CRIMINAL LAW — COMPUTER FRAUD AND ABUSE ACT — NINTH CIRCUIT AFFIRMS CONVICTION OF A FORMER EMPLOYEE WHO USED ANOTHER EMPLOYEE'S PASSWORD. — *United States v. Nosal* (*Nosal II*), 828 F.3d 865 (9th Cir. 2016), *reh'g denied and amended by* 2016 WL 7190670 (9th Cir. Dec. 8, 2016).

The Computer Fraud and Abuse Act[1] (CFAA), which addresses computer hacking, broadly criminalizes intrusion into computer systems, including all computers "used in or affecting interstate or foreign commerce or communication."[2] Among other provisions, the CFAA imposes criminal penalties on whoever "accesses a protected computer without authorization, or exceeds authorized access" to perpetrate a fraud.[3] Recently, in *United States v. Nosal* (*Nosal II*),[4] the Ninth Circuit affirmed the conviction of a defendant whose co-conspirators used someone else's login credentials to access the computers of the defendant's former employer.[5] In doing so, the court held that "without authorization" is an unambiguous term with a plain meaning; the court's interpretation meant that in this case *only* the system owner — and not a legitimate user of the system — could grant authorization.[6] The court could have minimized the CFAA's risk of overcriminalization by articulating a distinction between individuals who are explicitly denied or revoked access, and those who lack authorization from the system owner but may claim authorization from a legitimate user.

David Nosal was an employee of Korn/Ferry International (KFI), an executive search firm.[7] After he announced in 2004 that he intended to leave the company, he continued to work as a contractor under a noncompetition agreement.[8] Meanwhile, Nosal and other KFI employees were secretly launching a competing business.[9] KFI's "core asset" was a proprietary database called Searcher, hosted on KFI's in-

---

[1] 18 U.S.C. § 1030 (2012).

[2] *Id.* § 1030(e)(2)(B) (defining "protected computer"). For background on how the statute originally protected only government and financial systems, see generally Laura Bernescu, *When Is a Hack Not a Hack: Addressing the CFAA's Applicability to the Internet Service Context*, 2013 U. CHI. LEGAL F. 633, 637–42.

[3] 18 U.S.C. § 1030(a)(4). The statute requires that the access "furthers the intended fraud" and the accessor "obtains anything of value." *Id.* The mens rea under this section is "knowing[] and with intent to defraud." *Id.*

[4] 828 F.3d 865 (9th Cir. 2016). *Nosal II* is the second time the Ninth Circuit has considered the scope of the CFAA with respect to David Nosal. *See* United States v. Nosal (*Nosal I*), 676 F.3d 854 (9th Cir. 2012) (en banc). *See generally* Recent Case, United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc)*, 126 HARV. L. REV. 1454 (2013) (discussing the court's construction of the statutory term "exceeds authorized access").

[5] *See Nosal II*, 828 F.3d at 868–70.

[6] *See id.* at 875.

[7] *Id.* at 870.

[8] *Id.*

[9] *Id.*

ternal network, which held information about over a million executive search candidates.[10] Nosal and his partners had downloaded data from Searcher while they were employees at KFI, using their own credentials, for use in their competing business.[11] Because KFI revoked their logins when they ceased to work for the firm, they then asked Nosal's former assistant, Jacqueline Froehlich-L'Heureaux (FH), who remained employed at KFI, for her username and password.[12] She gave her credentials to Nosal's partners, who used those credentials to continue accessing Searcher on at least three discrete occasions.[13] After an anonymous tip, KFI launched an investigation and referred the matter to authorities.[14] The government indicted Nosal on nineteen criminal counts, five of which alleged CFAA violations under the "exceeds authorized access" clause of § 1030(a)(4) while Nosal was a KFI employee;[15] those CFAA counts were dismissed in *Nosal I*.[16] In 2013, the government filed a superseding indictment with three CFAA counts resting on accomplice liability for the three times Nosal's partners, without authorization, accessed Searcher with FH's credentials after they had left the firm.[17] The government also indicted Nosal on two trade secret misappropriation counts under the Economic Espionage Act[18] and one count of conspiracy.[19] A jury found him guilty on all counts.[20] Nosal moved for acquittal and for a new trial.[21]

The United States District Court for the Northern District of California denied the motions.[22] The court rejected Nosal's argument that a CFAA violation requires "circumvention of technological barriers," such as evading a firewall by pretending to connect from somewhere else, because neither the statute nor *Nosal I* requires such circumvention.[23] The court also rejected Nosal's argument that FH's permission to use her credentials to access Searcher was sufficient authorization,[24]

---

[10] *Id.*; *see also id.* at 870–71.

[11] *Id.* at 871.

[12] *Id.* at 869, 871.

[13] United States v. Nosal, No. CR-08-0237, 2013 WL 4504652, at *1 (N.D. Cal. Aug. 15, 2013).

[14] *Nosal II*, 828 F.3d at 871.

[15] *See* Indictment at 2–3, *Nosal*, 2013 WL 4504652 (No. CR-08-0237), ECF No. 1.

[16] *Nosal I*, 676 F.3d 854, 864 (9th Cir. 2012) (en banc).

[17] Second Superseding Indictment at 3, *Nosal*, 2013 WL 4504652 (No. CR-08-0237), ECF No. 309.

[18] 18 U.S.C. §§ 1831–1839 (2012).

[19] Second Superseding Indictment, *supra* note 17, at 3.

[20] Verdict Form, *Nosal*, 2013 WL 4504652 (No. CR-08-0237), ECF No. 408.

[21] Defendant's Motion for Acquittal Under Rule 29, *Nosal*, 2013 WL 4504652 (No. CR-08-0237), ECF No. 436; Defendant's Motion for a New Trial, *Nosal*, 2013 WL 4504652 (No. CR-08-0237), ECF No. 437.

[22] *Nosal*, 2013 WL 4504652, at *26.

[23] *Id.* at *3. Nonetheless, password protection could itself be considered a technological access barrier. *See id.*

[24] *Id.* at *3–4.

explaining that the *employer* determines authorization, not a password holder defying the employer.[25] Nosal timely appealed.[26]

A divided panel of the Ninth Circuit affirmed Nosal's conviction on all counts.[27] Writing for the majority, Judge McKeown[28] noted that *LVRC Holdings LLC v. Brekka*[29] had interpreted the phrase "intentionally accesses a computer without authorization."[30] *Brekka* "directly" resolved the issue: accessing a computer after the employer has rescinded permission is clearly "without authorization."[31] Judge McKeown further gave "without authorization" its plain and ordinary meaning, concluding, consistently with other circuits,[32] that the term was unambiguous.[33] Because authorization implicitly comes from "an authority," only the computer owner holds the power to allow or disallow access to its systems.[34] After KFI revoked their credentials, Nosal and his partners became "outsiders" no longer authorized to access Searcher.[35] FH, the assistant who supplied her credentials, "had no mantle or authority to give permission to former employees whose access had been categorically revoked by the company."[36] Therefore, Nosal violated the CFAA as an accomplice to his partners' unauthorized access to Searcher using FH's credentials.[37] The majority then rejected Nosal's objection that the jury instructions failed to require circumvention of a "technological access barrier."[38] Nothing in the statute requires hacking in the sense of breaking down virtual walls.[39] As for his accomplice liability, the facts supported a finding of deliberate ignorance, given an "unequivocal statement" in his partner's testimony.[40]

The majority also affirmed Nosal's conviction for trade secret theft under the Economic Espionage Act of 1996,[41] given the evidence presented at trial.[42] The court rejected Nosal's contention that the data

---

[25] *Id.* at *4 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)).

[26] Notice of Appeal, *Nosal*, 2013 WL 4504652 (No. CR-08-0237), ECF No. 506.

[27] *Nosal II*, 828 F.3d at 869–70.

[28] Judge McKeown was joined by Chief Judge Thomas.

[29] 581 F.3d 1127 (9th Cir. 2009).

[30] *Nosal II*, 828 F.3d at 869 (citing *Brekka*, 581 F.3d at 1135).

[31] *Id.* (citing *Brekka*, 581 F.3d at 1135).

[32] *Id.* at 876–77 (citing, for example, United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012)).

[33] *Id.* at 875.

[34] *Id.* ("Korn/Ferry owned and controlled access to its computers . . . and . . . it retained exclusive discretion to issue or revoke access . . . .").

[35] *Id.* at 875–76.

[36] *Id.* at 875.

[37] *Id.* at 878.

[38] *Id.*

[39] *See id.*

[40] *Id.* at 880.

[41] 18 U.S.C. § 1832(a)(2)–(4) (2012).

[42] *Nosal II*, 828 F.3d at 880–84.

taken were not trade secrets, because even compilations of public information can be trade secrets if they are commercially valuable and sufficiently protected.[43] Finally, the panel vacated and remanded the restitution award for further consideration of reasonableness.[44]

Judge Reinhardt dissented.[45] He would have reframed the question to avoid the risk of making criminals out of innocents.[46] As Judge Reinhardt noted, the same "without authorization" language is used throughout the CFAA, including in broad provisions that do not require fraud or specific intent — merely "obtain[ing] . . . information" from a computer system.[47] Thus, the majority's view that only the *owner* of the system has authority to grant access undermines the authorization upon which many forms of commonplace computer access depend: it could be a crime for an individual to log in to someone else's Facebook account with that person's permission, simply because the system owner prohibits it.[48] Judge Reinhardt would have permitted the common practice of "password sharing," in which legitimate users delegate access to the system.[49] According to Judge Reinhardt, nothing in the dictionary or the statutory text supported the position that *only* the system owner has authority to grant authorization — perhaps "without authorization" just means that the outsider has *neither* the permission of the owner nor that of a legitimate user.[50] At worst, the statute is ambiguous, in which case the rule of lenity favors interpreting the statute in favor of a criminal defendant.[51] Finally, he questioned the wisdom of relying on private entities and prosecutors, who are more likely to compound than to minimize these problems.[52]

The conflict between the majority and dissent highlights the difficulties courts face when interpreting the CFAA. The majority, concluding that users could not grant authorization, preferred to give force to the CFAA by limiting the power to grant authorization to owners. The dissent, concluding to the contrary, was motivated by the lurking risk of overcriminalization under a dated and unclear statute. But

---

[43] *Id.* at 881–84.

[44] *Id.* at 887–88. Although KFI's "actual loss" could include investigation costs and attorneys' fees, *see id.* at 886–87, the court remanded for the district court to reassess the foreseeability of nearly $1 million in costs and the potential duplicative efforts for which those costs were incurred, *id.* at 888.

[45] *Id.* at 888 (Reinhardt, J., dissenting).

[46] *See id.* at 890–91.

[47] *See* 18 U.S.C. § 1030(a)(2)(C) (2012).

[48] *See Nosal II*, 828 F.3d at 890–92 (Reinhardt, J., dissenting).

[49] *See id.*

[50] *Id.* at 892.

[51] *Id.* at 893–94.

[52] *See id.* at 894–96 ("Broadly interpreted, the CFAA is a recipe for giving large corporations undue power over their rivals, their employees, and ordinary citizens, as well as affording such indiscriminate power to the Justice Department . . . ." *Id.* at 896.).

there is a middle ground superior to both the majority and the dissent's divergent approaches. The court could have articulated a distinction based on *the status of the outsider*. Outsiders who have never been affirmatively denied authorization by the system owner should be able to rely on the authorization of subordinate users. But an outsider who has been banned from the system cannot circumvent that ban by getting a valid password from an individual user. Such a distinction coheres with the plain and ordinary meaning of "without authorization," the Ninth Circuit's prior CFAA jurisprudence, and its most recent cases. Importantly, this approach would have preserved the CFAA's deterrent goals without overcriminalizing common practices and would allow for economically beneficial forms of outsider access beyond household password sharing.

The court could have categorized outsiders who claim a subordinate user's authorization into two groups: those who have neither been explicitly granted nor affirmatively denied access by the system owner ("*neutral* outsiders") and those to whom the system owner has explicitly denied or revoked authorization ("*banned* outsiders"). Neutral outsiders can be thought of as strangers. Banned outsiders, by contrast, are known to the system owner, whether by name or electronic identifier (for example, IP address); a particularized determination resulted in their affirmative exclusion from the system. Neutral outsiders may rely on authorization from users subordinate to the system owner, because for them, even a user's permission to access the system *is* a discrete piece of authorization within the plain meaning of the term; hence, they are not "without" (that is, lacking) authorization. But banned outsiders may not similarly rely on such authorization, because for them a user's permission creates a conflict with the system owner's denial or revocation; the owner's judgment takes precedence for reasons of control and efficiency — not because the user *never* has the authority to let someone in.[53] The corollary of this distinction is that individual users may delegate authorization to neutral outsiders, but not to banned outsiders.[54] Of course, any authorization must be scrutinized for other potential defects, like misrepresentation and coercion, just as consent would be scrutinized in physical trespass. And the sys-

---

[53] System owners are usually in a better position than individual users to detect threats and malicious behavior, can implement technological deterrents and barriers, and have the sophistication to pursue legal remedies. In some circumstances, someone other than the system owner, such as a possessor or system operator, might hold that role, but those considerations are inapposite here: KFI was undisputedly the owner, FH's employer, and the holder of a trade secret interest in the information in its system.

[54] Judge Reinhardt takes a more absolute position: he would allow users like FH to grant authorization in such a way that *defeats* CFAA liability even if the system owner wants to keep out the outsider. *Nosal II*, 828 F.3d at 888 (Reinhardt, J., dissenting).

tem owner may always turn a neutral outsider into a banned one by explicitly blocking them or communicating a revocation.

Applying this neutral/banned outsider distinction would have comfortably situated the *Nosal II* court in the Ninth Circuit's CFAA case law. The distinction arises naturally from *Brekka*, which recognized the two kinds of outsiders: "[W]e hold that a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose . . . , *or* when the employer has rescinded permission to access the computer and the defendant uses the computer anyway."[55] In this holding, *Brekka* invoked the power of the employer — or system owner — in only the latter prong, dealing with banned outsiders. *Nosal I* further clarified that *general* policies and terms of use cannot define the scope of CFAA crimes, because such policies are often "lengthy" and "opaque," and nominally prohibit commonplace behavior that should not be criminalized.[56] Requiring the system owner to affirmatively deny access to a banned outsider,[57] before that outsider is precluded from relying on a subordinate user's authorization, furthers *Nosal I*'s "fair notice" rationale.[58]

Another Ninth Circuit decision by a different panel only a week after *Nosal II* signaled a similar approach to deciding who may grant and receive authorization. The court held in *Facebook, Inc. v. Power Ventures, Inc.*[59] that users could delegate authorization, but a system owner could supersede and revoke that authorization.[60] Users of Power's site had given the site their Facebook login credentials and permission to access Facebook's services on their behalf.[61] Facebook sent a cease-and-desist letter prohibiting Power from accessing Facebook's systems and instituted a technological block,[62] turning Power into a banned outsider. Facebook then sued when Power continued to access and misuse Facebook's systems, and the court affirmed Power's liability under the CFAA.[63] *Nosal II* and *Power Ventures* are consistent in

---

[55] 581 F.3d 1127, 1135 (9th Cir. 2009) (emphasis added). Though *Brekka* was about an employee and employer, its rule applies generally to computer users and owners. *Brekka*'s holding recognizes that the same terms are used throughout the CFAA with a common meaning, precluding any argument that overcriminalization worries can be addressed by interpreting "without authorization" differently in § 1030(a)(2). *See Nosal I*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc).

[56] 676 F.3d at 860; *see also id.* at 860–63.

[57] The framework urged here does more than require notice to "keep out." Such a scant limiting principle on "without authorization," imposing liability only if there is notice, would amount to letting all neutral outsiders in without even a user's permission.

[58] *Nosal I*, 676 F.3d at 863.

[59] 828 F.3d 1068 (9th Cir. 2016).

[60] *Id.* at 1077.

[61] *See id.* at 1072.

[62] *Id.* at 1073.

[63] *Id.* at 1079.

that the system owner's *revocation* of a specific outsider's authorization prevented the outsider from asserting valid authorization from individual users;[64] read together, both cases made banned outsiders liable. In fact, by allowing the system owner to have the *final* say, even though the system owner is not the only one with a say, *Power Ventures* arguably adopted a methodology very similar to the one advocated here: until Facebook made Power a banned outsider, the users' delegated authorization was valid.[65] Thus, applying the neutral/banned distinction would not change the disposition of the two cases.

This framework would appropriately balance the risk of overcriminalization against the need for effective legal deterrents and penalties for hacking. It reaches the right result for the kind of password sharing Judge Reinhardt cited. For example, if a company employee purports to authorize her spouse to check her work email, then so long as the company has not explicitly banned her spouse, her spouse would not commit a crime under this meaning of the CFAA by accessing the employee's email. On the other hand, this framework might conceivably allow some outsiders to conspire with insiders and then claim their access was authorized — but if such conspiracy is possible, whether the insider sends the treasure trove to the outsider or gives the password to retrieve it should not create a difference in whether a crime has been committed.[66] Even if some hackers were to assert a defense on the grounds that they received authorization from a legitimate user, this defense would be limited by the validity of the user's authorization. And the CFAA is not the only grounds for liability: state statutes[67] and trade secret laws,[68] among others, may still be enough to prosecute, and computer owners may still assert common law torts. *Nosal* is a perfect example: the defendant was also convicted of trade secret theft,[69] demonstrating that the CFAA need not be a catch-all-criminals statute.

Though the vagueness of the CFAA has long been noted,[70] concerns about delegated access are relatively novel. Few approaches to limiting the overbreadth of the CFAA explicitly consider the possibility

---

64 *See also* Appellee Facebook's Response to Appellants' Petition for Rehearing and Rehearing En Banc at 12 n.4, *Power Ventures*, 828 F.3d 1068 (Nos. 13-17102, 13-17154) ("Far from conflicting with *Nosal II*, the panel opinion [in *Power Ventures*] followed and relied upon it.").

65 *Power Ventures*, 828 F.3d at 1077 n.1.

66 Recent empirical studies have cast doubt on the popular conception of hackers as strangers on the internet, as nearly fifty percent of criminal and civil CFAA cases involve employees, consultants, or contractors — in other words, insiders. Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1480 tbl.1, 1483 tbl.4 (2016).

67 *E.g.*, CAL. PENAL CODE § 502 (West 2010).

68 *E.g.*, 18 U.S.C. § 1832(a)(2)–(4) (2012).

69 *Nosal II*, 828 F.3d at 883–84.

70 *E.g.*, Cyrus Y. Chung, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233, 236–37 (2010).

of users delegating to anyone[71] — hence the novel question of law confronted in *Nosal II*. Professor Orin Kerr proposes that a user should always be able to delegate to an outsider authorization for anything the user may access, though Kerr would impose an agency relationship between the user and the outsider, limiting what can be done with delegated authorization.[72] But while Kerr's proposal soundly permits household password sharing, its agency limitation may be fatal to all third-party websites and tools like Power. Agency strongly limits what the outsider may do even once inside the system, because acting for self-gain violates common law duties and terminates the agency, once again rendering the access unauthorized — and criminal.[73] Because third-party websites and tools, such as social media aggregators, often sustain their endeavors by extracting value from the user's data, conditioning the validity of their delegated authorization on agency principles may discourage the development of interoperable tools that interact with existing computer systems. Conversely, this neutral/banned outsider inquiry results in an essentially binary rule, hinging on the plain meaning of "without," while advantageously tilting toward permissiveness in the gray zone where the system owner has not said either *yes* or *no*. Third parties providing "add-on" features, like Power, should be able to experiment without first seeking affirmative approval from the system owner — subject to a later *no*.

The majority's failure to recognize a neutral/banned outsider distinction risks criminalizing innocuous activity. But since the distinction can be cleanly applied to this case, the *Nosal II* panel decision should be narrowly read as a case about banned outsiders.[74] Cabining the scope of the decision to this half of the neutral/banned distinction avoids the risk of criminalizing household password sharing and supplies a limiting principle.

---

[71] *But see* Orin S. Kerr, Essay, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1182–83 (2016) (considering password sharing in the context of computer trespass).

[72] Kerr suggests that if a third party exceeds the scope of its agency relationship with the user who gave it permission (for example, if Nosal then uses the access for his own purposes rather than to advance the interests of the principal), then a CFAA violation has occurred. Orin Kerr, *Password-Sharing Case Divides Ninth Circuit in* Nosal II, WASH. POST: VOLOKH CONSPIRACY (July 6, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/06/password-sharing-case-divides-ninth-circuit-in-nosal-ii [https://perma.cc/923D-ME7U].

[73] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2008); *cf.* RESTATEMENT (THIRD) OF AGENCY §§ 8.02, 8.03, 8.05 (AM. LAW INST. 2006) (prohibiting agent from using principal's confidential information for agent's benefit).

[74] Shortly before this comment's publication, the Ninth Circuit denied the petition for en banc rehearing and slightly amended its opinion to emphasize KFI's revocation of access to Nosal and his partners, further supporting a narrow reading of the case. *See* United States v. Nosal, 2016 WL 7190670, at *7 (9th Cir. Dec. 8, 2016).