Boston College Law Review

Volume 54
Issue 6 *Electronic Supplement*

Article 11

4-10-2013

Right for the Wrong Reasons: The Ninth Circuit Excludes Misappropriation from the CFAA's Ambit in *United States v. Nosal*

Andrew Trombly
Boston College Law School, andrew.trombly@bc.edu

RIGHT FOR THE WRONG REASONS: THE NINTH CIRCUIT EXCLUDES MISAPPROPRIATION FROM THE CFAA'S AMBIT IN *UNITED STATES v. NOSAL*

Abstract: On April 10, 2012, in *United States v. Nosal*, the U.S. Court of Appeals for the Ninth Circuit, sitting en banc, held that the Computer Fraud and Abuse Act ("CFAA") assigns criminal liability only in instances of hacking, not of misappropriation. In reaching this conclusion, the court engendered a split with two other circuits, which had previously held that the CFAA encompasses misappropriation as well as hacking. This Comment argues that, although the Ninth Circuit correctly excluded misappropriation from the CFAA's ambit, the court's rationale overlooked a more compelling policy consideration favoring the narrow interpretation: the potential disruption that a broad interpretation of the CFAA could cause within trade secret law.

Introduction

Under the Computer Fraud and Abuse Act ("CFAA"), a computer user who acquires information from a protected computer and, in doing so, "exceeds authorized access" of that computer may be subject to criminal penalties.[1] But how broadly should the phrase "exceeds authorized access" be construed?[2] More specifically, does the meaning of "exceeds authorized access" encompass misappropriation (that is, the subsequent and unauthorized use of information that a user was authorized to access in the first place)?[3] The Fifth and Eleventh Circuits have held that it does.[4] More recently, however, the Ninth Circuit departed from the precedents established by its sister circuits.[5] In 2012, in *United States v. Nosal* (*Nosal IV*), the U.S. Court of Appeals for the Ninth Circuit, sitting en banc, rejected a broader reading of "exceeds author-

[1] *See* 18 U.S.C. § 1030(a)(4) (2006 & Supp. V 2011) ("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, . . . shall be punished as provided in subsection (c) of this section." (emphasis added)).

[2] *See* United States v. Nosal (*Nosal IV*), 676 F.3d 854, 856–57 (9th Cir. 2012) (en banc).

[3] *Id.*

[4] *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

[5] *See Nosal IV*, 676 F.3d at 862.

ized access" that includes misappropriation, voicing concerns that such a reading would a make criminal of anyone who updates a fantasy football team at work or posts exaggerated information on dating websites.[6]

Part I of this Comment describes the crime allegedly committed by the *Nosal* defendants and recounts the case's procedural history prior to its arrival before the Ninth Circuit.[7] Part II examines the rationales underlying both the Fifth and Eleventh Circuits' adoption of a broader interpretation of the CFAA and the Ninth Circuit's adoption of a narrow interpretation.[8] Finally, Part III evaluates the Ninth Circuit's decision and concludes that the court, although correct in adopting its narrow interpretation, inappropriately based its holding on a far-fetched worry over the widespread criminalization that might flow from the broad interpretation.[9] In doing so, the court ignored a more compelling policy consideration favoring the narrow interpretation: the potential for the broad interpretation to erode trade secret law.[10]

I. Nosal's Motion to Dismiss the Computer Fraud and Abuse Act Charges Lodged Against Him

David Nosal, the principal defendant in *United States v. Nosal*, held a senior position at Korn/Ferry International ("KFI"), a headhunting firm, from 1996 until 2004.[11] In 2004, Nosal decided to leave KFI and launch his own competing firm.[12] After his departure, Nosal persuaded some of his former colleagues who were still working at KFI to provide him with confidential information stored on KFI's computer system to aid in the development of his new firm.[13] The information Nosal asked his former colleagues to acquire included KFI's proprietary lists of sources, names, and contact information.[14] Under the terms of KFI's computer use policy, Nosal's former colleagues were permitted to access this information, but they were not permitted to disclose it to individuals unaffiliated with KFI.[15]

---

[6] *See id.* at 860.

[7] *See infra* notes 11–37 and accompanying text.

[8] *See infra* notes 38–82 and accompanying text.

[9] *See infra* notes 83–101 and accompanying text.

[10] *See infra* notes 83–101 and accompanying text.

[11] United States v. Nosal (*Nosal I*), No. CR 08-00237 MHP, 2009 WL 981336, at *1 (N.D. Cal. Apr. 13, 2009).

[12] *Id.*

[13] *Nosal IV*, 676 F.3d at 856.

[14] *Id.*

[15] *Id.*

In 2008, the government filed an indictment with the U.S. District Court for the Northern District of California charging Nosal with twenty separate criminal counts related to his acquisition of proprietary information from the KFI computer system.[16] Among other alleged offenses, the indictment charged Nosal with violating § 1030(a)(4) of the CFAA, 18 U.S.C. § 1030.[17] That section assigns criminal liability to "[w]hoever . . . 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."[18] The government claimed that Nosal was liable under § 1030(a)(4) because Nosal's accomplices had accessed KFI's protected computer both "without authorization and by exceeding authorized access" and provided information to Nosal, an outside party, in violation of KFI's computer use policy.[19]

Nosal moved to dismiss the CFAA charges, arguing that the CFAA's text forbids only computer hacking, not misappropriation.[20] As Nosal observed, § 1030(a)(4) criminalizes only two specific acts: first, accessing a protected computer "without authorization," and second, "exceed[ing] authorized access" of a protected computer.[21] Nosal maintained that both prongs of criminal activity proscribed by § 1030(a)(4) target hackers, who by definition access computer systems without "authorization."[22] By contrast, neither prong targets users like his cocon-

---

[16] *Nosal I*, 2009 WL 981336, at *1–2. The indictment also charged two of Nosal's former colleagues who participated in his scheme. *Id.* The district court subsequently granted one codefendant's motion to sever her case from that of Nosal. *Id.*

[17] *Id.* at *2; *see* 18 U.S.C. § 1030(a)(4) (2006 & Supp. V 2011). The indictment also charged Nosal with trade secret misappropriation and mail fraud. *Nosal I*, 2009 WL 981336, at *2.

[18] 18 U.S.C. § 1030(a)(4). The CFAA separately defines the term "protected computer" at § 1030(e)(2), but that definition is widely considered to comprise broadly any computer connected to the Internet and is therefore ordinarily accorded little consequence. *See id.* § 1030(e)(2); *Nosal IV*, 676 F.3d at 859 (noting that the term "'protected computer' . . . effectively [includes] all computers with Internet access"); Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1032–33 (N.D. Ill. 2008) (holding that "a computer that provides access to worldwide communications through applications accessible through the internet qualifies as a protected computer"); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. Rev. 2164, 2167 (2004) (observing that the term "protected" computer "likely encompasses any computer linked to the Internet").

[19] *Nosal I*, 2009 WL 981336, at *4. Although it was Nosal's codefendants—and not Nosal himself—who actually accessed KFI's computer system, the indictment alleged that Nosal had aided and abetted his codefendants in the commission of the crime. *Nosal IV*, 676 F.3d at 856.

[20] *Nosal I*, 2009 WL 981336, at *4.

[21] *See* 18 U.S.C. § 1030(a)(4); *Nosal I*, 2009 WL 981336, at *4.

[22] *See Nosal I*, 2009 WL 981336, at *4.

spirators, who were initially authorized to access a protected computer and subsequently used information acquired from that computer in a prohibited manner.[23]

In 2009, in *Nosal I*, the U.S. District Court for the Northern District of California initially denied Nosal's motion on the ground that an employee who accesses an employer's protected computer intending to defraud the employer inherently accesses that computer "without authorization."[24] Shortly thereafter in 2009, however, in *LVRC Holdings v. Brekka*, the U.S. Court of Appeals for the Ninth Circuit held that satisfaction of the "without authorization" prong in § 1030(a)(4) turns only on whether an individual has received permission to access a protected computer, not on an individual's mental state or specific intent.[25]

In light of the *Brekka* decision, Nosal moved for reconsideration of the district court's initial denial of his motion to dismiss.[26] In 2010, in *Nosal II*, the U.S. District Court for the Northern District of California granted Nosal's motion and agreed with his contention that the *Brekka* decision precluded the defendants from being held criminally liable under the "without authorization" prong of § 1030(a)(4).[27] Deprived of its theory based on the "without authorization" prong of § 1030(a)(4), the government argued that the CFAA counts alternatively could be sustained under the "exceeds authorized access" prong.[28] Under this view, KFI's computer use policy, which prohibited the dissemination of information acquired from KFI's protected computer to outside parties, defined the scope of the access that KFI authorized its employees to have.[29] The government argued that Nosal's codefendants "exceed[ed] authorized access" by accessing KFI's protected computer and then using information acquired from that computer in a manner prohibited by KFI's computer use policy.[30]

---

[23] *See id.*

[24] *See id.* at *7. Here, the court took direction from an earlier decision issued by the U.S. Court of Appeals for the Seventh Circuit, which arrived at the same conclusion. *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that an employee who seeks to defraud an employer thereby waives any authorization to access that employer's computer).

[25] 581 F.3d 1127, 1135 (9th Cir. 2009).

[26] United States v. Nosal (*Nosal II*), No. C 08-0237 MHP, 2010 WL 934257, at *1 (N.D. Cal. Jan. 6, 2010).

[27] *Id.* at *6.

[28] *Id.* at *7.

[29] *Id.*

[30] *Id.*

The district court rejected this argument as well, finding it unsupported by the CFAA's text.[31] Although the CFAA offers no separate definition for "without authorization," it does offer one for "exceeds authorized access": specifically, "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[32] The government maintained that a user who is authorized to access a protected computer, but subsequently uses information acquired from that computer in a manner prohibited by the computer's owner, "alter[s]" that information in a manner to which the user is "not entitled" and thereby "exceeds authorized access."[33] The court disagreed, holding that the meaning of the word "alter" cannot be reconciled with the act of misappropriation, which, in the court's view, does not entail the alteration of information stored on a protected computer.[34] Concluding that these CFAA counts could not be sustained under either the "without authorization" prong or the "exceeds authorized access" prong, the district court granted Nosal's motion and dismissed these counts.[35]

The government appealed, and in 2011, in *Nosal III*, a panel of the U.S. Court of Appeals for the Ninth Circuit reversed the district court's dismissal of the CFAA counts.[36] Sitting en banc in *Nosal IV*, the court subsequently reversed the panel, affirming the district court's dismissal of the CFAA counts.[37]

II. Divergent Interpretations of "Exceeds Authorized Access"

Because the U.S. Court of Appeals for the Ninth Circuit's 2009 decision in *United States v. Brekka* had conclusively foreclosed the "without authorization" prong as a statutory basis for the CFAA charges against Nosal, the limited question facing both the *Nosal III* panel and, on rehearing, the *Nosal IV* en banc court was whether the charges could be

---

[31] *Id.*

[32] *See* 18 U.S.C. § 1030(e)(6) (2006).

[33] *See Nosal II*, 2010 WL 934257, at *7.

[34] *Id.* ("There is simply no way to read [18 U.S.C. § 1030(e)(6)] to incorporate corporate policies governing use of information unless the word alter is interpreted to mean misappropriate. Such an interpretation would defy the plain meaning of the word alter, as well as common sense.").

[35] *Id.* at *8. Other CFAA counts were sustained on factual grounds not relevant here. *See id.*

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

[37] *See Nosal IV*, 676 F.3d at 863–64.

sustained under the "exceeds authorized access" prong.[38] This question largely turned on whether "exceeds authorized access" can be read in a broad manner that expands the CFAA to encompass misappropriation.[39] Two other circuits had already adopted this broad interpretation of "exceeds authorized access," and the *Nosal III* panel endorsed that interpretation.[40] Worried that the broad interpretation would criminalize a vast swath of innocuous and widespread conduct, however, the *Nosal IV* en banc court broke ranks with its sister circuits, reversed the *Nosal III* panel's decision, and adopted the narrow interpretation of "exceeds authorized access"—one that excludes misappropriation from the CFAA's ambit.[41]

Section A of this Part examines the decisions rendered by the U.S. Courts of Appeals for the Fifth and Eleventh Circuits and the Ninth Circuit panel in *Nosal III*, all of which adopted the broad interpretation of the CFAA.[42] Section B discusses the Ninth Circuit's en banc decision in *Nosal IV*, which instead adopted the narrow interpretation.[43]

A. *The Fifth Circuit, Eleventh Circuit, and* Nosal III *Panel Adopt a Broad Interpretation and Include Misappropriation Within the CFAA's Ambit*

Both the Fifth and Eleventh Circuits already had considered the question of the CFAA's scope under the "exceeds authorized access" prong before the *Nosal III* panel rendered its decision, and both courts had adopted an interpretation of that prong that includes misappropriation.[44] Guided by these precedents, the *Nosal III* panel followed suit.[45] These three decisions recognize a common principle: that the term "authorized access" refers not only to the information that a user is permitted to access on a computer system, but also to the purposes for which a user is authorized to use that information.[46]

---

[38] *See* 18 U.S.C. § 1030(a)(4) (2006 & Supp. V 2011); United States v. Nosal (*Nosal IV*), 676 F.3d 854, 856 (9th Cir. 2012) (en banc); United States v. Nosal (*Nosal III*), 642 F.3d 781, 785, *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012).

[39] *See Nosal IV*, 676 F.3d at 856; *Nosal III*, 642 F.3d at 785.

[40] *See Nosal III*, 642 F.3d at 788 (endorsing the conclusions of its sister circuits); *accord* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that CFAA encompasses misappropriation); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (same).

[41] *See Nosal IV*, 676 F.3d at 859, 863.

[42] *See infra* notes 44–62 and accompanying text.

[43] *See infra* notes 63–82 and accompanying text.

[44] *See Rodriguez*, 628 F.3d at 1263; *John*, 597 F.3d at 272.

[45] *See Nosal III*, 642 F.3d at 789.

[46] *See id.*; *Rodriguez*, 628 F.3d at 1263; *John*, 597 F.3d at 272. Notably, these decisions, which adopted the broad interpretation of "exceeds authorized access" in the criminal context, were preceded by a First Circuit decision that adopted the broad interpretation

In 2010, in *United States v. John*, the U.S. Court of Appeals for the Fifth Circuit held that a defendant could be charged under the "exceeds authorized access" prong for using information she accessed from her employer's computer system in furtherance of a crime.[47] There, the defendant, a former bank teller, acquired personal customer information stored on the bank's protected computer and used it to defraud the bank's customers.[48] The defendant argued that she could not be found liable under the "exceeds authorized access" prong of § 1030(a)(2) because the bank had authorized her to access its customers' personal information as part of her position.[49] The court, however, rejected this argument.[50] Instead, the court held that a user "exceeds authorized access" not only by accessing information stored on a protected computer without permission, but also by using information acquired from a protected computer for a criminal purpose.[51] Because the defendant used information stored on the bank's computer in commission of a crime, the court held that she could be found liable under the "exceeds authorized access" prong even though her employer had authorized her to access that information.[52]

In 2010, in *United States v. Rodriguez*, the U.S. Court of Appeals for the Eleventh Circuit expanded the Fifth Circuit's view, holding that a defendant may "exceed[] authorized access" by using information stored on a computer system for *any* unauthorized purpose, regardless

---

for *civil* actions brought under the CFAA. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001) (holding that employees who accessed and used information on a computer system in violation of a confidentiality agreement "exceed[ed] authorized access" for purposes of civil liability under the CFAA).

[47] 597 F.3d at 271. The defendant was convicted under 18 U.S.C. § 1030(a)(2) of the CFAA, unlike the defendant in *Nosal*, who was charged under 18 U.S.C. § 1030(a)(4). *See id.* at 270. Unlike § 1030(a)(4), § 1030(a)(2) omits any specific intent requirement. *Compare* 18 U.S.C. § 1030(a)(4) (2006 & Supp. V 2011) (assigning a specific intent requirement of "with intent to defraud"), *with* 18 U.S.C. § 1030(a)(2) (assigning only a mens rea requirement of "intentionally" and omitting any specific intent requirement). Both sections, however, incorporate the same "exceeds authorized access" prong and therefore implicate the same interpretive question facing the court in *Nosal*. *See* 18 U.S.C. § 1030(a)(2), (a)(4).

[48] *John*, 597 F.3d at 269.

[49] *Id.* at 271.

[50] *Id.*

[51] *Id.* at 271. *Compare id.* at 272 (stating that "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized'"), *with* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (stating in dicta that the "exceeds authorized access" prong contemplates users who are authorized to access only a limited portion of a computer system).

[52] *See John*, 597 F.3d at 272.

of whether that purpose is criminal.[53] There, the defendant, a former employee of the Social Security Administration, was convicted of accessing sensitive personal information stored on his employer's computer in order to spy on multiple women in whom he was romantically interested.[54] As in *John*, the defendant argued that, because his employer had authorized him to access personal information stored on its computer as part of his job duties, he could not be found criminally liable under the "exceeds authorized access" prong of § 1030(a)(2).[55] The court rejected this argument, however, noting that the Social Security Administration's computer use policy prohibited its employees from accessing personal information for non-business purposes.[56] The court held that both the plain text of the CFAA and the terms of the employer's computer use policy established that the defendant had "exceed[ed] authorized access" by acquiring personal information for a purpose that his employer had not authorized.[57]

Taking direction from its sister circuits, in 2011, in *Nosal III*, a panel of the U.S. Court of Appeals for the Ninth Circuit also adopted the broad interpretation of "exceeds authorized access."[58] In reaching this conclusion, the panel addressed the district court's textual holding in *Nosal II* that the definition of "exceeds authorized access" prescribed by § 1030(e)(6) cannot be reconciled with the broad interpretation.[59] The panel disagreed with the district court, holding that the word "so" in that definition should be read as "in that manner."[60] On this reading, the panel held, an individual who receives authorization to access a protected computer but uses information acquired from that computer in violation of its use policy would not be "entitled" to "obtain" such information "in that manner."[61] Therefore, the panel concluded that

---

[53] *See* 628 F.3d at 1263. The defendant was convicted under § 1030(a)(2)(B) of the CFAA, unlike the *Nosal* defendants, who were convicted under § 1030(a)(4). *Id.* at 1262; *see* 18 U.S.C. § 1030(a)(2)(B), (a)(4) (2006 & Supp. V 2011). Although the two sections prescribe different mens rea and specific intent requirements, both sections incorporate the "exceeds authorized access" prong and therefore implicate the same interpretive question facing the court in *Nosal*. *See* 18 U.S.C. § 1030(a)(2)(B), (a)(4); *Nosal IV*, 676 F.3d at 856–57; *see also supra* note 47 (comparing these provisions).

[54] *See Rodriguez*, 628 F.3d at 1260–62.

[55] *See id.* at 1263; *John*, 597 F.3d at 271.

[56] *Rodriguez*, 628 F.3d at 1263.

[57] *Id.*

[58] *See Nosal III*, 642 F.3d at 789.

[59] *See id.* at 785–86.

[60] *See id.*

[61] *See id.*

such an individual would "exceed authorized access" and thereby violate the CFAA.[62]

B. *Sitting En Banc, the Ninth Circuit Adopts a Narrow Interpretation and Excludes Misappropriation from the CFAA's Ambit*

Sitting en banc in *Nosal IV*, the Ninth Circuit elected to break ranks with its sister circuits, reverse the decision rendered by the *Nosal III* panel, and instead adopt a narrower construction of the "exceeds authorized access" prong that excludes misappropriation from the CFAA's ambit.[63] The court offered three principal bases for its decision: first, that the CFAA's statutory language does not independently validate the broad interpretation of "exceeds authorized access";[64] second, that expanding the CFAA to encompass misappropriation would strain the CFAA beyond its original legislative purpose;[65] and third, that the broad interpretation would criminalize a vast domain of innocuous conduct.[66]

The court first considered whether the statutory text compels either the broad or narrow interpretation of "exceeds authorized access."[67] In *Nosal III*, the panel had concluded that the placement of the word "so" within the statutory definition of "exceeds authorized access" found in 18 U.S.C. § 1030(e)(6) validates the broad interpretation.[68] In *Nosal IV*, however, the court disagreed, observing that "so" could be understood in several alternative ways that did not require adopting the broad interpretation.[69] Identifying no conclusive interpretation furnished by the statutory text itself, the court turned to two other bases of statutory construction: legislative intent and policy implications.[70]

Upon consideration of these two bases, the court held that including misappropriation within the CFAA's ambit under the broad interpretation would strain the statute beyond its original legislative pur-

---

[62] *See id.*

[63] *See Nosal IV*, 676 F.3d at 863–64.

[64] *See id.* at 858.

[65] *See id.* at 857–58.

[66] *See id.* at 859.

[67] *See id.* at 856.

[68] *Nosal III*, 642 F.3d at 785–86; *see* 18 U.S.C. § 1030(e)(6) (2006).

[69] *See Nosal IV*, 676 F.3d at 858. For instance, the court suggested that "so" could simply refer to the mechanical method by which a computer user accesses information stored on a system, meaning that a user who is authorized only to view information on a computer screen might "exceed[] authorized access" by downloading that information onto a thumb drive. *See id.*

[70] *See id.* at 857–59.

pose.[71] In *Brekka*, the court had observed that Congress originally intended the CFAA to serve as an anti-hacking statute.[72] The court reiterated this account of the CFAA's legislative purpose in *Nosal IV*, concluding that the statute's legislative history confirmed the view that Congress enacted the statute to combat computer hacking.[73] To place misappropriation within the ambit of a statute that Congress originally intended to serve a more limited function would, in the court's view, impermissibly strain the statute beyond its articulated purpose.[74]

Beyond its concern over a strained legislative purpose, however, the court placed its greatest emphasis on the concern that the broad interpretation would criminalize a vast domain of innocuous behavior.[75] For instance, the court suggested that employees who innocently play video games or instant-message with friends while using their workplace computers ordinarily do so in violation of their employers' computer use policies.[76] Additionally, because the broad interpretation of the CFAA recognizes boundaries on "authorized access" established by such policies, a procrastinating employee might become criminally liable under that interpretation.[77] Moreover, the court noted, the broad interpretation might criminalize a range of innocuous behavior even more expansive than workplace procrastination.[78] Virtually every major commercial website requires its users to agree to a largely opaque terms-of-use policy as a condition of using that website.[79] Under the broad interpretation, therefore, a user might "exceed authorized access" and thereby incur criminal liability simply by violating the terms

---

[71] *See id.* at 858.

[72] *See Brekka*, 581 F.3d at 1130.

[73] *See Nosal IV*, 676 F.3d at 858 ("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.'" (quoting S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487 (Conf. Rep.))).

[74] *See id.* at 859.

[75] *See id.* at 859 ("Were we to adopt the [broad] interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct."). The *Nosal III* panel anticipated this concern but concluded that it was safely barred by the specific intent requirement prescribed by § 1030(a)(4). *See Nosal III*, 642 F.3d at 788–89.

[76] *See Nosal IV*, 676 F.3d. at 859. In articulating this concern, the court noted that although § 1030(a)(4) prescribes mens rea and specific intent requirements that could very well exclude innocuous conduct from criminal liability, other sections of the CFAA that also incorporate the "exceeds authorized access" prong do not. *See Nosal IV*, 676 F.3d at 859 (referencing 18 U.S.C. § 1030(a)(2)(C) as an example).

[77] *See Nosal IV*, 676 F.3d at 859.

[78] *See id.* at 860–61.

[79] *See id.* at 861.

of that policy, perhaps by posting misleading information on a dating website or misrepresenting one's age when trying to register for Google or Facebook as a minor.[80]

In short, the Ninth Circuit in *Nosal IV* adopted the narrow interpretation of "exceeds authorized access" in deference to its assessment of the CFAA's legislative purpose and the negative policy implications that the broad interpretation might engender.[81] In the Ninth Circuit's view, one "exceeds authorized access" only by accessing information stored on a protected computer that one is not authorized to access, not by misusing information after the fact or by violating a use policy established by the computer's owner.[82]

III. The *Nosal IV* Decision: Right for the Wrong Reasons

The en banc court in *Nosal IV* devoted the better part of its opinion to its concern that adopting the broad interpretation of "exceeds authorized access" could subject millions of otherwise innocent Americans to criminal prosecution.[83] That outcome is implausible, however, and in any event remains safely barred by the statutory text of 18 U.S.C. § 1030(a)(4) of the CFAA.[84] Moreover, the CFAA's legislative history itself provided the court with sufficient evidence of the statute's legislative intent to adopt the narrow interpretation without having to resort to policy analysis.[85] If the court insisted on articulating a policy basis for

---

[80] *See id.* at 862 ("Under the [broad] interpretation of the CFAA, . . . describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit.").

[81] *See id.* at 859–60.

[82] *See id.* at 863.

[83] *See* United States v. Nosal (*Nosal IV*), 676 F.3d 854, 859 (9th Cir. 2012) (en banc).

[84] *See Nosal IV*, 676 F.3d at 866 (Silverman, J., dissenting).

[85] *See* Allen v. State Bd. of Elections, 393 U.S. 544, 570 (1969) (holding that in cases "where the language of the statute does not make crystal clear its intended scope[,]" a court is "compelled to resort to the legislative history"). The CFAA's legislative history, although somewhat wanting in detail, generally supports the narrow interpretation adopted by the Ninth Circuit. *See Nosal IV*, 676 F.3d at 858; *see also* Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495–96 (D. Md. 2005) (concluding that the CFAA's legislative history evinces a legislative intent to target hacking); S. Rep. No. 101-544, at 4–5 (1990) (noting that the 1990 amendments to the CFAA, including the addition of a civil cause of action, were proposed "in response to . . . the threat posed by new techniques for creating and transmitting malicious programs and codes"); S. Rep. No. 99-432, at 2–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480 (describing instances of hacking as exemplars of "computer crime"); *id.* at 7, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485 (noting that excessive access by federal employee authorized to use computer should generally not warrant criminal penalties); Kyle Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. Ill. J.L. Tech. & Pol'y 429,

its holding, however, a better basis—which the court overlooked—would have been the erosion of existing trade secret law that the broad interpretation might cause.[86]

The policy rationale that the court did articulate in *Nosal IV*—that is, its concern over widespread criminalization of innocuous conduct—was both implausible and irrelevant to the case at hand.[87] Nosal was charged under § 1030(a)(4) of the CFAA, which requires that a defendant act knowingly, with the specific intent to defraud, and obtain something of value.[88] Even under the broad interpretation of "exceeds authorized access," therefore, no prosecution could be brought under § 1030(a)(4) against a defendant simply for updating a fantasy football team while at work.[89] Although other criminal provisions of the CFAA that incorporate the "exceeds authorized access" prong lack these elements and could therefore theoretically be applied arbitrarily, *Nosal IV* presented the Ninth Circuit with neither the factual nor the legal platform for adjudicating infirmities found outside of § 1030(a)(4).[90]

A better and more relevant policy basis for adopting the narrow interpretation is that including misappropriation within the ambit of § 1030(a)(4) could displace existing trade secret law by enabling civil trade secret plaintiffs to circumvent its requirements.[91] Under traditional trade secret law, a party seeking relief for theft or misappropriation of a trade secret must establish that the secret holds economic value, was not readily discernible to others, and benefited from reasonable attempts to preserve its secrecy.[92] These requirements exist to balance the interests of a trade secret owner against the public's interest in accessing the ideas of others.[93] The broad interpretation of "exceeds authorized access" would undermine this policy balance by expanding the CFAA

---

452 (concluding that the legislative history supports exclusion of misappropriation from the ambit of the CFAA).

[86] *See* Brenton, *supra* note 85, at 442.

[87] *See Nosal IV*, 676 F.3d at 866 (Silverman, J., dissenting).

[88] *See* 18 U.S.C. § 1030(a)(4) (2006 & Supp. V 2011); *Nosal IV*, 676 F.3d at 856.

[89] *See Nosal IV*, 676 F.3d at 866 (Silverman, J., dissenting).

[90] *See id.* ("The role of the courts is neither to issue advisory opinions nor to declare rights in hypothetical cases, but to adjudicate live cases or controversies." (quoting Maldonado v. Morales, 556 F.3d 1037, 1044 (9th Cir. 2009))).

[91] *See* Brenton, *supra* note 85, at 443 (explaining that allowing misappropriation claims under the CFAA could allow plaintiffs to bypass requirements imposed by traditional trade secret law).

[92] *See* Restatement (Third) of Unfair Competition: Definition of Trade Secret § 39 (1995); Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. Rev. 1425, 1447 (2009).

[93] *See* Restatement (Third) of Unfair Competition: Definition of Trade Secret § 39 (1995).

into an alternative method of recovery for prospective trade secret plaintiffs that omits the requirements for trade secrecy imposed by existing law.[94] Under the broad interpretation of "exceeds authorized access," any misappropriation of information stored on a protected computer, even by an authorized user, would violate § 1030(a)(4).[95] Furthermore, a separate provision of the CFAA creates a private right of action under which plaintiffs may recover damages caused by a violation of any of its criminal provisions, including § 1030(a)(4).[96] Consequently, the broad interpretation would allow prospective trade secret plaintiffs to seek civil recovery under the CFAA for *any* misappropriation of *any* information—trade secret or not—that is stored on a protected computer.[97] Allowing prospective trade secret plaintiffs to obtain relief without having to satisfy the requirements of trade secret status, however, would abrogate the public interest in the free exchange of ideas that existing trade secret law recognizes.[98]

Admittedly, enhancing private enforcement of trade secrets by reducing barriers to recovery might seem desirable in view of the vital position that all forms of intellectual property, including trade secrets, occupy in the modern economy.[99] That rationale, however, ignores the extensive body of law that already provides for trade secret protection, including both state and federal statutes and common law.[100] Because

---

[94] Brenton, *supra* note 85, at 443; *see also* Garrett D. Urban, Note, *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, 1390–91 (2011) (observing that a broad interpretation of the CFAA would displace existing trade secret law).

[95] *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

[96] *See* 18 U.S.C. § 1030(g) (2006 & Supp. V 2011) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

[97] *See* Brenton, *supra* note 85, at 438.

[98] *See id.*

[99] *See* Graham M. Liccardi, Comment, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. Marshall Rev. Intell. Prop. L. 155, 156 (2008) (advocating for the broad interpretation to expand federal availability of trade secret protection); Brenton, *supra* note 85, at 430. For instance, the Economics and Statistics Administration and U.S. Patent and Trademark Office estimate that the 75 industries most active in intellectual property development and utilization contributed $5.06 trillion to the U.S. economy in 2010, or 34.8% of the nation's gross domestic product that year. *See* Econ. and Statistics Admin. & U.S. Patent and Trademark Office, Intellectual Property and the U.S. Economy: Industries in Focus, at vi–vii (2012), *available at* http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf.

[100] *See* Restatement (Third) of Unfair Competition: Definition of Trade Secret § 39 (1995) (compiling trade secret statutes enacted by forty-two states and summarizing common law); *see, e.g.*, 18 U.S.C. § 1832 (2006) (providing a federal criminal penalty for

trade secrets already enjoy robust protection under existing intellectual property law, no need exists to expand trade secret protection by adopting the broad interpretation of the CFAA.[101]

Conclusion

Motivated by concerns over the criminalization of innocuous conduct, the Ninth Circuit, sitting en banc, adopted a narrow interpretation of the CFAA in *Nosal IV* and excluded misappropriation from the statute's ambit. The court reasoned that only the narrow interpretation ensured that defendants would not be placed behind bars for harmless behavior, such as checking ESPN.com at work. Its decision engendered a split with two of its sister circuits, which had previously held that a computer user can run afoul of the CFAA by using information acquired from a protected computer in an unauthorized manner.

Although the court arrived at the correct decision, its rationale partially missed the mark. The court correctly concluded that Congress intended the CFAA to proscribe computer hacking rather than misappropriation. Its worry over the widespread criminalization that might ensue under the broad interpretation, however, was both far-fetched and irrelevant to the actual case at hand. Moreover, the court overlooked a different and significant policy interest weighing in favor of the narrow interpretation: that the broad interpretation, which includes misappropriation, threatens to displace existing trade secret law and the policies that it incorporates.

Andrew Trombly

Preferred Citation: Andrew Trombly, Comment, *Right for the Wrong Reasons: The Ninth Circuit Excludes Misappropriation from the CFAA's Ambit in* United States v. Nosal, 54 B.C. L. Rev. E. Supp. 129 (2013), http://lawdigitalcommons.bc.edu/bclr/vol54/iss6/11/.

---

trade secret theft); Cal. Civ. Code §§ 3426.1–.11 (West 2012) (providing a tort remedy under California state law for trade secret theft); Mass. Gen. Laws ch. 93, § 42 (2012) (providing a tort remedy under Massachusetts state law for trade secret theft); N.H. Rev. Stat. Ann. § 350-B:1 to :9 (2012) (providing a tort remedy under New Hampshire state law for trade secret theft); Integrated Cash Mgmt. Servs., Inc. v. Digital Transactions, Inc., 920 F.2d 171, 173 (2d Cir. 1990) (restating New York common law elements for a claim of trade secret theft).

[101] *See Nosal IV*, 676 F.3d at 857 n.3; *supra* note 100 and accompanying text. Indeed—and, in fairness, as the court observed—the indictment against Nosal also charged him with trade secret theft under 18 U.S.C. § 1832, and those charges remained pending when the en banc court issued its decision. *Id.*