The Ninth Circuit's Deficient Examination of the Legislative History of the Computer Fraud and Abuse Act in *United States v. Nosal*

*William A. Hall, Jr.**

Abstract

In United States v. Nosal*, the Ninth Circuit held that the government may not prosecute certain cases under the Computer Fraud and Abuse Act ("CFAA") where a computer was accessed by a user with some right of access (i.e., an insider) for a prohibited purpose. The* Nosal *court's interpretation relied on a narrow interpretation of the meaning of the phrase "exceeds authorized access" in 18 U.S.C. § 1030(e)(6), and cited applicable legislative history in support of its holding.* Nosal *has since been adopted by two sister circuits and numerous federal district courts.*

This Article contends that the Ninth Circuit failed to examine the legislative history of several important pieces of related federal computer crime legislation, and ignored an axiomatic principle of statutory interpretation in interpreting committee reports related to the passage of the CFAA. It concludes that the Ninth Circuit's analysis of applicable legislative history was deficient and that, contrary to Nosal*'s conclusion, the legislative history of the CFAA and related statutes make clear that Congress intended to permit prosecutions of insiders who "exceed [their] authorized access" by accessing a computer system for a prohibited purpose.*

Table of Contents

* Senior Trial Attorney, Computer Crime and Intellectual Property Section, United States Department of Justice; former Counsel, Senate Judiciary Committee; former Law Clerk, Judge Danny J. Boggs; J.D., Harvard Law School; B.A., Dartmouth College. All views expressed in this Article are my own, and are not necessarily those of the Department of Justice or the United States Government.

December 2016 Vol. 84 No. 6

INTRODUCTION

On April 10, 2012, the en banc United States Court of Appeals for the Ninth Circuit issued a majority opinion that significantly limited the scope of our country's main computer crime statute, the Computer Fraud and Abuse Act ("CFAA").[1] That opinion, handed down in *United States v. Nosal*,[2] marked the first time where a federal circuit court held that the government may not prosecute so-called "insider" cases under the CFAA where a computer was accessed for a prohibited purpose.[3] An insider has some current authorization to access the computer at issue, but exceeds the scope of that authorization by obtaining or altering information on that computer for a prohibited purpose.

In the two-plus decades before the issuance of *Nosal*, few federal courts had seriously questioned the proposition that the government could prosecute such insider cases under the CFAA.[4] Nevertheless, *Nosal* has since been followed by the Second and Fourth Circuits,[5] and numerous district courts around the country.[6]

In *Nosal*, the Ninth Circuit claimed that its interpretation of the CFAA was "a more sensible reading of the text and legislative history

---

1 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)); *see* United States v. Nosal, 676 F.3d 854, 854 (9th Cir. 2012) (en banc).

2 United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

3 *See Nosal*, 676 F.3d at 863–64 (holding that the definition of "'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*").

4 Indeed, two federal circuits have held to the contrary. *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–83 (1st Cir. 2001) (holding that a violation of a confidentiality agreement that prohibited use of information "contrary to [the employer's] interests" constituted "exceed[ing] authorized access" under the CFAA).

5 United States v. Valle, 807 F.3d 508, 527 (2d Cir. 2015); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012).

6 *See, e.g.*, Allied Portables, LLC v. Youmans, No. 2:15-cv-294-FtM-38CM, 2015 WL 3720107, at *4–5 (M.D. Fla. June 15, 2015); Cranel Inc. v. Pro Image Consultants Grp., LLC, 57 F. Supp. 3d 838, 845–46 (S.D. Ohio 2014); Amphenol Corp. v. Paul, 993 F. Supp. 2d 100, 109–10 (D. Conn. 2014); JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 523–24 (S.D.N.Y. 2013); Sebrite Agency, Inc. v. Platt, 884 F. Supp. 2d 912, 917–18 (D. Minn. 2012).

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."[7] However, when considering the legislative history of the CFAA and related statutes, it is clear that Congress intended to permit prosecutions of insiders who "exceed[their] authorized access" by accessing a computer system for a prohibited purpose.[8] Further, part of Congress's intent in criminalizing such conduct was to deter the "theft of intangible information" not protected elsewhere by traditional criminal statutes.[9] Part I examines the *Nosal* en banc opinion, focusing on its claims concerning the legislative history of the CFAA and its employment of terminology. Part II explores the legislative history of the CFAA, a predecessor statute, and the CFAA's subsequent amendments. The Conclusion submits that, contrary to the Ninth Circuit's reading of the CFAA, Congress's clear intent was to permit prosecutions of insiders who access a computer system for a prohibited purpose.

I. *United States v. Nosal*'s Examination of the Computer Fraud and Abuse Act

The *Nosal* en banc court summarized the facts in the case as follows:

> David Nosal used to work for Korn/Ferry, an executive search firm. Shortly after he left the company, he convinced some of his former colleagues who were still working for Korn/Ferry to help him start a competing business. The employees used their log-in credentials to download source lists, names[,] and contact information from a confidential database on the company's computer, and then transferred that information to Nosal. The employees were authorized to access the database, but Korn/Ferry had a policy that forbade disclosing confidential information. The government indicted Nosal on twenty counts, including . . . violations of the CFAA. The CFAA counts charged Nosal with violations of 18 U.S.C. § 1030(a)(4), for aiding and abetting the Korn/Ferry employees in "exceed[ing their] authorized access" with intent to defraud.[10]

---

7 *Nosal*, 676 F.3d at 863.

8 18 U.S.C. § 1030(e)(6) (2012).

9 S. Rep. No. 104-357, at 7 (1996).

10 *Nosal*, 676 F.3d at 856 (brackets in original) (footnote omitted).

The *Nosal* court also noted that "[t]he opening screen of the database also included the warning: 'This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only.'"[11]

The district court, acting on a motion for reconsideration filed by Nosal, dismissed the CFAA charges against him.[12] The government appealed, and a panel of the Ninth Circuit reversed the dismissal of the CFAA counts.[13] A motion for en banc review was then granted.[14]

A. Nosal*'s Holding*

In briefing and at oral argument, the main issue before the court was the meaning of the definition of "exceeds authorized access" in the CFAA.[15] The statute defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[16] Nosal contended that this definition only covers instances where the accesser has obtained information that the accesser is not entitled to obtain, under any circumstances.[17] The government argued that Nosal's interpretation of "exceeds authorized access" was "inconsistent with the final words of the definition, 'obtain or alter information in the computer that the accesser is not entitled *so* to obtain or alter.'"[18] The government continued:

> Because of the presence of the word "so," the meaning of the concluding phrase in 18 U.S.C. § 1030(e)(6) is unambiguous: someone exceeds authorized access when he obtains or alters information that he is not entitled to obtain or alter *in those circumstances*. The word "so" clarifies that the accesser might have been entitled to obtain the information *in some other circumstances*, but not in the way he did—*i.e.*, he was "not entitled *so* to obtain" the information.[19]

---

11 *Id.* at 856 n.1.

12 United States v. Nosal, C 08-0237 MHP, 2010 WL 934257, at *8 (N.D. Cal. Jan. 6, 2010), *rev'd*, 642 F.3d 781 (9th Cir. 2011), *and rev'd en banc*, 676 F.3d 854 (9th Cir. 2012).

13 United States v. Nosal, 642 F.3d 781, 782 (9th Cir. 2011), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012).

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

15 *See Nosal*, 676 F.3d at 857; Appellee's Brief at 10–13, *Nosal*, 676 F.3d 854 (No. 10-10038); Reply Brief for the United States at 7–8, *Nosal*, 676 F.3d 854 (No. 10-10038).

16 18 U.S.C. § 1030(e)(6) (2012).

17 Appellee's Brief, *supra* note 15, at 10–13.

18 Reply Brief for the United States, *supra* note 15, at 7–8 (quoting 18 U.S.C. § 1030(e)(6)).

19 *Id.* at 8.

The en banc Ninth Circuit disagreed, rejecting the government's argument about the wording of the definition for "exceeds authorized access."[20] The court observed, "[t]he government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. This places a great deal of weight on a two-letter word that is essentially a conjunction."[21] The Ninth Circuit further noted, "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose."[22]

In the eyes of the *Nosal* court, the wording of the definition for "exceeds authorized access" in 18 U.S.C. § 1030(e)(6) could be interpreted in two different ways, and Congress had been silent about which meaning it intended.[23] The court explained:

> Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, "[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system." . . . According to the government . . . the "exceeds authorized access" prohibition must apply to people who are authorized to use the computer, but do so for an unauthorized purpose. But it is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.[24]

Based on this reasoning, and after discussion of various policy considerations[25] and the rule of lenity,[26] the *Nosal* court upheld the

---

20 *Nosal*, 676 F.3d at 857.

21 *Id.*

22 *Id.*

23 *Id.* at 858.

24 *Id.* (brackets in original) (citation omitted).

25 *See id.* at 859–62. Although much has been written concerning these policy considerations and their validity, the purpose of this Article is to focus on the legislative history of an aspect of the statute.

26 *See id.* at 862–63.

district court's dismissal of the CFAA charges against Nosal. The court reasoned, "[b]ecause Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail to meet the element of 'without authorization, or exceeds authorized access' under 18 U.S.C. § 1030(a)(4)."[27]

B. Nosal*'s (Deliberate?) Choice of the Word "Use" over "Purpose"*

In interpreting the definition of "exceeds authorized access" in the CFAA, the *Nosal* court also made a related holding: "[W]e hold that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions."[28] The court continued, "[t]herefore, we hold that 'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*."[29] "If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly."[30]

This is an interesting employment of the term "use restrictions" by the Ninth Circuit because under the CFAA, "exceed[ing] authorized access" is defined as using one's authorized "access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[31] In other words, a plain reading of the statutory language shows that the key question concerning a restriction[32] at issue is whether, at the time of the access, such access was in violation of an imposed condition or limitation, such as a prohibition on using the access to obtain information for a particular purpose. The question is not, as the Ninth Circuit implies, whether the information was subsequently used in a prohibited manner after being obtained.[33] In other words, Congress was concerned about the user's intentions at *the time of access*, not about whether the user *later* misused information obtained by means of such access.

The Ninth's Circuit's employment of the term "use restrictions" thus muddies the waters separating three very different factual scenarios of "exceed[ing] authorized access" in which the information ob-

---

27 *Id.* at 864.

28 *Id.* at 863.

29 *Id.* at 863–64.

30 *Id.* at 863.

31 18 U.S.C. § 1030(e)(6) (2012).

32 As opposed to using terminology such as "access restriction," "use restriction," or "purpose-based restriction," this Article will simply use here the term "restriction" which generally means a rule or policy that conditions or limits a user's authority to access a computer.

33 *See Nosal*, 676 F.3d at 863–64.

tained is later misused—only one of which is actually criminalized by the CFAA.[34] The first scenario does indeed constitute violative conduct. This is where the accesser knew all along that he or she was not entitled to access the information; for example, by intentionally accessing the information for a prohibited purpose. The second scenario, however, is not prohibited by the CFAA: where the accesser accessed the information for a permissible purpose, even though the user simultaneously had another improper purpose at the time of access.

Neither is the third scenario prohibited: where the accesser accessed the information for a permissible purpose at the time of access, but *later* misuses the information.[35] Notably, all of the major CFAA provisions that prohibit "exceed[ing] authorized access" to engage in misconduct require either knowledge or intentionality at the time of access as an element of the offense.[36] For example, the Ninth Circuit Jury Instructions Committee's model criminal jury instructions sets out the first element for 18 U.S.C. § 1030(a)(2)(C) as: "[T]he defendant intentionally . . . [exceeded authorized access to] a computer."[37] The Ninth Circuit has itself held, concerning access that is "without authorization," that the use of "intentionally" requires that the government demonstrate that a defendant had a wrongful intent in accessing the computer at issue.[38]

The legislative history of the CFAA also makes clear that the government must demonstrate a defendant's knowledge of the restriction at issue. In 1986, Congress altered the scienter requirement in 18

---

34 *See id.*

35 For example, a credit card company employee legitimately obtains personally identifying information for work-related purposes, but subsequently develops nefarious intentions and sells the information on the black market. Here, there is no violation of "exceed[ing] authorized access," because the employee did not have an improper purpose for obtaining the information *at the time of access*.

36 *See* 18 U.S.C. § 1030(a)(1) ("having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct"); *id.* § 1030(a)(2) ("intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains"); *id.* § 1030(a)(4) ("knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct"); *id.* § 1030(a)(7) ("intent to extort from any person any money or other thing of value").

37 NINTH CIRCUIT COMM. ON MODEL CRIMINAL JURY INSTRUCTIONS, MANUAL OF MODEL CRIMINAL JURY INSTRUCTION FOR THE DISTRICT COURTS OF THE NINTH CIRCUIT 8.97 (2010) (brackets in original).

38 *See* United States v. Sablan, 92 F.3d 865, 869 (9th Cir. 1996) (noting that "the computer fraud statute does not criminalize otherwise innocent conduct" and thus the defendant "must have had a wrongful intent in accessing the computer in order to be convicted under the statute").

U.S.C. § 1030(a)(2) from "knowingly" to "intentionally."[39] A Senate Judiciary Committee report was prepared in association with this change.[40] The Second Circuit noted that the report indicated that "Congress sought only to proscribe intentional acts of unauthorized access, not 'mistaken, inadvertent, or careless' acts of unauthorized access."[41] "The Senate Report concluded that '[t]he substitution of an "intentional" standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another.'"[42]

Therefore, the Ninth Circuit's employment of the terminology "use restrictions" and "misappropriation liability" is imprecise.[43] Mere misuse of information has never been sufficient to sustain a CFAA conviction resting on an "exceeds authorized access" theory if the government could not also prove that, at the time of access, a restriction existed and the defendant knew of the restriction.[44] Because of this, the term "purpose-based restrictions" much more accurately reflects the nature of the rules or policies generally at issue in cases such as *Nosal* than does the phrase "use restrictions." Notably, Congress seems to have understood this even back in 1984. When the predecessor to the CFAA was originally enacted, federal criminal law prohibited "access[ing] a computer with authorization, [and then] us[ing] the opportunity such access provides for *purposes* to which such authorization does not extend."[45]

It may also be useful to view the *Nosal* court's slippery use of terminology in the context of some of the policy arguments it raised concerning the proper scope of the CFAA. The court stated:

> Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an

---

39 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, sec. 2(a)(1), § 1030(a)(2), 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030(a)(2)).

40 S. REP. NO. 99-432, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483.

41 United States v. Morris, 928 F.2d 504, 507 (2d Cir. 1991) (quoting S. REP. NO. 99-432, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 2483).

42 *Id.* at 508 (brackets in original) (quoting S. REP. NO. 99-432, at 6, *reprinted in* 1986 U.S.C.C.A.N. at 2484).

43 *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

44 *See* United States v. Sablan, 92 F.3d 865, 869 (9th Cir. 1996).

45 Counterfeit Access Device and Computer Fraud and Abuse Act (CADCFAA) of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)) [hereinafter CADCFAA of 1984] (emphasis added).

> email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.
>
> . . . Whenever we access a web page, commence a download, post a message on somebody's Facebook wall, shop on Amazon, bid on eBay, publish a blog, rate a movie on IMDb, read www.NYT.com, watch YouTube[,] and do the thousands of other things we routinely do online, we are using one computer to send commands to other computers at remote locations. Our access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands.[46]

One can see here how talking in terms of "use restrictions" aided the *Nosal* court in making these arguably hyperbolic claims.[47] In offering up these examples of "innocuous" violations of purpose-based restrictions of computer systems (which were perhaps set forth to raise the specter that they could be prosecuted under the CFAA), the Ninth Circuit glossed over the reality that the government, in an "exceeds authorized access" prosecution, must prove beyond a reasonable doubt a defendant knew of the restriction at issue.[48] Notably, the *Nosal* court failed to explain how the government could possibly prove this mental-state requirement beyond a reasonable doubt in a prosecution where the defendant was only "dimly aware" of the restriction at issue and did not "read[ ] or understand[ ]" it.[49]

II. Legislative History in the Area of Computer Crime

In its opinion, the *Nosal* court opined:

> The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. . . . While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminal-

---

46 *Nosal*, 676 F.3d at 860–61.

47 *See id.* at 860 ("While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you *could* be.").

48 *See id.* at 859 (leaving out the "intent[ional]" requirement when discussing 18 U.S.C. § 1030(a)(2)(C)).

49 *Id.* at 861.

> ize conduct beyond that which is inherently wrongful, such as breaking into a computer.[50]

This statement is rather remarkable, when one considers that the Ninth Circuit's opinion sets forth only a perfunctory examination of the legislative history surrounding Congress's actions in the area of computer crime[51]—namely, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ("CADCFAA"),[52] the 1986 passage of the CFAA,[53] and the National Information Infrastructure Protection Act of 1996 ("NIIPA").[54]

A. The Counterfeit Access Device and Computer Fraud and Abuse Act

The CADCFAA represented the first specific federal legislation in the area of computer crime.[55] According to a House Judiciary Committee report prepared in association with its passage, the CADCFAA was enacted because "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."[56] After describing what it termed a series of "'hacker' incidents" in its report, the Committee observed that:

> [T]here is a tremendous attitudinal problem that gives the Committee some concern. People can relate to mugging a little old lady and taking her pocketbook, but the perception is that perhaps there is not something so wrong about *taking information* by use of a device called a computer even if it

---

50 *Id.* at 859.

51 This analysis is largely confined to footnote 5 of the *Nosal* opinion. *See id.* at 858 n.5 (noting the original 1984 language concerning insiders, and merely asserting that the 1984 "language was removed and replaced by the current phrase and definition" through the 1986 amendments). This is despite the government's significant briefing on the issue. *See* Brief for the United States at 15–20, *Nosal*, 676 F.3d 854 (No. 10-10038); Reply Brief for the United States, *supra* note 15, at 10–14.

52 Counterfeit Access Device and Computer Fraud and Abuse Act (CADCFAA) of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)).

53 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

54 National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, 110 Stat. 3491 (codified as amended at 18 U.S.C. § 1030 (2012)).

55 *See* H.R. REP. NO. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691 ("There is no specific Federal legislation in the area of computer crime. Any enforcement action in response to computer-related crime must 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.").

56 *Id.*, *reprinted in* 1984 U.S.C.C.A.N. at 3692.

> costs the economy millions now and potentially billions in the future.[57]

The CADCFAA enacted several new federal computer crimes. In pertinent part, the statute prohibited "knowingly access[ing] a computer without authorization, or having accessed a computer with authorization, us[ing] the opportunity such access provides for purposes to which such authorization does not extend," to commit one of two acts.[58] The first prohibited act was by means of such conduct "obtain[ing] information contained in a financial record of a financial institution, . . . or contained in a file of a consumer reporting agency on a consumer."[59] The second prohibited act was "by means of such conduct knowingly us[ing], modif[ying], destroy[ing], or disclos[ing] information in, or prevent[ing] authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation."[60] These two prohibitions are the clear historical antecedents of today's 18 U.S.C. § 1030(a)(2) and (3).[61]

In describing what it meant by "having accessed a computer with authorization, us[ing] the opportunity such access provides for purposes to which such authorization does not extend," the House Judiciary Committee noted the following:

> [T]he provision also would make it a criminal offense for anyone who has been authorized to use a computer to access it knowing that the access is for a purpose not contemplated by the authorization. As a result, it prohibits access to a computer to obtain the described data when the perpetrator knows that the access is not authorized or that it is not within the scope of a previous authorization. The provision does not attempt to reach the scope of information incidentally obtained or the use of information that has been obtained legitimately. The provision therefore does not extend to any type or form of computer access that is for a legitimate business purpose. Thus, any access for a legitimate purpose that

---

57 *Id.* at 10–12, *reprinted in* 1984 U.S.C.C.A.N. at 3695–97 (emphasis added).

58 CADCFAA of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–91 (codified as amended at 18 U.S.C. § 1030(a)(2)–(3) (2012)).

59 *Id.* (codified as amended at 18 U.S.C. § 1030(a)(2)).

60 *Id.* § 2102(a), 98 Stat. at 2191 (codified as amended at 18 U.S.C. § 1030(a)(3)).

61 *Compare* CADCFAA of 1984, § 2102(a), *with* 18 U.S.C. § 1030(a)(2)–(3). A third prohibited act, "by means of one or more instances of such conduct obtain[ing] anything, or caus[ing] a loss, of a value aggregating $5,000 or more during any one year period and affects interstate or foreign commerce," did not survive to final passage of the bill by Congress. *Compare* H.R. REP. NO. 98-894, at 3, *with* CADCFAA of 1984, § 2102(a).

> is pursuant to an express or implied authorization would not be affected.[62]

Between the plain language of the CADCFAA and the House Judiciary Committee's explanation of the meaning of this phrase, it is hard to imagine how Congress could have been much clearer in 1984 that it intended to permit prosecutions of insiders who access a computer system for a prohibited purpose. The Committee specifically talks of prohibiting access to a computer "for a purpose not contemplated by the authorization"[63]—in marked contrast to the *Nosal* court's "skeptic[ism]" that "Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer."[64] The Committee also repeatedly spoke of the scope of authorization as turning on the perpetrator's "purpose,"[65] which is inconsistent with the Ninth Circuit's frequent employment of the term "use restrictions" and its claim that "the text and legislative history" of the CFAA demonstrated Congress's sole intent "to punish hacking—the circumvention of technological access barriers."[66]

B. The Computer Fraud and Abuse Act

In 1986, Congress passed the CFAA, which made amendments and additions to 18 U.S.C. § 1030.[67] As noted above, Congress substituted the phrase "exceeds authorized access" for the wordy phrase "access[ing] a computer with authorization, [and then] us[ing] the opportunity such access provides for purposes to which such authorization does not extend" in 18 U.S.C. § 1030(a)(2).[68] In association with its passage, the Senate Judiciary Committee published a report in which it stated that, in substituting "for the more cumbersome phrase[,] . . . [t]he Committee intends this change to simplify the language in 18 U.S.C. [§] 1030(a)(1) and (2), and the phrase 'exceeds authorized access' is defined separately in Section (2)(g) of the bill."[69] The House Judiciary Committee report associated with the passage of the CFAA likewise explained the rationale for the change as "merely

---

62 H.R. REP. NO. 98-894, at 21, *reprinted in* 1984 U.S.C.C.A.N. at 3707.

63 *Id.*, *reprinted in* 1984 U.S.C.C.A.N. at 3707.

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

65 H.R. REP. NO. 98-894, at 21, *reprinted in* 1984 U.S.C.C.A.N. at 3707.

66 *Nosal*, 676 F.3d at 863.

67 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

68 *Compare id.* sec. 2(c), § 1030(a)(2), *with* CADCFAA of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–91 (codified as amended at 18 U.S.C. § 1030).

69 S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.

to clarify the language in existing law."[70] Therefore, neither the Senate nor House Judiciary Committee manifested any intent to change the substantive meaning of "exceeds authorized access;" rather, the 1986 amendment was, in their minds, intended to "simplify" and "merely . . . clarify" the "more cumbersome phrase" in the CADCFAA.[71]

Further insight into Congress's intent can also be gleaned from section 2(b)(2) of the CFAA.[72] Prior to the CFAA, 18 U.S.C. § 1030(a)(3) criminalized the conduct of:

> [w]hoever . . . knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation.[73]

The CFAA eliminated all insider conduct from the scope of subsection 1030(a)(3), making it a crime to "intentionally, without authorization to access any computer of a department or agency of the United States, access[ ] such a computer . . . that is exclusively for the use of the Government of the United States or . . . [with] conduct [that] affects the use of the Government's operation of such computer."[74]

In pertinent part, the Senate Judiciary Committee explained its rationale for this change as follows:

> The Committee wishes to be very precise about who may be prosecuted under the new subsection (a)(3). The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct . . . .

---

70 H.R. REP. NO. 99-612, at 11 (1986).

71 *Id.*; S. REP. NO. 99-432, at 9, *reprinted in* 1986 U.S.C.C.A.N. at 2486.

72 Computer Fraud and Abuse Act of 1986, sec. 2(b)(2), § 1030(a)(3).

73 CADCFAA of 1984, § 2102(a), 98 Stat. 2190, 2190–91 (codified as amended at 18 U.S.C. § 1030(a)(3) (2012)).

74 Computer Fraud and Abuse Act of 1986, sec. 2(b), § 1030(a)(3).

> . . . [T]he Committee has declined to criminalize acts in which the offending employee merely "exceeds authorized access" to computers in his own department . . . . It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at. This is especially true where the department in question lacks a clear method of delineating which individuals are authorized to access certain of its data. The Committee believes that administrative sanctions are more appropriate than criminal punishment in such a case. The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers—no matter how slightly—he could be prosecuted under this subsection. That danger will be prevented by not including "exceeds authorized access" as part of this subsection's offense.[75]

The Senate Judiciary Committee further observed that it was being animated by concerns lodged by Senators Charles Mathias and Patrick Leahy "that the existing statute casts a wide net over 'whistleblowers,' who disclose information they have gleaned from a government computer."[76] These senators supplied Additional Views appended to the report, which noted that the CFAA's "complete revision of [sub]section 1030(a)(3)"[77] served to:

> eliminate coverage for authorized access that aims at "purposes to which such authorization does not extend." This removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization. As the committee report points out, administrative sanctions should ordinarily be adequate to deal with real abuses of authorized access to Federal computers (assuming, of course, that no other provision of section 1030 is violated).[78]

The House Judiciary Committee likewise noted that this change to 18 U.S.C. § 1030(a)(3) in the CFAA to eliminate "'insider' cover-

---

75 S. REP. NO. 99-432, at 7, *reprinted in* 1986 U.S.C.C.A.N. at 2485.

76 *Id.* at 8, *reprinted in* 1986 U.S.C.C.A.N. at 2485.

77 *Id.* at 21, *reprinted in* 1986 U.S.C.C.A.N. at 2494.

78 *Id.*, *reprinted in* 1986 U.S.C.C.A.N. at 2494–95.

age should alleviate concerns that first arose in 1984 under existing law about disclosures, by 'whistleblowers', of government information that was stored in a computer."[79]

The changes to subsection 1030(a)(3) made in 1986 are critical to comprehending Congress's understanding of the term "exceeds authorized access." When Congress removed coverage under subsection 1030(a)(3) for insiders who access a computer system for a prohibited purpose, it made no such effort to remove it from subsections 1030(a)(1) (obtaining national security information)[80] and 1030(a)(2) (accessing a computer and obtaining information).[81] In fact, the CFAA also created a new offense at 18 U.S.C. § 1030(a)(4) that included coverage for "exceed[ing] authorized access" in a computer to defraud and obtain value.[82]

Interestingly, the *Nosal* court noted that it reviewed the Senate Judiciary Committee's report, observing that

> Senators Mathias and Leahy—members of the Senate Judiciary Committee—explained that the purpose of replacing the original broader language was to "remove[ ] from the sweep of the statute one of the murkier grounds of liability, under which a[n] . . . employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances."[83]

---

79 H.R. REP. NO. 99-612, at 11 (1986).

80 Computer Fraud and Abuse Act of 1986, Pub L. No. 99-474, sec. 2(c), § 1030(a)(1), 100 Stat. 1213, 1213 (codified as amended at 18 U.S.C. § 1030(a)(1) (2012)) (amended to read: "Whoever . . . knowingly accesse[s] a computer without authorization or exceed[s] authorized access, and by means of such conduct . . . obtain[s] 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, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation . . . shall be punished.").

81 *Id.*, sec. 2(c), § 1030(a)(2) (amended to read: "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, . . . or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) . . . shall be punished.").

82 *Id.*, sec. 2(d), § 1030(a)(4) (making it a crime when one "knowingly and with intent to defraud, accesses a Federal interest 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").

83 United States v. Nosal, 676 F.3d 854, 858–59 n.5 (9th Cir. 2012) (en banc) (quoting S. REP. NO. 99-432, at 21, *reprinted in* 1986 U.S.C.C.A.N. at 2494–95).

The Ninth Circuit concluded, "[w]ere there any need to rely on legislative history, it would seem to support Nosal's position rather than the government's."[84]

This assertion by the *Nosal* court is particularly puzzling because the legislative history in the CFAA concerning the 1986 amendments and additions to 18 U.S.C. § 1030 suggest the exact opposite. It is a mystery why the court considered the legislative history of a narrow subsection of section 1030—not implicated in the case before it—to interpret other provisions of the same statute that Congress specifically intended to have broader coverage. As the Supreme Court has observed, "[w]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[85]

Applying this axiomatic principle of statutory interpretation to the CFAA, by eliminating coverage in subsection 1030(a)(3) for insiders who access a computer system for a prohibited purpose,[86] but keeping such coverage in subsections (a)(1) and (a)(2),[87] and adding coverage for such in the new subsection (a)(4),[88] it seems clear Congress intended in 1986 to continue to permit insider cases to be brought under the CFAA where a computer was accessed for a prohibited purpose. Congress removed insider coverage in *only* subsection 1030(a)(3) in order to eliminate the risk of prosecution under that subsection for government employees acting as whistleblowers or who inadvertently "exceed[their] authorized access" by "perus[ing] data belonging to the[ir] department that [they are] not supposed to look at."[89]

C. The National Information Infrastructure Protection Act

In 1996, Congress adopted an important series of amendments to 18 U.S.C. § 1030 in the National Information Infrastructure Protection Act ("NIIPA").[90] In pertinent part, the NIIPA expanded the scope of subsection 1030(a)(2) to include coverage for accessing "in-

---

84 *Id.* at 859 n.5.

85 Russello v. United States, 464 U.S. 16, 23 (1983) (quoting United States v. Wong Kim Bo, 472 F.2d 720, 722 (5th Cir. 1972)).

86 Computer Fraud and Abuse Act of 1986, sec. 2(b), § 1030(a)(3).

87 18 U.S.C. § 1030(a)(1)–(2).

88 Computer Fraud and Abuse Act of 1986, sec. 2(d), § 1030(a)(4).

89 S. REP. NO. 99-432, at 7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485.

90 National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, 110 Stat. 3491 (codified as amended at 18 U.S.C. § 1030).

formation from any department or agency of the United States" and "information from any protected computer if the conduct involved an interstate or foreign communication."[91] The NIIPA defined a "protected computer" as one that "is used in interstate or foreign commerce or communication" or is

> exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government.[92]

In doing this, Congress converted subsection 1030(a)(2) from a provision with limited coverage (financial records and credit reports) to one of significant scope (adding government computers and computers used in interstate commerce).[93] The Senate Judiciary Committee's report associated with the NIIPA notes that:

> [I]ncreasingly[,] computer systems provide the vital backbone to many other industries, such as transportation, power supply systems, and telecommunications. The bill would amend section 1030(a)(2) and extend its coverage to information held on (1) Federal Government computers and (2) computers used in interstate or foreign commerce on communications, if the conduct involved an interstate or foreign communication.[94]

The Senate Judiciary Committee also provided a detailed justification for adding computers used in interstate commerce to subsection 1030(a)(2)'s scope:

> The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign *theft of information* by computer. This information, stored electronically, is intangible, and it has been held that the *theft of such information* cannot be charged under more traditional criminal statutes

---

91 National Information Infrastructure Protection Act of 1996, sec. 201(1)(B), § 1030(a)(2).

92 *Id.*, sec. 201(4)(A), § 1030(e)(2).

93 *Id.*, sec. 201(1)(B), § 1030(a)(2). Congress later amended subsection 1030(e)(2)(B) (definition of "protected computer") to expand this coverage to computers "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." 18 U.S.C. § 1030(e)(2)(B); Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, sec. 207, § 1030(e)(2)(B), 122 Stat. 3560, 3563 (codified as amended at 18 U.S.C. § 1030(e)(2)(B) (2012)).

94 S. REP. NO. 104-357, at 7 (1996).

> such as Interstate Transportation of Stolen Property, 18 U.S.C. [§] 2314. [*See*] *United States* v. *Brown*, 925 F.2d 1301, 1308 (10th Cir. 1991). This subsection would ensure that the *theft of intangible information* by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. In instances where the information stolen is also copyrighted, the *theft* may implicate certain rights under the copyright laws. The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information.[95]

This language is striking to revisit in the wake of *Nosal*, which notably fails to even address the NIIPA.[96] In this 1996 report, the Senate Judiciary Committee made it clear that it intended 18 U.S.C. § 1030(a)(2)(C) to protect against "the theft of intangible information by the unauthorized use of a computer."[97] This clear expression of the Committee's intent substantially undermines the *Nosal* court's claims that Congress did not clearly "incorporate misappropriation liability into the CFAA,"[98] and that Congress was not concerned with "misappropriation of trade secrets."[99]

An examination of *United States v. Brown*,[100] the case cited in the committee report, is further illuminating. In *Brown*, the Tenth Circuit held that violations of the National Stolen Property Act[101] could not be predicated on the basis that the allegedly stolen property was computer source code.[102] This was because "[p]urely intellectual property is not within th[e statutory] category" contemplated within the language of the statute: "goods, wares[,] or merchandise."[103]

The defendant at issue in *Brown* worked as a computer programmer for a software company, and was later found to be in possession of a hard disk that contained portions of the source code for a proprietary computer program.[104] Notably, the defendant argued on appeal that "the government could at most show" that he had made a copy of the source code while still employed at the victim company,[105] and the

---

95 *Id.* at 7–8 (emphasis added).

96 *See generally* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

97 S. REP. NO. 104-357, at 7.

98 *Nosal*, 676 F.3d at 863.

99 *Id.*

100 United States v. Brown, 925 F.2d 1301 (10th Cir. 1991).

101 National Stolen Property Act, 18 U.S.C. §§ 2311, 2314–15 (2012).

102 *Brown*, 925 F.2d at 1307–08.

103 *Id.* at 1307.

104 *Id.* at 1302–03.

105 *See id.* at 1303, 1305 (noting that defendant moved to another state after his termination

indictment alleged that the code itself had been "stolen."[106] *Brown* appears to be, on its face, an example of a case in which the accesser obtained information that, at the time of access, the accesser knew he was not entitled to access, and later misused the information. The Senate Judiciary Committee's statement that its expansion of subsection (a)(2) was intended in part to address the gap created by *Brown* therefore makes it even more obvious that in 1996, Congress intended to permit prosecutions of insiders who access a computer system for a prohibited purpose under 18 U.S.C. § 1030(a)(1), (2), and (4).

Conclusion

The Ninth Circuit's decision in *Nosal* has seriously impacted the federal government's ability to bring insiders who commit crimes involving sensitive computer systems to justice. Of course, those who embrace the decision will likely come to the conclusion that this outcome is, as the old techie saying goes, not a bug but a feature.[107]

This Article has no intent of wading into the active debates in policy circles concerning the appropriate scope of the CFAA. Rather, the purpose of this Article has been simply to set forth and analyze the *Nosal* decision and compare its claims about the legislative history of the CFAA to the historical record.

As Judge Alex Kozinski of the Ninth Circuit stated before Congress in 1993 in setting forth criteria for courts' use of legislative history:

> [L]egislative history can be an immensely valuable tool for resolving certain types of problems in statutory interpretation. First and foremost, legislative history helps courts understand what problem the legislature was trying to solve. Especially where some time has passed between a statute's enactment and its interpretation, legislative history can provide insights into the statute's historical context. And it can expose assumptions shared by both proponents and opponents of the legislation—especially where the assumptions

---

and that defendant "claimed that the government could at most show that a copy of the program was made at [the victim company] and was then transported in interstate commerce").

106 *Id.* at 1305 (quoting indictment and also noting that the government argued below that the defendant "still knows that it is not something that he has a right to take").

107 *See Its a Feature*, Webopedia, http://www.webopedia.com/TERM/I/its_a_feature.html (last visited Aug. 23, 2016) ("It's not a bug, it's a feature" is a "sarcastic slang term used to describe unpleasant experiences in software.").

> seemed so obvious that no one bothered to articulate them in the statute.[108]

Although some of the general concerns raised by legal scholars about the dangers of overuse of legislative history are valid,[109] the controversy over the scope of the CFAA fits all the above-described criteria for being a context where the use of legislative history can be an "immensely valuable tool."[110] Specifically, many years have gone by since the passage of the CADCFAA, CFAA, and NIIPA, and the assumptions made by Congress at the time these statutes were enacted are of the utmost relevance.

The same jurist who set forth these criteria, Judge Alex Kozinski, penned the majority opinion in *Nosal* nearly two decades later—an opinion that is arguably the most influential circuit court opinion issued so far this decade in the area of computer crime. *Nosal* has, as of the date of this Article, been cited in ninety-five lower court opinions,[111] and its core holding has been adopted by two sister circuits.[112] The influence of *Nosal* is of serious concern, however, when the actual historical record is examined—a task that the Ninth Circuit did not conduct adequately, in marked contrast to its detailed examination of various policy considerations.[113]

When the legislative histories of the CADCFAA, CFAA, and NIIPA are reviewed, it is clear that Congress intended that the scope of the term "exceeds authorized access"—defined in 18 U.S.C. § 1030(e)(6) as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"[114]—was to include the conduct of insiders who access a computer system for a prohibited

---

108 *Interbranch Relations: Hearings Before the J. Comm. on the Org. of Cong.*, 103d Cong. 83 (1993) (statement of J. Alex Kozinski, U.S. Court of Appeals for the Ninth Circuit).

109 *See generally* Frank H. Easterbrook, *What Does Legislative History Tell Us?*, 66 CHI.-KENT L. REV. 441, 441 (1990) (rejecting the belief that the "subjective intent of legislators . . . represents 'the law' if found"); Honorable Alex Kozinski, *Should Reading Legislative History Be an Impeachable Offense?*, 31 SUFFOLK U. L. REV. 807, 811 (1998) (It has "bec[o]me quite common to have legislative history used in lieu of statutory language," which "if given effect, severely limits or contradicts the statutory language.").

110 *Interbranch Relations: Hearings Before the J. Comm. on the Org. of Cong.*, *supra* note 108, at 83.

111 *See* Westlaw Search, WESTLAW NEXT, http://www.next.westlaw.com (search in search bar for "676 F.3d 854 (9th Cir. 2012)"; then click "Citing References" on top banner; then click "Cases" on the side banner) (last accessed May 15, 2016).

112 United States v. Valle, 807 F.3d 508, 527 (2d Cir. 2015); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012).

113 United States v. Nosal, 676 F.3d 854, 862–63 (9th Cir. 2012) (en banc).

114 18 U.S.C. § 1030(e)(6) (2012).

purpose. Contrary to the Ninth Circuit's contentions, the relevant Senate and House Judiciary Committee reports associated with these statutes did in fact "speak . . . clearly."[115] The *Nosal* court's ignorance of Congress's clear intent may not trouble those who subscribe to theories such as dynamic statutory interpretation,[116] but it should concern those who believe, in the words of Judge Clyde Hamilton of the Fourth Circuit, that one's "role as an Article III jurist is not to decide what the law should be, but rather to apply the rules of statutory construction in order to give meaning to the statute Congress created."[117]

115 *Nosal*, 676 F.3d at 863.

116 *See generally, e.g.*, WILLIAM N. ESKRIDGE, JR., DYNAMIC STATUTORY INTERPRETATION 5–6 (1994) (arguing "that statutory interpretation is *dynamic*" in that "[t]he interpretation of a statutory provision by an interpreter is not necessarily the one which the original legislature would have endorsed, and as the distance between enactment and interpretation increases, a pure originalist inquiry becomes impossible and/or irrelevant").

117 Robinson v. Shell Oil Co., No. 93-1562, 1995 WL 25831, at *3 (4th Cir. Jan. 18, 1995) (Hamilton, J., dissenting), *vacated en banc*, 70 F.3d 325 (4th Cir. 1995), *rev'd*, 519 U.S. 337 (1997).