentially serious results."[4] The CFAA was enacted to punish those people for accessing computers without authority.[5]

In 2011, David Nosal moved to dismiss his indictment of violating the Computer Fraud and Abuse Act.[6] The Ninth Circuit held "that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly."[7] At issue in *Nosal (I)* were the actions of Becky Christian and Mark Jacobson while they still worked at Korn/Ferry.[8] In 2015, David Nosal appealed his conviction under the CFAA regarding the acts of his co-conspirators after they left Korn/Ferry.[9] The court held that the actions taken after leaving Korn/Ferry were in violation of the CFAA, and affirmed Nosal's conviction.[10] The Ninth Circuit's broad reading of the Computer Fraud and Abuse Act in *United States v. Nosal (II)* undermines the purpose of the Act and creates a legal shield for big network companies.

II. BACKGROUND

David Nosal worked as a high-level regional director at

1 United States v. Nosal (*Nosal (II)*), 844 F.3d 1024 (9th Cir. 2016).
2 *Id*. at 1038.
3 H.R. REP. 98-894, 1984 U.S.C.C.A.N. 3689.
4 1984 U.S.C.C.A.N. at 3695.
5 18 U.S.C. §1030 (2008).
6 United States v. Nosal (*Nosal (I)*), 676 F.3d 854 (9th Cir. 2012).
7 *Id*. at 863.
8 *Id*.
9 *Nosal (II*), 844 F.3d 1024.
10 *Id*.

Korn/Ferry International.[11] Korn/Ferry is a global executive search firm known for headhunting corporate jobs. In 2004, Nosal was passed over for a promotion and decided to leave Korn/Ferry. After announcing his intention to leave, Korn/Ferry entered negotiations with Nosal. After deliberation, Nosal agreed to stay on as a private contractor for a year and finishes searches in which he already began. Nosal signed a basic non-competition agreement and was "'given a lot of money' to 'stay out of the market.'"[12] As part of the agreement, Nosal's credentials from Korn/Ferry's search system, Searcher, were revoked. However, if Nosal needed to run a search he could ask a fellow employee to run it for him.

After deciding to leave Korn/Ferry, Nosal convinced Becky Christian, Mark Jacobson and Jacqueline Froehlich-L'Heureaux ("FH") to leave with him to create a competing company. Since Nosal could no longer access Searcher, he relied on Christian and Jacobson to run searches and pass the information along to him. They began to download confidential information to build a base in which to build their competing business. Although Christian and Jacobson had authorized access to the system, by passing along the information to Nosal, they violated Korn/Ferry's confidentiality and computer use policies.[13] This was the issue in *United States v. Nosal (I)*.[14] The Ninth Circuit had to determine if by violating Korn/Ferry's confidentiality and computer use policies, Christian and Jacobson had also violated the Computer Fraud and Abuse Act by "exceeding" their 'authorized access." The court held that "[b]ecause Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail[end] to meet the element of "without authorization, or exceeds authorized access" under 18 U.S.C. §1030(a)(4)."[15]

In January of 2005, Becky Christian left Korn/Ferry International.[16] Under the direction of David Nosal, she opened her own executive search firm, called Christian & Associates. Nosal retained eighty percent of the fees. A few months later, Mark Jacobson left Korn/Ferry, and the three began working for their new clients. However, Christian & Associates lacked access to Searcher. After Nosal, Christian and Jacobson left Korn/Ferry, all their credentials were revoked. Without access to Searcher, Christian & Associates would have a difficult time finding candidates to fill the corporate positions. Foreseeing this problem, Nosal asked FH to remain at Korn/Ferry. Since FH still worked at Korn/Ferry, she still had authorized access to Searcher. On three separate

11 *Id*. at 1030.
12 *Id*.
13 *Id*. at 1031.
14 *Nosal (I)*, 676 F.3d at 854.
15 *Id*. at 864.
16 *Nosal (II)*, 844 F.3d at 1030.

occasions, Nosal and his co-conspirators ran a search using FH's credentials. They believed that since FH had never run a search before, it would be easier to just log into Searcher using her credentials than trying to talk her through the process. In April and July 2005 Christian logged into Searcher using FH's credentials, and later in July 2005 Jacobson did the same. In July of 2005, after being tipped off by an anonymous email, Korn/Ferry contacted government authorities.[17]

A. UNITED STATES V. NOSAL (II) - MAJORITY

United States v. Nosal (II) was argued on October 20, 2015, and filed on July 5, 2016.[18] The Ninth Circuit had to determine whether the actions taken by Nosal, Christian, Jacobson and FH violated the Computer Fraud and Abuse Act. The court also had to make other determinations regarding the Economic Espionage Act, but this article is only focusing on the controversial holding regarding the CFAA. "Put simply, [the court had] 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."[19] As noted above, the actions at issue in this case are the actions taken by Nosal's co-conspirators after they left Korn/Ferry International.

The law at issue in this case is 18 USC §1030(a)(4).[20] This section of the Computer Fraud and Abuse Act states that 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 use is not more than $5,000 in any 1-year period;

has violated the Act.[21] The court had to determine if the actions of Christian and Jacobson fell within the statute.

In her opinion, Justice McKeown first establishes that "exceeds authorized access" and "without authorization" are to be defined differently under the CFAA.[22] In *LVRC Holdings LLC v. Brekka*, the Ninth Circuit distinguished the two phrases.[23] "Exceeds authorized

17 *Id*. at 1030-31.
18 *Id*.
19 *Id*. at 1030.
20 *Id*.
21 18 U.S.C §1030(a)(4).
22 *Nosal (II)*, 844 F.3d at 1029-30.
23 LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

access refers to inside hackers, whereas "without authorization" refers to outside hackers. An inside hacker is a person who has authorized access to a computer, but accesses unauthorized information. An outside hacker is a person who has no authority to access the computer at all.[24]

In *Nosal (I)*, "[d]istinguishing between access restrictions and use restrictions, [the court] concluded that the 'exceeds authorized access' prong of §030(a)(4) of the CFAA 'does not extend to violations of [a company's] use restrictions.'"[25] In other words, the CFAA does not extend to company confidentiality and computer use regulations. Since Christian and Jacobson had access to the information while they still worked at Korn/Ferry, they were considered inside hackers. Christian and Jacobson may have broken Korn/Ferry's computer use policies, but they had authorized access to the information, thus they did not "exceed authorized access."[26]

The actions involved in this case occurred after Christian and Jacobson left Korn/Ferry.[27] Therefore, they are to be viewed as outside hackers. This means the court needs to determine if they accessed Searcher "without authorization."

There is no definition for "without authorization" in 18 U.S.C. §1030.[28] Therefore, the court had to determine how to define "without authorization" according to the law.[29] The court had to first determine how to define "authorization." The court uses dictionaries, other circuit decisions, and the plain ordinary language to define "authorization." "Authorization" ultimately means "[o]fficial permission to do something; sanction or warrant."[30]

Using the straight forward definition of "authorization," the court concluded "that 'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[31] The court continued that the "definition 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."[32] The court concluded that if "without authorization" means "without permission," then logically, once permission has been revoked, any further access

24 *Id*. at 1133.
25 *Nosal (II)*, 844 F.3d at 1029.
26 *Nosal (I)*, 676 F.3d at 863-64.
27 *Nosal (II)*, 844 F.3d at 1029.
28 18 U.S.C. §1030.
29 *Nosal (II)*, 844 F.3d at 1034-35.
30 *Authorization*, BLACK'S LAW DICTIONARY, 159 (10th ed. 2014).
31 *Nosal (II)*, 844 F.3d at 1028.
32 *Id*.

would be unauthorized.

The court states:

> Our analysis is consistent with that of our sister circuits, which have also determined that the term "without authorization" is unambiguous. Although the meaning of 'exceeds authorized access' in the CFAA has been subject to much debate among the federal courts, the definition of "without authorization" has not engendered dispute. Indeed, Nosal provides no contrary authority that a former employee whose computer access has been revoked can access his former employer's computer system and be deemed to act with authorization.[33]

This conclusion by the Ninth Circuit is supported by other circuit court rulings. In *United States v. Valle*, the Second District held that "common usage of 'authorization' suggests that one 'accesses a computer without authorization' if he accesses a computer without permission to do so at all."[34] The Fourth Circuit concluded "based on the ordinary, contemporary, common meaning of 'authorization,' that an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer. Thus, he accesses a computer 'without authorization' when he gains admission to a computer without approval."[35] The Sixth Circuit also supports this holding in its holding in *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, stating "a defendant who accesses a computer 'without authorization' does so without sanction or permission."[36]

The definition of "authority" requires that someone, or some entity, be able to grant access into the computer. "Here, that entity was Korn/Ferry and FH had no mantle or authority to give permission to former employees whose access had been categorically revoked by the company. There is no question that Korn/Ferry owned and controlled access to its computers, including the Searcher database, and that it retained exclusive discretion to issue or revoke access to the database."[37] According to the court, only Korn/Ferry can authorize access into Searcher, but not an employee who has authorized access. "Nosal and his co-conspirators acted 'without authorization' when they continued to access Searcher by other means after Korn/Ferry rescinded permission to access its computer system."[38]

Justice McKeown also kept in mind the reasoning behind Nosal (I):

---

33 *Id*. at 1036-37.

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

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

36 Pulte Homes, Inc. v. Laborers' int'l Union of N. Am., 648 F.3d 295, 303-04 (6th Cir. 2011).

37 *Nosal (II)*, 844 F.3d at 1035-36.

38 *Id*. at 1034.

> We are mindful of the examples noted in Nosal I—and reiterated by Nosal and various amici—that ill-defined terms may capture arguably innocuous conduct, such as password sharing among friends and family, inadvertently "mak[ing] criminals of large groups of people who would have little reason to suspect they are committing a federal crime."[39]

The court, on numerous occasions expressed that this holding would only affect former employees whose access had been revoked. But, is that the case?

B. UNITED STATES V. NOSAL (II) – DISSENT

The dissent, written by Justice Reinhardt, seems to think that the majority completely missed the mark.[40] He claims that '[t]his case is about password sharing."[41] The dissent claims that the majority erred by having such a broad definition of "without authorization" under 18 USC §1030, and makes several compelling arguments.

The first argument put forward by the dissent is that this ruling goes against what the court held in *Nosal (I)*.[42] In *Nosal (I)*, the court "reject[ed] the approach of a few other circuits which had interpreted the CFAA looking 'only at the culpable behavior of the defendants before them, and fail[ing] to consider the effect on millions of ordinary citizens.'"[43] The dissent continues to explain, "[i]n doing so, we stated that they turned the CFAA into a 'sweeping Internet policing mandate,' instead of maintaining its 'focus on hacking.'"[44] The holding in *Nosal (I)* was supposed to narrow the scope of the Computer Fraud and Abuse Act to acts involving hacking, not to criminalize everyday activities of millions of Americans. For the court to now claim that password sharing violates the CFAA, it "make[s] the millions of people who engage in this ubiquitous, useful, and generally harmless conduct into unwitting federal criminals."[45]

The second argument put forward by the dissent is that however wrong Nosal's and his co-conspirators' actions were, they did not fall under the purpose of the Computer Fraud Abuse Act.[46] The purpose of the CFAA was to prevent hacking. The dissent quotes the House Report quoted above, stressing that the Act was designed to prevent hackers who

---

39 *Id*. at 1038 (quoting *Nosal (I)*, 676 F.3d 854, 859).
40 *See id*.
41 *Id*. at 1048 (Reinhardt, J., dissenting).
42 *See id*. at 1048-49 (Reinhardt, J., dissenting).
43 *Id*. at 1048 (Reinhardt, J., dissenting) (quoting *Nosal (I),* 676 F.3d at 862).
44 *Id*.
45 *Id*.
46 *Id*. at 1049 (Reinhardt, J., dissenting) (quoting *Nosal (I*), 676 F.3d 854, 862).

"break and enter" into a computer. The majority opinion "loses 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."[47] The dissent strengthens this point by pointing out that "[i]t would not have been a violation of the CFAA if they had simply given FH step-by-step directions, which she then followed."[48] These demonstrates how this case is actually about password sharing. FH shared her password with Christian and Jacobson, who then accessed Searcher. Under the majority opinion, this is in violation of the CFAA. However, if FH had conducted the search herself and passed the information along, this action would have fallen under *Nosal (I)* and would have not been a violation of the CFAA. By using credentials willingly given to them by someone who had authorized access to the system, Christian and Jacobson violated the CFAA.

The third argument put forward by the dissent, is that when a word or phrase appears in a statute, it has the same meaning throughout the statute.[49] The dissent focuses on another part of the statute; Section 1030(a)(2)(c). Section 1030(a)(2)(c) states that "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" violates the CFAA.[50] Section 1030(e)(2)(b) defines a "protected computer" as "a computer . . . which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[51] In reality, this covers every computer and other devices. Since words and phrases must be defined the same way within each statute, "[t]he construction that [the court] adopt[s] in Nosal's case will apply with equal force to all others, and the reading of 'without authorization' [the court] adopt[s] for subsection (a)(4) will apply with equal force to subsection (a)(2)C)."[52] Therefore, "[s]ubsection (a)(2)(C) criminalizes nearly all intentional access of a 'protected computer' without authorization."[53] Under this interpretation of the law, anyone who accesses a "protected computer," whether given the password to access the "protected computer" or not, would be in violation of the CFAA. Many Americans' daily activities would make them criminals under the Computer Fraud and Abuse Act.

---

47 *Id*.
48 *Id*.
49 *Id*. at 1053-54 (Reinhardt, J., dissenting).
50 18 U.S.C. §1030.
51 *Id*.
52 *Nosal (II)*, 844 F.3d at 1052 (Reinhardt, J., dissenting).
53 *Id*. at 1050 (Reinhardt, J., dissenting).

The dissent also emphasizes that "[t]he majority is wrong to conclude that a person necessarily accesses a computer account 'without authorization' if he does so without the permission of the system owner."[54] As long as one authorized party gives permission, the access is with authorization. The dissent supports this broader reading of the statute with examples of everyday activities performed by many Americans, such as, logging into a colleague's account while they are unable to come into the office, checking a friend's email and/or Facebook page, a spouse logging into a bank account to pay a bill, and violating the system owner's access policy by accessing a personal email account.[55] According to the dissent, all these acts are suspect of violating the Computer Fraud and Abuse Act under the majority's holding. "Thus, the 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."[56] Since Christian and Jacobson were given permission to enter Searcher by FH, their access to the system was with authority.

The dissent draws no distinction between former employees and non-employees. Justice Reinhardt emphasizes that it is "password sharing" that is the central issue of this case.[57] It is of no importance that Nosal, Christian and Jacobson were former employees of Korn/Ferry whose access to the system was revoked. Christian and Jacobson used FH's credentials, with her permission, to access a system that she had authority to access. This is synonymous with FH sharing her password with Christian and Jacobson. "Accordingly, [the dissent] would hold that consensual password sharing is not the kind of 'hacking' covered by the CFAA. That is the case whether or not the voluntary password sharing is with a former employee and whether or not the former employee's own password had expired or been terminated."[58]

III. ANALYSIS

A close analysis of *United States v. Nosal (II)* reveals some troubling conclusions. Both the majority and the dissent make strong arguments supported by case law and statutory interpretation. However, each side has a different view of what the central issue of the case is: the majority views the central issue as whether an employee whose access was revoked can enter the system using another employee's credentials,

54 *Id*. at 1051 (Reinhardt, J., dissenting).
55 *Id*.
56 *Id*.
57 *Id*. at 1048 (Reinhardt, J., dissenting).
58 *Id*. at 1049 (Reinhardt, J., dissenting).

whereas the dissent views the central issue as password sharing.[59] The majority opinion is the law, but is that the purpose of the Computer Fraud and Abuse Act?

A. WHAT IS THE PURPOSE OF THE COMPUTER FRAUD AND ABUSE ACT?

The Computer Fraud and Abuse Act was passed in 1984 as an "anti-hacking" law.[60] At the time the bill was passed, there was "no specific federal legislation in the area of computer crime. Any enforcement action in response to computer-related crime [had to] rely on statutory restrictions that were designed for other offenses, such as mail fraud (18 U.S.C 1341) or wire fraud (18 U.S.C. 1343) statutes."[61] The Housing Report cites two cases in which the prosecutor got lucky on some minor detail to be able to press charges. In the first case, *U.S. v. Seidlitz*, the defendant accessed a former employer's account to steal information. If he had not made two of the fifty access calls over state lines, it would not have been a federal crime. The second case mentioned by the report is an unreported case where the defendant was a former employee of the Federal Reserve. After entering the private sector, he continued to access the Federal Reserve's system to steal money. If he had not affected interstate commerce, the federal government would have been powerless against him. The two cases were used to show the great desire for federal computer fraud legislation.[62]

There were no laws regulating computer usage prior to the adoption of the Computer Fraud and Abuse Act.[63] Law enforcement was powerless against "hackers," and the American people did not know the limits to their own computer usage. The Committee stated that "[o]ver the past quarter of a century [the American] society has witnessed an amazing technological transformation. The computer ha[d] become an integral part of everyday lives, critical to [the] national defense, financial transactions, and information transmissions."[64] Computers and computer systems have become commonplace in American society, and there were no laws to govern computer usage. "The Committee concluded that the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access to them, require a clearer statement of proscribed activity."[65]

---

59 *Id*.
60 H.R. REP. NO. 98-894, (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689.
61 *Id*. at 3691.
62 *Id*. at 3691-92.
63 *Id*.
64 *Id*. at 3694.
65 *Id*. at 3692.

"As computer networking and distributed data processing [grew] so has the 'user-friendliness' of accessing computer resources through networks."[66] As more and more Americans used computers and network systems, the desire for protection grew. Even though "[m]ost systems use some sort of variant of an identification code/password system," the number of hacking incidents increased.[67] The Housing Committee concluded that "it has been the realization that criminals possess the capability to access and control high technology processes vital to our everyday lives which has spurred the recent alarm over computer-related crime."[68] It is clear from the Housing Report that the Computer Fraud and Abuse Act was passed in order to criminalize "hacking" and other computer related crimes, not to punish those who access a system with the permission of an authorized user.

B. WHAT NOSAL (II) MEANS TODAY

After the majority opinion in *United States v. Nosal (II)*, it is not abundantly clear on what the law regarding "without authorization" under the Computer Fraud and Abuse Act really means.[69] The Court tries to limit the scope of *Nosal (II)* to "former employees whose computer access was categorically revoked and who surreptitiously accessed data owned by their former employer."[70] But, the CFAA mentions the word "employee" only once, and it is not in 18 USC §1030(a)(4).[71] 18 USC §1030(a)(1) states, whoever:

> having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data . . . with reason to believe that such information so obtained could be used to the injury of the United States . . . willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted . . . or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.[72]

The only time the word "employee" is used throughout the entirety of the

---

66 *Id*. at 3696.

67 *Id*.

68 *Id*. at 3694.

69 *Nosal (II)*, 844 F.3d 1024

70 *Id*. at 1038.

71 18 USCA §1030 [West]. 18 U.S.C.A. §1030 [West]. [Remove the bracketed "West" if citing to current official code; add year after "West" if citing to current unofficial code]

72 *Id*. (emphasis added).

Computer Fraud and Abuse Act is in reference to an "employee of the United States."[73] Does 18 USC §1030(a)(4) only apply to former employees? The Ninth Circuit attempted to clarify the scope of the CFAA in *Facebook, Inc. v. Power Ventures, Inc.*.[74]

In *Facebook, Inc. v. Power Ventures, Inc.*, Power Ventures operated the social networking site of Power.com. Power.com would aggregate all the user's social networking accounts into one account on Power.com. The idea was for each user to connect with all their social networking contacts all on one page. In December of 2008, Power.com began a promotional campaign to get Facebook users to join Power.com. Power.com promised to pay the first 100 people who brought in 100 friends from Facebook, $100 each. In order to do this, Power.com members would click on the promotional "Yes, I do" button. This button would create an event, photo or status on the user's Facebook page. When users clicked the "Yes, I do" button, a message was sent to all the user's Facebook friends. In some instances, depending on the privacy settings of each user, an email was generated and sent to the user's Facebook friends. The emails were sent to external email addresses. They were form emails inviting the recipients to an event hosted by Power.[75] "The 'from' line in the e-mail stated that the message came from Facebook; the body was signed, 'The Facebook Team.'"[76]

On December 1, 2008, Facebook became aware of the actions by Power.com, and sent a "cease and desist" letter to Power Ventures, ordering it to stop its activities.[77] Facebook attempted to persuade Power Ventures to sign its 'Developer Terms of Use Agreement', and to join Facebook. When Power Ventures refused, Facebook blocked Power Ventures' Internet Protocol (IP) address. In response to the block, Power Ventures switched IP addresses and continued with its promotional program.[78]

Facebook sued, claiming that Power Ventures violated the Computer Fraud and Abuse Act. This case was a civil action with many differences to *United States v. Nosal (II)*, but the court nonetheless clarified its holding in *Nosal (II)*. The court analyzed its holdings in Brekka, *Nosal (I)*, and *Nosal (II)*.[79]

> From those cases, we distill two general rules in analyzing authorization under the CFAA. First, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when

---

73 *Id*.
74 Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068 (9th Cir. 2016).
75 *Id*. at 1063.
76 *Id*.
77 *Id*.
78 *Id*.
79 *Id* at 1066-69.

> such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. Second, a violation of the terms of use of a website—without more—cannot be the basis for liability under the CFAA.[80]

These two general rules seem to broaden the meaning of the Computer Fraud and Abuse Act beyond just employees whose permission has been revoked. This was one of the fears the dissent expressed in *Nosal (II)*. However, the court in this case seems to take that fear into account, and tries to change what was stated in the majority opinion in *Nosal (II)*.

In *United States v. Nosal (II)*, the court stated that a person needs permission from the system owner in order to access the system with authority.[81] According to the court in *Nosal (II)*, only the system owner can give permission to access the system. The court seems to change its view in *Facebook, Inc. v. Power Ventures, Inc.*. In this case, "Power users arguably gave Power permission to use Facebook's computers to disseminate messages. Power reasonably could have thought that consent from *Facebook users* to share the promotion was permission for Power to access *Facebook's* computers."[82] It was the Facebook users who gave Power Ventures permission to access Facebook information, not Facebook itself. The court held that "[b]ecause Power had at least arguable permission to access Facebook's computers, it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA."[83] The court seems to hold that as long as a defendant has "arguable permission" to access the system, then it is not "without authorization" under the Computer Fraud and Abuse Act.

However, the court continues to hold that if a person's permission to access the system has been explicitly revoked, and they continue to access the system, then they are accessing a computer "without authorization." In *Facebook, Inc. v. Power Ventures, Inc.*, Facebook issued a "cease and desist" order to Power Ventures, and even blocked Power Ventures' IP address. "The record shows unequivocally that Power knew that it no longer had authorization to access Facebook's computers, but continued to do so anyway."[84] Power Ventures continued to access Facebook's system using permission from Facebook users, even after being told by Facebook that the access was unauthorized. Facebook had expressly rescinded the permission granted by its users to Power Ventures. Therefore, under *Facebook*, permission to a computer system can be granted by the systems users, but once it is expressly revoked by

---

80 *Id* at 1067.
81 *Id*.
82 *Id*.
83 *Id*.
84 *Id*.

the system, further access to the system is "unauthorized access" under the CFAA.[85] The court "therefore [held] that, after receiving written notification from Facebook on December 1, 2008, Power accessed Facebook's computers 'without authorization' within the meaning of the CFAA and is liable under that statute."[86]

Once permission to access the computer system has been revoked by the system owner, permission is then needed by both the user of the computer system whose authorized access will be used, and by the system owner itself in order to access the computer system with "authorization."[87] "[F]or Power to [have] continue[d] its campaign using Facebook's computers, it needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers)."[88] In summary, "arguable permission" to access a computer system can be given by one of the system's users, but once that permission is "explicitly" revoked, permission is needed by both the user and the system owner in order to access a computer system with "authorization."[89]

This holding is consistent with the holding in *Nosal (II)*, according the court. Nosal, Christian and Jacobson accessed Searcher after their permission had been revoked.[90] Once they left the company, their passwords and credentials could no longer grant them access to the system. It was an affirmative revocation of permission by Korn/Ferry. FH could no longer give permission to access the system in the same way that "[t]he consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission."[91] Once permission has been revoked, access to the system is no longer "authorized," unless permission is granted by both the user and system owner, regardless of whether proper credentials are used or not.

C. THE LEGAL CONSEQUENCES OF NOSAL (II)

The legal consequences of the decisions in *US v. Nosal (II)* and *Facebook, Inc. v. Power Ventures, Inc.* are numerous. Prior to these rulings, there was much criticism about employers using the Computer Fraud and Abuse Act against former employees.[92] The vague and

85 *Id*.
86 *Id*. at 1068.
87 *Id*.
88 *Id*.
89 *Id*.
90 *Id*.
91 *Id*.
92 *See* Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current*

contradicting interpretations of the statute have left employers with the power to "to pursue civil charges against former employees who used their computer access to act against their employers' interests."[93]

The ruling in *Nosal (II)*, however, has broadened CFAA liability beyond employees and hackers to include everyday computer users.[94] The court holds that anyone who accesses a "protected computer" must receive authorization from the system owner, even though no prior decision held that the "requisite permission must come from the system owner and not a legitimate account holder."[95] This ruling leads to an interpretation of the statute where "[s]ubsection (a)(2)(C) criminalizes nearly all intentional access of a 'protected computer' without authorization."[96] In order to make David Nosal liable under the CFAA the Ninth District broadened the meaning of the statute and the meaning of "without authorization."

A "narrower interpretation [of 'without authorization'] is . . . a more sensible reading of the text and legislative history of a 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."[97] The CFAA was passed to prevent hacking, not to punish former employees. By holding that "a former employee whose computer access credentials were affirmatively revoked . . . acted 'without authorization' in violation of the CFAA when he . . . used the login credentials of a current employee to gain access to confidential computer data . . . and to circumvent . . . revocation of access"[98] the Ninth Circuit opened up liability under the CFAA to anyone who accesses a "protected computer" after having their credentials revoked.

What does it mean to have credentials revoked? The Ninth Circuit fails to clarify what it means to have credentials revoked. Under the common use of the English language, "credentials" means the person "has a right to exercise official power,"[99] and "revoke" means "to annul by recalling or taking back."[100] Therefore, when a person's credentials are revoked, their right to exercise official power (or enter the system) is taken back. In other words, the person loses their right to access to the system. In the case of David Nosal, revocation of his credentials clearly

---

Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act, 52 WM. & MARY L. REV. 1369 (2011).

93 *Id*. at 1410.

94 *Nosal (II)*, 844 F.3d 1024.

95 *Id*. at 1052 (Reinhardt dissent).

96 *Id*.

97 *Nosal (I)*, 676 F.3d 854, 863.

98 *Nosal (II)*, 844 F.3d at 1038.

99 *Revoke*, MERRIAM-WEBSTER (2018).

100 *Id*.

occured when Korn/Ferry deleted his username and password from Searcher.[101] But, revocation of credentials is not always easy determine. For example, in order to access Netflix, a person must first create a Netflix account. The Netflix account consists of a username and password in which the user selects after paying a fee. After creating an account, the user has access to the Netflix service. According to the terms of use, there are two ways in which access to Netflix can be revoked.[102] The first way for access to be revoked is if the user cancels their payment method. After canceling payment, the user's "account will automatically close at the end of [the user's] current billing period."[103] The other way in which access to Netflix can be revoked is if Netflix terminates the account. Under the terms of use, "[Netflix] may terminate or restrict [a user's] use of [their] service, without compensation or notice if [the user is], or if [Netflix] suspect[s] that [the user is] (i) in violation of any of these Terms of Use or (ii) engaged in illegal or improper use of the service."[104] Under *Nosal (II)* it is unclear which, if any, of these situations count as a revocation of credentials. Using the common English language, it can be argued that both qualify as a revocation of credentials. If that is the case, under *Nosal (II)*, a person who cancels their Netflix account is in violation of the CFAA if they access Netflix through someone else's (friend, family member, roommate, etc.) account.

The Ninth Circuit tried to clarify this ambiguity in *Facebook, Inc. v. Power Ventures, Inc.*[105] In *Facebook*, the court held that Power Ventures, Inc. had violated the CFAA by accessing Facebook's system after being issued a cease a and desist letter.[106] A cease and desist letter from Facebook is clearly an explicit revocation of access into the system. The Ninth Circuit narrowed the scope of the CFAA to people whose access had explicitly been revoked. It is obvious that Power Ventures, Inc. had its access to Facebook revoked when Facebook issued a cease and desist letter.[107] However, when this ruling is combined with *Nosal (II)*, "explicit revocation" does not seem so clear.

David Nosal lost authority to access Searcher when his credentials were erased from the system.[108] In *Facebook*, the Ninth Circuit held that "after receiving written notification from Facebook . . . . Power accessed Facebook's computers 'without authorization' within the meaning of the

101 *See Nosal (II)*, 844 F.3d.

102 NETFLIX, *Netflix Terms of Use*, https://help.netflix.com/legal/termsofuse?locale=en&docType=termsofuse (last visited Feb 24, 2017).

103 *Id*.

104 *Id*.

105 Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068 (9th Cir. 2016).

106 *Id*.

107 *Id*.

108 United States v. Nosal (*Nosal II*), 844 F.3d 1024 (9th Cir. 2016).

CFAA and is liable under that statute."[109] Does this holding mean that written notification is required? In order for *Nosal (II)* to align with *Facebook*, erasing David Nosal's credentials from the system must qualify as explicit revocation of access.

It is unclear whether David Nosal was told prior to his credentials being erased that they would be erased in writing or in person, or if he simply knew that his credentials would be erased pursuant to his written contract, or if he just tried entering Searcher and realized his credentials did not work. All these circumstances lead to a broad and ambiguous meaning of explicit revocation of access. If David Nosal was expressly told in writing that his credentials for Searcher were revoked, then there is no issue differentiating his case from *Facebook*. But, if those facts are true, is that what the court intended? Must written revocation be required, or can non-written revocation be explicit? For example, when a user is banned from accessing a website or service for violating the terms of agreement, is it required for the service provider to send a written revocation notice, or is a simple block of the IP address sufficient? These are important questions that the Ninth Circuit left unanswered. However, these questions are moot compared to the effects of a broad the reading of "unauthorized access" and "explicit revocation" in *Nosal (II)* and *Facebook*.[110]

1. EFFECTS ON EMPLOYEES

"The CFAA currently contains seven separate causes of action that may result in criminal or civil liability. Of these, four are frequently used by employers in civil cases against former employees."[111] Over the years, there have been an increasing number of employers filing Computer Fraud and Abuse Act claims against former employees.[112] This has led to much criticism of the Computer Fraud and Abuse Act and is seen "as 'another arrow in the quiver' of legal options for employers to use against former employees."[113] With an already increasing amount of litigation between employers and former employees under the Computer Fraud and Abuse Act, the broad interpretation of "without authorization" in *Nosal (II)* actually has a mitigating effect on the amount of litigation between

---

109 *Facebook, Inc*. 828 F.3d, at 1068.

110 *Id*.; *Nosal II*, 844 F.3d.

111 Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1376 (2011).

112 *See id*.

113 *Id*. at 1371 (quoting David W. Garland & Linda B. Katz, *Computer Fraud and Abuse Act: Another Arrow in the Quiver of an Employer Faced with a Disloyal Employee-Part I*, METROPOLITAN CORP. COUNS., May 2006, at 5.)

employers and former employees. *Nosal (II)* narrows the scope of "without authorization" under the Computer Fraud and Abuse Act to employees whose access had been revoked.[114] This minimizes the use of employers who can file a claim against a former employee. A claim can only be filed under the Computer Fraud and Abuse Act if the former employee accessed the system after their credentials had been revoked.

2. EFFECTS ON CONSUMERS

Unlike with employers and employees, the ruling in *Nosal (II)* has a large negative impact on the American public. American consumers and system subscribers are left defenseless under the Ninth Circuit's broad interpretation of "without authorization." Under this interpretation, "violations of use restrictions imposed by employers or websites [turn] into crimes under the CFAA…put[ting] so many citizens 'at the mercy of [their] local prosecutor.'"[115]

"Netflix is the world's leading Internet television network with over 93 million members in over 190 countries . . . ."[116] Of the 93 million subscribers, about 55% of them live in America.[117] All Netflix subscribers pay to use the system.[118] The subscribers are free to use Netflix for as long as they subscribe to the service. Subscribers are also free to cancel their subscription at any time.[119] As discussed above, cancelling a Netflix subscription may count as "revoking credentials," thus making it "unauthorized access" for that former subscriber to access Netflix through anyone else's account. This leaves millions of Americans subject to prosecution under the Computer Fraud and Abuse Act.

The broad ruling in *Nosal (II)* puts even more American users of social media at risk. Facebook is a clear example of the reach of the Ninth Circuit's holding in *Nosal (II)*. In 2016, 197.7 million Americans used Facebook.[120] "Facebook has tried to limit and control access to its website. A non-Facebook user generally may not use the website to send messages, post photographs, or otherwise contact Facebook users

---

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

115 *Id*. at 1048 (quoting United States v. Nosal *(Nosal I)*, 676 F.3d 854, 862 (9th Cir. 2012)).

116 NETFLIX, Overview, https://ir.netflix.com/ (last visited Feb 24, 2017).

117 *See* Jeff Dunn, *Netflix is booming on the back of subscribers outside of the US*, BUSINESS INSIDER (Oct. 18, 2016), http://www.businessinsider.com/netflix-subscribers-us-international-chart-2016-10.

118 NETFLIX, *Netflix Terms of Use*, https://help.netflix.com/legal/termsofuse?locale=en&docType=termsofuse (last visited Feb 24, 2017).

119 *Id*.

120 *See Number of Facebook users in the United States from 2015 to 2021 (in millions)*, STATISTA, https://www.statista.com/statistics/408971/number-of-us-facebook-users/ (last visited Feb 24, 2017).

through their profiles."[121] In order to access the Facebook system, a person must first create an account. Once an account is created, the user has access to all the services that Facebook has to offer. Under the *Nosal (II)* holding, any Facebook user whose access has been revoked may not use Facebook again without the permission of Facebook.[122] As discussed above, revocation of access can be voluntary (the Facebook user cancels his/her account), or forced (Facebook deletes the user's account). A user, whose account is deleted by Facebook, clearly cannot access Facebook without getting permission from Facebook to create a new account. This easily fits under the holding in *Nosal (II)*, and is even mentioned in Facebook's Terms of Service.[123] An issue arises when a Facebook user willfully deletes their Facebook account. After deleting their account, the former user can no longer access Facebook's services. Therefore, under *Nosal (II)* and *Facebook*, a former user must obtain permission from Facebook in order to access Facebook for any task. For example, a former Facebook user who voluntarily deleted their account would need to acquire permission from Facebook to use a friend's account to find a save a picture of a mutual friend that they wish to print as part of a birthday present! Without Facebook's permission, the former user is in violation of the Computer Fraud and Abuse Act. That seems wildly absurd.

Social media and Netflix users are not the only Americans effected by the broad holding in *Nosal (II)*; law students may be effected significantly as well. Law students and law firms rely heavily on the use of legal databases. Westlaw and Lexis are vital to any law student's success. In order to access Westlaw and Lexis, an account must be created.[124] Upon creating the account, the user pays a fee depending on how much access to the Westlaw system that they want. Westlaw "in its sole discretion, may terminate [a user's] website access if [their] conduct is found to be unlawful, inconsistent with, or in violation of, the letter or spirit of these Terms, or for any other reason."[125] A user's whose account has been terminated can no longer access Westlaw without creating another account, thus gaining permission from Westlaw to regain access into the system. A person whose account has been terminated who tries to access Westlaw without creating a new account is in clear violation of

121 Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1072 (9th Cir. 2016)

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

123 FACEBOOK, *Terms of Service*, https://www.facebook.com/terms (last visited Feb 24, 2017) (Section 2-3 states "If we disable your account, you will not create another one without our permission." Section 3-5 states, "You will not solicit login information or access an account belonging to someone else." Section 2-3 only applies to accounts deleted by Facebook, while Section 3-5 applies to all Facebook users.).

124 THOMSON REUTERS, *Terms of Use Legal Solutions*, http://legalsolutions.thomsonreuters.com/law-products/about/legal-notices/terms-of-use (last visited Feb 24, 2017).

125 *Id.*

the Computer Fraud and Abuse Act. This kind of behavior is what the Ninth Circuit wished to outlaw in its holding in *Facebook*.[126] However, many law students could be in danger of violating the Computer Fraud and Abuse Act without ever having Westlaw terminate their account.

For most law students, the account is paid for by the law school. The law student has unlimited access to Westlaw and Lexis for the three years in which they are enrolled in law school. Once a law student graduates from the law school, the student loses his/her access to Westlaw. The access to the system has been "revoked." Many law students will regain access through their new employer. Does this violate the Computer Fraud and Abuse Act? It can be argued that it does. The new employee has had their authority to access Westlaw revoked. As a new employee at the firm, they now use new credentials to access a system in which their credentials have been revoked.[127]

This situation can be argued against in multiple ways. First, if the new lawyer must create his/her own account once being hired by the company, then the new lawyer is regaining permission to access Westlaw from Westlaw itself. Second, it can be argued that when the law firm bought the bundle package from Westlaw, the firm essentially bought the authority to allow new users to access the system on their behalf. Finally, if the new lawyer uses a company login, it can be argued that the new lawyer is simply an agent of the firm, and the firm has authority to access Westlaw. The agency theory may work great for big law firms, but it may lead to more legal issues for small firms.

Suppose a law student obtains an internship at a small law firm. The small law firm once had purchased an account with Westlaw, but had cancelled that account because it became a financial burden on the firm. The small law firm then hires an intern in law school. The intern, through their law school, has access to Westlaw. The small law firm asks the intern to do legal research on its behalf. If the intern is acting as an agent of the small law firm, then the small law firm is violating the Computer Fraud and Abuse Act through the intern.[128] Under the Ninth Circuit's interpretation of the Computer Fraud and Abuse Act, the small law firm committed essentially the same act as David Nosal. David Nosal no longer had access to Searcher. He then entered the system using someone else's credentials at the company. After having his access revoked, David Nosal used someone else's credentials to enter a system he no longer had access to.[129] In this case, the small law firm had its access of Westlaw revoked. The firm then used the intern, whose credentials had not been revoked, to access a system it no longer had access to. If the intern is an

126 *See Facebook, Inc*., 828 F.3d 1068.
127 *See generally Nosal (II),* 844 F.3d 1024.
128 *Id*. at 1040.
129 *Id*. at 1039-40.

agent of the law firm, then the law firm had "unauthorized access" to Westlaw and has violated the Computer Fraud and Abuse Act.

There is little concern of a District Attorney going after consumers under the CFAA. The most substantial problem facing consumers with a broad interpretation of the Computer Fraud and Abuse Act is the legal power service providers now obtain. Netflix, Facebook, Westlaw, and other service providers can now use the Computer Fraud and Abuse Act to avoid being sued by their users. For example, suppose a Netflix user is disgruntled by the way Netflix handled a dispute, and has a viable cause of action against Netflix. Through discovery, Netflix uncovers that the plaintiff has let a former user use their account. Netflix can now threaten to press charges against the plaintiff (or file a crossclaim) for aiding and abetting in the commitment of violating the Computer Fraud and Abuse Act. This pressure can cause the plaintiff to either settle or drop the claim completely. Plaintiffs will be forced to drop their claims out of fear of federal persecution. Beyond federal persecution, the system providers can file a counterclaim and actually win more money for their CFAA claim than the plaintiff ever asked for in their original claim. The Ninth Circuit has opened the door for large service providers to strong-arm plaintiffs into dropping their claims and further protecting themselves. A broad interpretation of the "without authorization" clause of the Computer Fraud and Abuse Act leaves American consumers and system users vulnerable to persecution and may prevent them from pursuing litigation against system providers.

D. COUNTER ARGUMENTS

The Ninth Circuit interpreted "without authorization" under the Computer Fraud and Abuse Act in a broad manner.[130] There can be much debate over the scope of the ruling in *Nosal (II)*. In *Nosal (II)* the Ninth Circuit held that a person whose credentials were revoked cannot access the system without the permission of both a person who has authorized access and from the system provider.[131] In *Facebook*, the Ninth Circuit narrowed the scope of the Computer Fraud and Abuse Act to explicit revocation of access.[132] A very broad ruling leads to the many issues discussed above. However, based on the facts of both cases, it can be argued that the scope of the Computer Fraud and Abuse Act is not as broad.

David Nosal was fired from his job at Korn/Ferry.[133] He then

130 *See Facebook, Inc*., 828 F.3d 1068.
131 *Nosal (II)*, 844 F.3d 1024, 1038.
132 *Facebook, Inc*., 828 F.3d 1068, 1077.
133 *Nosal (II)*, 844 F.3d1024, at 1030.

proceeded to use a current employee's credentials to access the Searcher database.[134] It can be argued that the ruling in *Nosal (II)* only applies to former employees of a company. In fact, the majority opinion states that "[t]he circumstance here—former employees whose computer access was categorically revoked and who surreptitiously accessed data owned by their former employer—bears little resemblance to asking a spouse to log in to an email account to print a boarding pass."[135] The court clearly did not want the holding to extend to the simple act of password sharing. The Ninth Circuit also mentioned "former employee" throughout its opinion, stressing that the decision is to applied to former employees and no one else.[136]

The facts of *Facebook* can also be used to narrow the scope of the Computer Fraud and Abuse Act.[137] Power Ventures used Facebook users to access Facebook.[138] Facebook has policies in place for companies to advertise and reach out to new users. Power Ventures purposely circumvented Facebook's policies to reach Facebook users.[139] Under the ruling in *Nosal (I)*, "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions."[140] Therefore, at this point, Power Ventures had not violated the Computer Fraud and Abuse Act.[141] Issues occurred after Facebook issued a cease and desist letter to Power Ventures to stop using Facebook in violation of the terms of use.[142] Facebook even took steps to block Power Ventures' IP address.[143] Power Ventures ignored the cease and desist and circumvented the IP address block and continued to access Facebook.[144] "The record shows unequivocally that Power knew that it no longer had authorization to access Facebook's computers, but continued to do so anyway."[145] It can be argued that unequivocal knowledge is the standard when regarding considering revocation of access. Power Ventures knew that Facebook had not allowed access to the system.[146] David Nosal also knew that he did not have authority to access Searcher.[147]

If the standard is unequivocal knowledge of no authority to access a system, the problems facing Netflix users and Facebook users disappear.

---

134 *Id*. at 1031.
135 *Id*. at 1038.
136 *Id*. at 1033.
137 *See Facebook, Inc*., 828 F.3d 1068, 1077.
138 *Id*. at 1072.
139 *Id*. at 1073.
140 *Nosal (I)*, 676 F.3d 854, 863.
141 *Facebook, Inc*., 828 F.3d at 1077.
142 *Id*. at 1077-78.
143 *Id*.
144 *Id*.
145 *Id*. at 1067.
146 *Id*.
147 *Nosal (II),* 844 F.3d 1024.

There is no reasonable reason for a former Netflix or Facebook user to believe that by cancelling their account they are precluded from accessing the system through a friend or family member's account. The same applies for the small law firm. A small law firm has the knowledge that without an account they cannot access Westlaw. However, they know that most law students do have authorized access into the system. Perhaps the small law firm hires law students as interns in order to get access into the system. The knowledge standard applies to the knowledge that accessing the system will be "unauthorized access.". A small law firm has no knowledge that a law student accessing the system on the firm's behalf is "unauthorized access."

The knowledge standard could also be argued the opposite way. It can be a stricter standard of knowledge that there is no authorized access without a loophole. The Netflix user, the Facebook user and the small law firm are fully aware that they cannot access the system without an account. Therefore, any access to that system without creating their own account is "unauthorized access." It can be argued that this interpretation is too broad and the standard is knowledge of "unauthorized access." However, this knowledge standard does not help the users whose accounts have been terminated. A person whose account has been terminated has knowledge that they have violated the terms of use, thus being prohibited from accessing the system. Therefore, a person whose account has been terminated knows, or should know, that they no longer have the authority to use the system. A narrower interpretation of "unauthorized access" still does not dispel all of the legal problems expressed above.

IV. CONCLUSION

The Computer Fraud and Abuse Act was intended to be an anti-hacking law.[148] As technology become more advanced and more prevalent, Congress amended the CFAA to broaden the scope of the law to cover the new technologies.[149] In the statute, the term "without authorization" is left undefined.[150] The courts are left to interpret what "without authorization" means as narrowly or broadly as they see fit. In recent years, employers have filed complaints under the Computer Fraud and Abuse Act against former employees.[151] The courts have interpreted

148 H.R. REP. 98-894, 1984 U.S.C.C.A.N. 3689.

149 Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1376 (2011).

150 18 USCA §1030 (West 2018).

151 Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52

both "without authorization" and "unauthorized access" broadly to allow employers to do this. In *United States v. Nosal (II)*, the Ninth Circuit interpreted "without authorization" so broadly that it effects everyday Americans, not just employees of a company.[152]

The Ninth Circuit held "that Nosal, a former employee whose computer access credentials were affirmatively revoked . . . acted 'without authorization' in violation of the CFAA when he . . . used the login credentials of a current employee to gain access to confidential computer data owned by the former employer and to circumvent Korn/Ferry's revocation of access."[153] Under the *Nosal (II)* ruling, a person whose access to a system has been revoked has no authority to access they system unless they gain permission from both a user whose credentials they will be using to access the system, and the system provider itself.[154] Failure to obtain permission from both parties results in a violation of the Computer Fraud and Abuse Act.[155] The Supreme Court of the United States denied certori, thus making the Ninth Circuit's interpretation in *Nosal (II)* the law.[156]

The Ninth Circuit later tried to narrow the broad interpretation of "without authorization" in *Facebook, Inc. v. Power Ventures, Inc.*.[157] In *Facebook*, the Ninth Circuit held that "after receiving written notification from Facebook on December 1, 2008, Power accessed Facebook's computers 'without authorization' within the meaning of the CFAA and is liable under that statute."[158] *Nosal (II)*'s holding was narrowed to users whose access was explicitly revoked, rather than just all users who no longer have access.[159] However, the court failed to define "explicit revocation" under the Computer Fraud and Abuse Act.[160] Aligning the facts of *Nosal (II)* with those of *Facebook*, the new holding for "without authorization" under the Computer Fraud and Abuse Act is as follows: a user who had access to a system, but no longer has access because authorization has been knowingly revoked, whether by voluntary or involuntary means, can no longer access that system without the permission of the user whose credentials will be used to access the system

---

WM. & MARY L. REV. 1369, 1376 (2011).

152 *Nosal (II)*, 844 F.3d 1024.

153 *Id*. at 1038.

154 *Id*.

155 *Id*.

156 Aurora Barnes, Nosal v. United States SCOTUSblog (2018), available at: http://www.scotusblog.com/case-files/cases/nosal-v-united-states/ (last visited Apr 4, 2018).

157 *Facebook, Inc*., 828 F.3d 1068.

158 *Id*. at 1068.

159 *Id*.

160 *See id*.

and the system provider itself.[161]

The broad reading of "without authorization" under the Computer Fraud and Abuse Act opens the door for many problems for millions of Americans. If a Netflix user stops paying for their account, the account will be terminated.[162] Is this explicit revocation of access? Does the former Netflix user need permission from Netflix in order to use their roommate's Netflix account? If a Facebook user cancels their Facebook account, do they need permission from Facebook to use their spouse's account to view a picture? If a small law firm hires a law student as an intern, does the firm need permission from Westlaw for the student to access Westlaw on their behalf if they formerly had a Westlaw account? A broad interpretation of "without authorization" would answer all these questions in the affirmative. Many Americans violate the Computer Fraud and Abuse Act every day under this broad interpretation. The Ninth Circuit's interpretation of "without authorization" under the Computer Fraud and Abuse Act is too broad and leaves millions of Americans at the mercy of large system providers.

161 *See id*.; *Nosal (II)*, 844 F.3d 1024.

162 *See* NETFLIX, *supra* note 102.