STATUTORY INTERPRETATION — COMPUTER FRAUD AND ABUSE ACT — NINTH CIRCUIT HOLDS THAT EMPLOYEES' UNAUTHORIZED USE OF ACCESSIBLE INFORMATION DID NOT VIOLATE THE CFAA. — *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc).

In 1986, Congress passed the Computer Fraud and Abuse Act[1] (CFAA) to address the growing problem of intentional trespass into others' computer files,[2] known as "hacking." One of the CFAA's provisions, § 1030(a)(4), targets individuals who access a computer "without authorization" or "exceed[] authorized access," provided that certain fraud and materiality requirements are met.[3] Another provision of the statute, § 1030(a)(2)(C), sweeps far more broadly by omitting the fraud and materiality requirements.[4] Under the CFAA, a person "exceeds authorized access" if she accesses a computer "with authorization" and uses the access "to obtain or alter information in the computer that [she] is not entitled so to obtain or alter."[5] The scope of this definition, and of the CFAA more generally, has been widely debated.[6]

Recently, in *United States v. Nosal*,[7] the Ninth Circuit, sitting en banc, held that defendant employees did not "exceed[] authorized access" by transmitting confidential information in violation of company policy.[8] The court interpreted the phrase "exceeds authorized access" to target only restrictions on *access* to information, not limitations on its *use*.[9] That is, an employee can exceed her authorized access only if she is either barred from the information altogether or accesses it in an impermissible manner.[10] The majority *multiplied* two canons of statutory interpretation — the presumption of consistent

[1] Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (2006 & Supp. V 2011)).

[2] *See* S. REP. NO. 99-432, at 1–4 (1986).

[3] 18 U.S.C. § 1030(a)(4) (targeting anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period").

[4] 18 U.S.C. § 1030(a)(2)(C) (targeting anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer").

[5] 18 U.S.C. § 1030(e)(6).

[6] *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

[7] 676 F.3d 854 (9th Cir. 2012) (en banc).

[8] *See id.* at 856, 864. *Nosal* created a circuit split with the Fifth, Seventh, and Eleventh circuits. *See id.* at 862. The Fourth Circuit recently adopted *Nosal*'s interpretation in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 203 (4th Cir. 2012).

[9] *Nosal*, 676 F.3d at 863–64.

[10] *See id.* at 858.

usage and the avoidance canon — to select an interpretation of "exceeds authorized access" that would resolve the concern that § 1030(a)(2)(C) may be unconstitutionally vague. Neither canon alone was determinative; the majority's interpretation emerged only when the presumption of consistent usage *created* an interpretive problem and the avoidance canon *resolved* it. *Nosal*'s "multiplying canons" technique is a potentially powerful tool of statutory interpretation, and future scholarship should explore its merits. Yet even if sensible, this technique did not achieve the majority's goal in *Nosal*: § 1030(a)(2)(C) remains vulnerable to constitutional attack.

From approximately April 1996 to October 2004, David Nosal worked at Korn/Ferry International (KFI), an executive search firm.[11] Shortly after leaving the firm to start a competing business, Nosal convinced his former coworkers to use their account credentials to download information from a confidential database on KFI's computer system and transfer that information to Nosal.[12] The coworkers had authorization to access the database, but KFI's policy forbade disclosure of confidential information.[13] The government charged Nosal with, inter alia, violations of § 1030(a)(4) for aiding and abetting his former coworkers in "exceeding [their] authorized access" with intent to defraud.[14] Nosal filed a motion to dismiss the indictment, arguing that the CFAA targeted hacking, not misuse of information obtained with permission.[15]

The district court initially denied Nosal's motion, holding that accessing a computer "knowingly and with the intent to defraud . . . renders the access unauthorized or in excess of authorization."[16] The court determined that the CFAA was unambiguous and refused to apply the rule of lenity.[17] However, the court reconsidered Nosal's motion in light of the Ninth Circuit's intervening decision in *LVRC Holdings LLC v. Brekka*,[18] in which the Ninth Circuit narrowly interpreted the phrases "without authorization" and "exceeds authorized access." On reconsideration, the court held that an employee "exceeds authorized access" only if she does not have permission to

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

[12] *See id.* at *1, *4.

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

[14] *Id.* at 856. The government indicted Nosal on twenty charges, including trade secret theft, mail fraud, and conspiracy. *Id.*

[15] *Id.*

[16] *Nosal*, 2009 WL 981336, at *6–7.

[17] *Id.* at *7. According to the rule of lenity, "ambiguity concerning the ambit of criminal statutes should be resolved in the favor of lenity." United States v. LeCoe, 936 F.2d 398, 402 (9th Cir. 1991) (quoting Rewis v. United States, 401 U.S. 808, 812 (1971)) (internal quotation marks omitted).

[18] 581 F.3d 1127 (9th Cir. 2009); *see* United States v. Nosal, No. C 08-0237, 2010 WL 934257, at *1 (N.D. Cal. Jan. 6, 2010).

access the information for any reason.[19] The court dismissed five CFAA counts against Nosal,[20] and the government appealed.[21]

The Ninth Circuit initially reversed and remanded.[22] The court held that an employee "exceeds authorized access" when she "violates the employer's computer access restrictions — including use restrictions."[23] Nosal successfully petitioned for rehearing en banc.[24]

The en banc panel affirmed the district court's judgment.[25] Writing for the court, Chief Judge Kozinski[26] engaged in a three-step analysis. First, he determined that the phrase "exceeds authorized access" was textually ambiguous. On the one hand, "it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files."[27] On the other hand, the phrase could broadly target anyone who has "unrestricted physical access to a computer, but is limited in the use to which she can put the information."[28] The court rejected the argument that the words "so" and "entitled" in the statutory definition compelled the latter interpretation.[29]

Next, the court employed the "standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning."[30] The court determined that interpreting "exceeds authorized access" differently in §§ 1030(a)(4) and 1030(a)(2)(C) was "impossible," since "Congress provided a *single* definition of 'exceeds authorized access' for all iterations of the statutory phrase."[31] Therefore, it was necessary to consider other statutory provisions when interpreting § 1030(a)(4).

[19] *Nosal*, 2010 WL 934257, at *6–7.

[20] *Id.* at *8–9.

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

[22] *Id.* at 789.

[23] *Id.* at 785.

[24] United States v. Nosal, 661 F.3d 1180 (9th Cir. 2011) (ordering rehearing en banc).

[25] *Nosal*, 676 F.3d at 864.

[26] Chief Judge Kozinski was joined by Judges Pregerson, McKeown, Wardlaw, Gould, Paez, Clifton, Bybee, and Murguia.

[27] *Nosal*, 676 F.3d at 856–57.

[28] *Id.* at 857.

[29] *Id.* at 857–58. In the phrase "accesser is not entitled so to obtain or alter," the government interpreted "entitle" as "furnish with a right" and "so" as "in that manner." *Id.* at 857. Thus, the government argued that KFI's use policy furnished the employees with certain rights, and the employees exceeded their authorized access when they violated the use policy. *Id.* The court disagreed: "An equally or more sensible reading of 'entitled,'" Chief Judge Kozinski wrote, "is as a synonym for 'authorized.'" *Id.* The word "so" has meaning even if it does not refer to use restrictions, and Congress may have simply used it "as a connector or for emphasis." *Id.* at 858.

[30] *Nosal*, 676 F.3d at 859 (alteration in original) (quoting Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007)) (internal quotation marks omitted).

[31] *Id.*

Finally, the court focused on the "broadest provision" of the CFAA — § 1030(a)(2)(C) — and implicitly applied the canon of constitutional avoidance. Under the broad interpretation of "exceeds authorized access," Chief Judge Kozinski wrote, "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" if their employers' policies forbid personal uses of work computers.[32] Homely users of social media sites should similarly beware: "[D]escribing yourself as 'tall, dark and handsome' . . . will earn you a handsome orange jumpsuit."[33] The court implicitly expressed concern that § 1030(a)(2)(C) may be unconstitutionally vague, explaining that "[u]biquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement" and that resting criminal liability on the "vagaries" of lengthy and opaque use policies that are subject to change at any time would create significant notice problems.[34] The court affirmed that "[people] shouldn't have to live at the mercy of [their] local prosecutor" and "remain[ed] unpersuaded by the decisions of [its] sister circuits that . . . looked only at the culpable behavior of the defendants before them."[35]

The court held that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions" and confirmed its approach by invoking the rule of lenity.[36] Nosal's former colleagues did not exceed their authorized access because they had permission to access the company database.[37] Thus, the Ninth Circuit affirmed the district court's dismissal of five counts against Nosal for failure to state an offense.[38]

Judge Silverman dissented.[39] "In ridiculing scenarios not remotely presented by *this* case," Judge Silverman wrote, "the majority [did] a good job of knocking down straw men — far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy."[40] Judge Silverman explained that none of the circuits analyzing the CFAA had adopted the majority's interpreta-

[32] *Id.* at 860.

[33] *Id.* at 862. According to the court, "millions of unsuspecting individuals" — users of such popular sites as Craigslist, eBay, Facebook, Google, IMDb, JDate, LinkedIn, Match.com, MySpace, Netflix, Pandora, Twitter, Wikimedia, and YouTube — could become federal criminals overnight if the CFAA were interpreted to criminalize use violations. *See id.* at 859, 861 n.8.

[34] *Id.* at 860. Notice and "arbitrary and discriminatory enforcement" are the two concerns underlying the void-for-vagueness doctrine. *See* Kolender v. Lawson, 461 U.S. 352, 357–58 (1983).

[35] *Nosal*, 676 F.3d at 862.

[36] *Id.* at 863.

[37] *Id.* at 864.

[38] *Id.*

[39] *Id.* (Silverman, J., dissenting). Judge Silverman was joined by Judge Tallman.

[40] *Id.*

tion.[41] He emphasized § 1030(a)(4)'s scienter and intent to defraud requirements and argued that courts "need to wait for an actual case or controversy" to decide the constitutionality of other provisions of the CFAA, such as § 1030(a)(2)(C), which may lack these requirements.[42]

Nosal offers a novel way in which canons of statutory interpretation can interact with one another. The *Nosal* majority *multiplied* two canons — the presumption of consistent usage and the avoidance canon — to select one of two textually permissible interpretations of "exceeds authorized access." Standing alone, neither canon was determinative. The canons justified the majority's interpretation only when applied in sequence: the presumption of consistent usage created an interpretive problem — the potential unconstitutional vagueness of § 1030(a)(2)(C) — that would not have otherwise arisen in a prosecution under § 1030(a)(4), and the avoidance canon resolved this problem. This technique is potentially powerful, and future scholarship should explore the circumstances in which canon multiplication is an appropriate tool of statutory interpretation. Yet even if *Nosal*'s "multiplying canons" approach is sound, the court's failure to draw a substantive distinction between "access" and "use" produced an interpretation that will not shield § 1030(a)(2)(C) from a vagueness challenge.

The *Nosal* majority multiplied canons to produce an interpretation of "exceeds authorized access" that cannot be justified by either of the canons standing alone. The court first applied the presumption that "identical words and phrases within the same statute should normally be given the same meaning"[43] — a presumption the Supreme Court has consistently affirmed.[44] In *Gustafson v. Alloyd Co.*,[45] the Court explained that the presumption of consistent usage followed from the Court's "duty to construe statutes, not isolated provisions,"[46] and was necessary "if the Act [in question was] to be interpreted as a symmetrical and coherent . . . scheme, one in which the operative words have

[41] *Id.* at 865.

[42] *Id.* at 866.

[43] *Id.* at 859 (majority opinion) (quoting Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007)) (internal quotation mark omitted).

[44] *See, e.g.*, FCC v. AT&T Inc., 131 S. Ct. 1177, 1184–85 (2011); *Powerex*, 551 U.S. at 232. *But see* Envtl. Def. v. Duke Energy Corp., 549 U.S. 561, 575–76 (2007) (explaining that the presumption is not irrebuttable and "context counts"). The presumption of consistent usage is at its peak where, as in *Nosal*, Congress has evinced intent to create a consistent scheme by providing a single definition of a key statutory phrase. *See* Jean-Louis v. Att'y Gen., 582 F.3d 462, 474–75 (3d Cir. 2009) (finding courts' reasoning about other provisions applicable to a given provision because Congress provided a single statutory definition of a shared key term); *cf.* USX Corp. v. Liberty Mut. Ins. Co., 444 F.3d 192, 200 (3d Cir. 2006) (rejecting a proposed interpretation of a contract in which a single term had two different meanings despite "its inclusion in a single definition section" of an insurance policy).

[45] 513 U.S. 561 (1995).

[46] *Id.* at 568.

a consistent meaning throughout."[47] Thus, the *Nosal* court properly searched for a meaning of "exceeds authorized access" that would make sense for the statute as a whole.[48] But once the court applied the presumption of consistent usage and examined provisions of the CFAA other than § 1030(a)(4), an interpretive problem arose: § 1030(a)(2)(C) likely would be unconstitutional under a broad interpretation of "exceeds authorized access."[49] The court then turned to another canon, constitutional avoidance, to address the hazard revealed by the presumption of consistent usage.

The avoidance canon resolved this interpretive problem and completed the multiplication, leading the court to adopt the narrow interpretation of "exceeds authorized access." The Supreme Court has reaffirmed that courts have a duty to avoid, when reasonably possible, interpretations that create "grave and doubtful constitutional questions."[50] Standing alone, the avoidance canon could not justify a narrow interpretation of "exceeds authorized access" because Nosal was indicted under § 1030(a)(4), the narrow fraud and materiality requirements of which foreclose any constitutional problems.[51] The avoidance canon counseled in favor of the narrow interpretation only when multiplied with the presumption of consistent usage.[52]

Canon multiplication is a novel approach to statutory interpretation. While scholars and judges have hotly debated whether canons should be used at all,[53] the literature largely has not addressed the *in-*

[47] *Id.* at 569.

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

[49] The court's concerns about § 1030(a)(2)(C) were well founded. *See* United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009) (holding that a conviction under § 1030(a)(2)(C) based only on the defendant's intentional violation of a website's terms of service would violate the void-for-vagueness doctrine); Andrew T. Hernacki, Comment, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1563–64 (2012) (arguing that broad interpretations of § 1030(a)(2)(C) raise overbreadth and vagueness problems).

[50] *E.g.*, Gonzalez v. United States, 553 U.S. 242, 251 (2008); *see also* Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council, 485 U.S. 568, 575 (1988) (collecting Supreme Court cases confirming this "cardinal principle").

[51] *See, e.g.*, Gonzales v. Carhart, 550 U.S. 124, 149 (2007) ("[S]cienter requirements alleviate vagueness concerns.").

[52] The court confirmed its interpretation by appealing to yet a third canon — the rule of lenity. *See Nosal*, 676 F.3d at 863.

[53] *Compare* ANTONIN SCALIA, A MATTER OF INTERPRETATION 28 (1997) ("[T]hese artificial rules increase the unpredictability, if not the arbitrariness, of judicial decisions."), *and* Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are to Be Construed*, 3 VAND. L. REV. 395, 401–06 (1950) ("[T]here are two opposing canons on almost every point." *Id.* at 401.), *and* Richard A. Posner, *Statutory Interpretation — In the Classroom and in the Courtroom*, 50 U. CHI. L. REV. 800, 806 (1983) ("[M]ost of the canons are just plain wrong . . . ."), *with* Adrian Vermeule, *Interpretive Choice*, 75 N.Y.U. L. REV. 74, 140–41 (2000) (arguing that the principal value of canons to the legislature is their predictability),

teraction among canons, particularly where one canon creates an interpretive issue and another resolves it.[54] Yet canon multiplication is a potentially powerful interpretive technique. Multiplication may allow courts to achieve desirable results that are out of the reach of any one canon alone. The *Nosal* court, for example, multiplied canons to preserve the constitutionality of a statute. Future work should study canon multiplication and identify the circumstances in which it is an appropriate tool of statutory interpretation.

Even if the *Nosal* court reasonably *multiplied* canons, it miscalculated: § 1030(a)(2)(C) likely still suffers from vagueness concerns under the court's chosen interpretation. First, the court's distinction between access and use disintegrates if access is conditional.[55] Compare the statements, "You have access to file *X only* if you read it for business purposes" (conditional access restriction), and "Here is access to file *X*; read *X* for business purposes only" (use restriction). These statements are substantively indistinguishable; they differ in form only. If access is conditional,[56] then an employee's liability for exceeding authorized access turns on the phrasing rather than the substance of the company's policy, hardly mitigating the court's concern that § 1030(a)(2)(C) may be unconstitutionally vague.

Moreover, the court's analysis fails to resolve the court's constitutional anxiety even if access is binary. The *Nosal* majority was concerned that "[u]biquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement" and that resting criminal liability on the "vagaries" of lengthy and opaque use policies that are subject to change at any time would create significant notice problems.[57] Yet the court's distinction between access and use does not ameliorate these concerns. For example, as the court noted, Google, until very recently, forbade minors from using its services.[58] This restriction is an *access*

and CASS R. SUNSTEIN, AFTER THE RIGHTS REVOLUTION 154 (1990) (arguing that "interpretive principles" may "promote better lawmaking").

[54] While leading scholars have noted the multiplicity of canons, they have not discussed the ways in which these canons interact. *See, e.g.*, JOHN F. MANNING & MATTHEW C. STEPHENSON, LEGISLATION AND REGULATION 218–356 (2010) (describing various semantic and substantive canons, and showing that multiple canons may independently support the same interpretation, but not discussing the layering of canons involved in multiplication).

[55] *See Nosal*, 676 F.3d at 865 (Silverman, J., dissenting) ("A person of ordinary intelligence understands that he may be . . . authorized to do something but prohibited from going *beyond* what is authorized."); *see also* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2d Cir. 2004) ("[D]istinctions between authorized access and an unauthorized end use of information strike the Court as too fine.").

[56] It is entirely plausible to recognize conditional access to information. Just like individuals may place conditions on access to their homes, employers and website operators should be able to restrict access to their information. *See* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 482 (2003).

[57] *Nosal*, 676 F.3d at 860.

[58] *Id.* at 861.

restriction under the court's interpretation: rather than limit minors' use of its service, Google forbade them from accessing those services altogether. Minors in violation of this policy would thus exceed their authorized access, even though this restriction was buried inside a "lengthy, opaque, subject to change and seldom read" use policy and invited "arbitrary and discriminatory enforcement."[59] Similarly, employees who engage in activities "routinely *prohibited*"[60] by lengthy and opaque company policies, such as watching sports highlights on ESPN.com, would exceed their authorized access by accessing unauthorized information, despite analogous notice and enforcement problems.[61] Thus, the court's interpretation of "exceeds authorized access" does not ameliorate the concern that § 1030(a)(2)(C) may be unconstitutionally vague.

Nosal illustrates the principle that canons of statutory interpretation can be *multiplied* to produce an interpretation that cannot be justified by any one of the canons standing alone. This novel approach remains ill defined in the literature and merits more attention. Even if analytically sensible, however, canon multiplication counseled in favor of an interpretation that did not shield § 1030(a)(2)(C) from constitutional attack.

[59] *Id.* at 860.

[60] *Id.* (emphasis added). However, the CFAA does not criminalize such activities for a different reason. To exceed authorized access, one must "access a computer . . . [and] use such access to obtain or alter information *in the computer*." 18 U.S.C. § 1030(e)(6) (2006 & Supp. V 2011) (emphasis added). When an employee browses Facebook from her work computer, she obtains information stored on Facebook's servers, not on her computer's hard drive. She neither obtains nor alters any information in her work computer (with the trivial exception of browser cookies) and hence does not exceed her authorized access. *See* Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028, at *1–2 (M.D. Fla. May 6, 2011). The CFAA's legislative history confirms that § 1030(a)(2)(C) was designed to combat theft of information, not innocuous web browsing. *See* S. REP. NO. 104-357, at 7 (1996) (explaining that § 1030(a)(2)(C) "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 [is] protected"). This argument undercuts *Nosal*'s concern with criminalizing large swaths of common workplace behavior. At least in the employment context, then, a broad interpretation of "exceeds authorized access" likely would not render § 1030(a)(2)(C) unconstitutionally vague. This observation is particularly significant in light of *United States v. Aleynikov*, 676 F.3d 71, 73 (2d Cir. 2012), which narrowed the scope of two other statutory tools available to combat employees' theft of computer trade secrets. However, the CFAA remains constitutionally vulnerable with respect to users of social media sites who violate the sites' opaque terms of use.

[61] As an alternative, the court could have adopted Professor Orin Kerr's code-based theory of authorization, under which an individual acts "without authorization" or "exceeds authorized access" only when she circumvents a *code-based* restriction on her computer privileges. Kerr, *supra* note 6, at 1599–1600. This theory of authorization not only is more faithful to the CFAA's antihacking purpose, but also arguably preserves the statute's constitutionality. *Id.* at 1600. In *Weingand v. Harland Financial Solutions, Inc.*, No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012), a district court rejected the argument that *Nosal* adopted the code-based theory and held that one could state a CFAA claim by alleging access without permission even if not barred by technical means.