No. 16-1344

IN THE

Supreme Court of the United States

DAVID NOSAL,

Petitioner,

v.

UNITED STATES OF AMERICA

Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

PETITION FOR A WRIT OF CERTIORARI

THOMAS P. SCHMIDT
HOGAN LOVELLS US LLP
875 Third Avenue
New York, NY 10022

DENNIS P. RIORDAN
TED SAMPSELL-JONES
RIORDAN & HORGAN
523 Octavia Street
San Francisco, CA 94102

NEAL KUMAR KATYAL
Counsel of Record
EUGENE A. SOKOLOFF
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5600
neal.katyal@hoganlovells.com

Counsel for Petitioner

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

QUESTION PRESENTED

The Computer Fraud and Abuse Act ("CFAA") imposes civil and criminal penalties on anyone who "accesses a computer without authorization" or who "exceeds authorized access." 18 U.S.C. § 1030(a). But three decades' experience with the statute has failed to produce any consensus on *whose* authorization matters.

In this case, the Ninth Circuit held that a computer's owner has exclusive discretion to authorize access—an account holder cannot independently confer authorization. That tracks the approach adopted by the First, Fifth, and Seventh Circuits, which define authorization in terms of the computer owner's intentions, expectations, and contractual or agency relationships. But it splits sharply with the Second and Fourth Circuits, which reject such factors as irrelevant and instead construe the CFAA narrowly as an anti-hacking statute.

The question presented is:

Whether a person who obtains an account holder's permission to access a computer nevertheless "accesses a computer without authorization" in violation of the CFAA when he acts without permission from the computer's owner.

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

Page(s)

CASES:

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

IN THE

Supreme Court of the United States

No. 16-

DAVID NOSAL,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of Certiorari to the
United States Court of Appeals
for the Ninth Circuit

PETITION FOR A WRIT OF CERTIORARI

Petitioner David Nosal respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit in this case.

OPINIONS BELOW

The Ninth Circuit's original opinion is reported at 828 F.3d 865. The Ninth Circuit's amended opinion is reported at 844 F.3d 1024. Pet. App. 1a-70a. The District Court's order denying petitioner's motions for a new trial and for acquittal is unreported but available at 2013 WL 4504652. Pet. App. 71a-138a. The District Court's order denying petitioner's motion to dismiss the indictment is reported at 930 F. Supp. 2d 1051. Pet. App. 139a-163a.

JURISDICTION

The Ninth Circuit entered judgment on December 8, 2016. That same day, the Court of Appeals denied a timely petition for rehearing en banc. On February 24, 2017, Justice Kennedy granted petitioner's timely application to extend the time for filing a petition for a writ of certiorari to and including April 7, 2017. On March 24, 2017, Justice Kennedy granted petitioner's application to further extend the time to and including May 5, 2017. This Court has jurisdiction under 28 U.S.C. § 1254(1).

STATUTE INVOLVED

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is reproduced in an appendix to this petition. Pet. App. 164a-167a.

INTRODUCTION

This case presents one of the most important and recurring questions in an age of networked computing: When does someone have permission to access someone else's computer? Any time a person logs in to their office computer or signs in to their Gmail or Facebook account, she "accesses" computers belonging to her employer, or the website's or service's owner. In this case, a divided panel of the Ninth Circuit held that doing any of those things without the owner's permission violates a federal criminal statute, the Computer Fraud and Abuse Act ("CFAA").

The panel majority's ruling puts it at the extreme end of a 4-2 circuit split. On one side, the First, Fifth, Seventh, and Ninth Circuits look to the owner's intentions, expectations, and contractual or agency relationships to determine whether access to

a computer is "authorized" under the statute. On the other side, the Second and Fourth Circuits reject such factors as irrelevant.

The Ninth Circuit's decision exposes a broad range of innocuous, day-to-day activity to criminal prosecution. If a computer's owner has exclusive discretion to grant or revoke authorization, a person could violate the statute any time he logged in to a computer in violation of the owner's policies or terms of service. Take, for example, a person who uses his spouse's password to log into the family's online banking account to pay a bill. Or an assistant who logs into an executive's email account to print out a presentation. If the banking and email services prohibit password-sharing, the Ninth Circuit's reasoning would transform these quotidian acts into violations of the CFAA, punishable by a fine and up to a year in prison, even if the users had no criminal intent.

Because the Ninth Circuit's decision exacerbates a deep division among the courts of appeals over the scope of an important federal criminal statute, and because the decision massively and unpredictably expands the scope of liability, this Court should grant review.

STATEMENT

A. Statutory Background

Congress originally enacted the CFAA in 1984 in response to the "advent of the activities of so-called 'hackers' who have been able to access (trespass into) both private and public computer systems." H.R. Rep. No. 98-894, at 10 (1984). Hackers, the House Judiciary Committee warned in proposing a subsequent amendment, "are trespassers, just as much as

if they broke a window and crawled into a home while the occupants were away." H.R. Rep. 99-612, at 5-6 (1986). "The conduct prohibited" by the CFAA was thus "analogous to that of 'breaking and entering' rather than using a computer * * * in committing the offense." H.R. Rep. 98-894, at 20 (1984); *see* S. Rep. 99-432, at 9 (1986).

The CFAA criminalizes accessing a computer "without authorization" or "exceeding authorized access." 18 U.S.C. § 1030(a). It also provides for private civil actions for damages. *Id.* at § 1030(g). The subsection at issue in this case punishes whoever "knowingly, and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access." *Id.* at § 1030(a)(4). The statute also prohibits "obtain[ing] * * * information" without authorization, regardless of culpable intent. *Id.* at § 1030(a)(2)(C). These provisions apply to any "protected computer," defined as a computer "which is used in or affecting interstate or foreign commerce or communication." *Id.* at § 1030(e)(2)(B). And the term "computer" is itself broadly defined to include, among other things, "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions." *Id.* at § 1030(e)(1). In other words, the statute reaches virtually any device connected to the Internet.

B. Factual And Procedural Background

1. David Nosal worked for Korn/Ferry International, a global executive search firm. As part of its business, Korn/Ferry maintained a database of prospective executive candidates. Pet. App. 6a-8a.

Employees used this database to identify potential placements. *Id.*

In 2004, Nosal left Korn/Ferry to start his own search firm. *Id.* at 6a. Nosal was joined in early 2005 by two former colleagues. *Id.* at 7a. Before they left Korn/Ferry, Nosal's colleagues downloaded material from the company's database. Pet. App. 8a. And, in the months following their departure, Nosal's colleagues asked Nosal's former assistant at Korn/Ferry to lend them her credentials so that they could continue to access the database. *Id.* at 8a-9a. Alerted to this activity, Korn/Ferry launched an internal investigation and eventually persuaded federal authorities to initiate criminal proceedings. *Id.* at 9a.

2. The Federal Government indicted Nosal in 2008 on a series of charges, including eight counts under the CFAA, 18 U.S.C. § 1030(a)(4). Nosal moved to dismiss the CFAA counts on the ground that the statute prohibits hacking into a computer, not misappropriating information. The District Court granted Nosal's motion in part and denied it in part. It dismissed five CFAA counts that were based on Nosal's colleagues' use of their own credentials to download information from Korn/Ferry's database while they were still Korn/Ferry employees—the "own-password" counts. But it denied Nosal's motion as to the three remaining counts, which were based on occasions when Nosal's colleagues used the password of his former assistant to access the database after they had left the firm—the "password-sharing" counts. The Government filed an interlocutory appeal, *see* 18 U.S.C. § 3731, and the Ninth Circuit eventually affirmed en banc. *See United States* v.

Nosal, 676 F.3d 854 (9th Cir. 2012) (Kozinski, J.) ("*Nosal I*").[1]

The Court of Appeals explained that the CFAA's "purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets." *Id.* at 863. It rejected the Government's contention that Nosal's colleagues "exceed[ed] authorized access" when they downloaded information in violation of Korn/Ferry policy. *Id.* at 864. The court warned that adopting such an interpretation of the statute would "expand [the CFAA's] scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer." *Id.* at 859.

3. On remand from *Nosal I*, the Government filed a second superseding indictment that charged the three password-sharing CFAA counts, two counts of trade secret theft under the Economic Espionage Act ("EEA"), 18 U.S.C. § 1832, and one conspiracy count. Pet. App. 10a. The District Court denied Nosal's renewed motion to dismiss the password-sharing counts. It found that *Nosal I* had not "explicitly h[e]ld that the CFAA is limited to hacking crimes." *Id.* at 156a. Even if it had, the District Court concluded that the indictment sufficiently alleged "circumvention of technological access barriers" by alleging that Nosal's colleagues had accessed Korn/Ferry's database by entering a borrowed password. *Id.* at 157a. The case proceeded to trial.

---

[1] Circuit precedent barred Nosal from cross-appealing the District Court's refusal to dismiss the password-sharing counts. *See United States* v. *Fort*, 472 F.3d 1106, 1121 (9th Cir. 2007).

Nosal asked that the jury be instructed that "[a] person accesses a computer without authorization when he circumvents technological access barriers." C.A. E.R. 1083; *see id.* at 109. The District Court refused. Instead, the court told the jury that it was up to Korn/Ferry "to grant or deny permission to [a] person to use the computer" and that "[a] person uses a computer 'without authorization' when the person has not received permission from Korn/Ferry to use the computer for any purpose * * * or when Korn/Ferry has rescinded permission to use the computer." *Id.* at 109. The jury returned a verdict of guilty on all counts and the District Court denied Nosal's motions for acquittal and for a new trial. Pet. App. 10a.

The jury was also instructed that, if Nosal was guilty of conspiracy, he was liable under each of the other counts, so long as the jury found that one of his alleged co-conspirators had committed the charged offense and that it furthered the conspiracy's purpose. *See* C.A. E.R. 106-107; *Pinkerton* v. *United States*, 328 U.S. 640, 646-648 (1946). Because the jury entered a general verdict on the conspiracy count, it is not clear whether it found that the conspiracy's purpose was to misappropriate trade secrets (in violation of the EEA) or to gain unauthorized access to a computer (in violation of the CFAA). Jury Verdict 1, *United States* v. *Nosal* (N.D. Cal. No. 3:08-cr-00237), Doc. 408. The Government did not dispute below that this general verdict means that, if the courts below misconstrued the elements of the CFAA, Nosal's convictions on all counts must be vacated. *See* Pet. App. 69a-70a n.17 (Reinhardt, J., dissenting).

4. A divided panel of the Ninth Circuit affirmed. In an amended opinion issued after the court denied Nosal's petition for rehearing en banc, the panel majority concluded that "Korn/Ferry owned and controlled access to its computers, including the [company's] database, and it retained *exclusive discretion to issue or revoke access* to the database." *Id.* at 19a (emphasis added). "Implicit in the definition of authorization," the majority explained, "is the notion that someone, including an entity, can grant or revoke that permission." *Id.* at 18a. The majority found that "[h]ere, that entity was Korn/Ferry." *Id.* Accordingly, it held that Nosal "acted 'without authorization'" when his colleagues accessed Korn/Ferry's database using a borrowed password after the company had "affirmatively revoked" his credentials when he left his job. *Id.* at 24a. The court used that same reasoning to reject Nosal's challenge to the District Court's jury instruction making owner permission the sole determinant of "authorization." *Id.* at 24a-26a. The majority went on to reject Nosal's challenges to the EEA and conspiracy counts. *Id.* at 26a-40a. But it vacated and remanded the District Court's restitution award. *Id.* at 41a-47a.

Judge Reinhardt dissented. He warned that the majority's opinion "loses sight of the anti-hacking purpose of the CFAA" and "threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens." *Id.* at 49a (Reinhardt, J., dissenting). "The question that matters," Judge Reinhardt argued, "is not what authorization *is* but who is entitled to give it." *Id.* at 56a. Because the statute is ambiguous on that score, Judge Reinhardt would have applied the rule of lenity and "adopt[ed] [a]

construction of CFAA that criminalizes access only by those without permission from *either* an account holder *or* the system owner." *Id.* at 58a-59a.

This petition followed.

REASONS FOR GRANTING THE PETITION

The Ninth Circuit's construction of the CFAA threatens to criminalize a broad swath of innocuous activity that ordinary people engage in every day. That alone is reason enough for this Court's immediate review. The decision also deepens longstanding confusion among the circuits over who may authorize access under the CFAA.

I. THE COURTS OF APPEALS ARE DIVIDED OVER WHO MAY AUTHORIZE ACCESS UNDER THE CFAA

The panel majority held that a computer's owner has "*exclusive* discretion" to "issue or revoke access" under the CFAA. Pet. App. 19a (emphasis added). The nation's largest Circuit, the Ninth, thus joins the First, Fifth, and Seventh in defining authorization in terms of a computer owner's intentions, expectations, and contractual or agency relationships. That contradicts the views of the Second and Fourth Circuits that such factors are irrelevant. So while a person who logs in to a computer account using a borrowed password against the owner's wishes commits a federal crime in the First, Fifth, Seventh, and Ninth Circuits, proof of the same conduct would not establish CFAA liability in the Second and Fourth Circuits.

1. Start with the Second and Fourth Circuits: Those courts have construed the CFAA narrowly as an anti-hacking statute that bars only the computer

equivalent of breaking and entering. They categorically reject any inquiry into the owner's policies or preferences. The conduct alleged in this case could not satisfy that standard because, whatever Korn/Ferry's relationship with Mr. Nosal may have been, Nosal's former assistant voluntarily lent her valid access credentials to his colleagues.

a. In *WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F.3d 199 (4th Cir. 2012), the Fourth Circuit equated authorization with the practical ability to access a computer. The court explained that "an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer." *Id.* at 204. But the court understood approval in a narrow sense. It held that even though the defendant plainly violated his employer's policies when he downloaded company information to benefit a competitor, his acts were "authorized" because he "had *access* to [the plaintiff's] intranet and computer servers." *Id.* at 206-207 (emphasis added) (citing 18 U.S.C. § 1030(a)(2)(C), (a)(4), (a)(5)(B)-(C)). In other words, the employer broadly "authorized" the defendant to access its computers by providing him with the *means* to access them.

The Fourth Circuit's reasoning suggests that authorized access, like the key to an apartment, can be shared with third parties. After all, *WEC Carolina* never specifies *whose* "permission" is required. *Id.* at 206; *see* Pet. App. 56a (Reinhardt, J., dissenting). An owner "might choose to rescind" authorization if a user shares access. *WEC Carolina*, 687 F.3d at 206. But it can do so only by changing the locks; a violation of access rules does not void the authorization. *Id.* at 206-207.

b. The Second Circuit took a similar approach in *United States* v. *Valle*, 807 F.3d 508 (2d Cir. 2015), reversing a conviction for "exceed[ing] authorized access" based on a police officer's use of a law enforcement database without a "law enforcement purpose." *Id.* at 523. The court concluded that the rule of lenity required reading the CFAA to prohibit only "hacking" offenses analogous to criminal trespass or "breaking and entering." *Id.* at 525 (quoting H.R. Rep. No. 98-894, at 3706); *see id.* at 524-526. It rejected the Government's argument that liability depends on "fact-specific questions" such as "whether the applicable authorization was clearly defined and whether the abuse of computer access was intentional." *Id.* at 528 (internal quotation marks omitted). Because the officer had access to the information he viewed, he was "authorized" to view it, even though he "violated the terms of his employment by putting his authorized computer access to personal use." *Id.* at 523 (citing 18 U.S.C. § 1030(a)(2)(B)).

The Second Circuit's decision—and its references to "hacking" and "breaking and entering"—suggest that access is "authorized" so long as it does not breach some technological access barrier. As in *WEC Carolina*, the implication is that a person who uses a borrowed password accesses a computer with the authorization the password itself implies.

2. The Ninth Circuit has now joined the First, Fifth, and Seventh Circuits in looking instead to the computer owner's intentions, expectations, and contractual or agency relationships to determine whether access is authorized. Yet it is the only Circuit to categorically bar account-holder authorization; the First, Fifth, and Seventh Circuits have read "authorization" flexibly, leaving the door open to

password-sharing and other forms of derivative authorization consistent with the owner's interests and reasonable expectations.

a. In *International Airport Centers, L.L.C.* v. *Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit construed "authorization" in light of agency-law principles. The court held that that an employee acted "without authorization" when he deleted incriminating files from his employer-issued laptop. *Id.* at 420 (citing 18 U.S.C. § 1030(a)(5)(A)(ii)). The court reasoned that deleting the information was a "breach of [the employee's] duty of loyalty" that "terminated his agency relationship * * * and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420-421.

Although the agency-based reasoning in *Citrin* limits an account holder's discretion, it would allow an account holder to delegate access to a third party in appropriate circumstances without seeking the owner's consent. *Cf.* Restatement (Third) of Agency § 8.06 (2006) (a principal's consent is required only to negate a breach of duty). The question would center on whether the delegation was consistent with the account holder's duties to the owner. *See Citrin*, 440 F.3d at 420. Thus, for example, an attorney could authorize her assistant to respond to email through her law firm account on her behalf. The assistant's access would be "authorized" in the Seventh Circuit as long as the delegation was "necessary or incidental to achieving the [firm's] objectives." Restatement (Third) of Agency § 2.02 (2006).

b. The Fifth Circuit similarly interprets authorization in light of the "expected norms of intended use,"

without requiring permission from the computer owner. *United States* v. *Phillips*, 477 F.3d 215, 219 (5th Cir. 2007). In *Phillips*, the court of appeals considered whether a student acted "without authorization" when he developed a computer program that accessed confidential data on his university's network. *Id.* at 217-218, 219 (citing 18 U.S.C. § 1030(a)(5)(A)(ii)). The court concluded that running the program "was not an intended use of the [university's] network within the understanding of any reasonable computer user." *Id.* at 220; *see id.* at 220-221; *accord United States* v. *John*, 597 F.3d 263, 271 (5th Cir. 2010).

The Fifth Circuit's "intended-use analysis" opens the door to a wide range of access-sharing. If, for example, a school that issued laptops to its students would "reasonabl[y] expect[]" that parents would occasionally use them, that use would be "authorized" in the Fifth Circuit. *Phillips*, 477 F.3d at 220 (quoting *EF Cultural Travel BV* v. *Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001)) (in parenthetical).

c. Like the Seventh Circuit, the First Circuit considers an account holder's duties to a computer's owner. But it has also suggested, like the Fifth Circuit, that the owner's reasonable expectations matter. The defendant in *EF Cultural Travel* used inside information gleaned from his time as an employee to help develop a program that "scraped" data from his former employer's website. 274 F.3d at 579-580. The court recognized that any member of the public could in theory gather the same data from the site. *Id.* at 583. "Practically speaking, however," only the scraper program, enhanced by the defendant's insider knowledge, could do so effectively. *Id.*

The court thus held that the defendant likely "exceeded authorized access" to the website. *Id.* at 580-581 (citing 18 U.S.C. § 1030(a)(4)); *see Citrin*, 440 F.3d at 420 (noting that the "difference between 'without authorization' and 'exceeding authorized access' is paper thin" if "not quite invisible"). Because the First Circuit's decision rested on the fact that the defendant was prohibited by a confidentiality agreement from using his inside knowledge to develop the scraper, it had no need to "reach the more general arguments made about statutory meaning." *EF Cultural Travel*, 274 F.3d at 581-582. But the court clearly found it relevant that an ordinary user could not easily have obtained the same data from the website. *Id.* at 583; *see also id.* at 582 n.10 (noting the role of intent and expectations in assessing whether access is authorized).

Under the First Circuit's hybrid analysis, a user's access is "authorized" so long as it comports with the user's obligations—if any—to the computer's owner, and with the owner's reasonable expectations. Absent a contractual limitation, an account holder would presumably be able to share access with a third party so long as the third party's access was consistent with the computer's intended use.

d. The Ninth Circuit now applies the most restrictive definition of "authorized" access. The panel majority in this case concluded that a computer's owner "retain[s] exclusive discretion to issue or revoke access." Pet. App. 19a. And it approved an instruction to the jury that "[w]hether a person is authorized to access the computers in this case depends on the actions taken by [a computer's owner] to grant or deny permission to that person to use the computer." Pet. App. 24a. The Ninth Circuit

thus rejects the flexibility of the First, Fifth, and Seventh Circuits' approaches. At the same time, the Ninth Circuit's analysis turns on an examination of the owner's preferences, policies, and relationships—factors the Second and Fourth Circuits emphatically reject. Indeed, the panel majority suggested that whether access is "authorized" could depend on how "stark[ly]" the owner states its preferences and how "sympathetic" the access was, Pet. App. 19a—an argument indistinguishable from one the Second Circuit dismissed out of hand in *Valle*. 807 F.3d at 528; *see supra* p. 11.[2]

The split is entrenched and the grab-bag of approaches it subsumes undermines the statute's integrity and "fail[s] to provide fair notice to ordinary people who are required to conform their conduct to the law." *United States* v. *Kozminski*, 487 U.S. 931, 949-950 (1988). This Court's intervention is urgently needed.

II. THIS CASE IS A SUPERIOR VEHICLE TO ADDRESS THE QUESTION PRESENTED

The decision below was followed one day later by a ruling from a different panel of the Ninth Circuit, holding that Facebook had exclusive discretion to control access to its users' accounts even though they had consented to access by a third-party social media

---

[2] Although the panel majority recognized that *Nosal I* held that the CFAA does not punish "violations of corporate computer use restrictions or violations of a duty of loyalty," Pet. App. 15a (internal quotation marks omitted), it distinguished that decision on the ground that *Nosal I* addressed "unauthorized *use* of information" whereas "Nosal is [now] charged with unauthorized *access*." Pet. App. 16a (emphases added).

platform. *Facebook, Inc.* v. *Power Ventures, Inc.*, 844 F.3d 1058, 1067-68 (9th Cir. 2016).[3] The defendants in *Power Ventures* filed a petition for a writ of certiorari from this Court on March 9, 2017. *See Power Ventures, Inc.* v. *Facebook, Inc.*, No. 16-1105. The question presented by *Power Ventures* is closely related to the one presented by this case: both go to whether an account holder may confer "authorization" under the CFAA. *See* Pet. at 11-13, 23-26, *Power Ventures*, *supra* (No. 16-1105) (discussing the decision below). But this case is a better vehicle to address the question for three reasons.

First, the petitioners in *Power Ventures* do not contend that their case implicates the split described above. Instead, they base their argument largely on facts peculiar to the "novel" application of the CFAA to online social networks, which is "in stark contrast to prior CFAA private claimants—typically employers or former employers." Pet. at 9, 12, *Power Ventures*, *supra* (No. 16-1105); *cf id.* at 24 (explaining that this case *does* implicate a split). That points up a second reason to prefer this vehicle; the facts in this case are in the statute's heartland and easily analogized to the leading cases in the Circuits. Finally, this case involves an application of the Act's criminal sanctions, while *Power Ventures* is a private civil case. Resolving the question presented here in

---

[3] Because the defendants "could have thought that consent from *Facebook users* to" use their accounts "was permission for [the defendants] to access *Facebook's* computers," the *Power Ventures* court held that the defendants were liable only for accessing Facebook after the company issued a cease and desist letter "expressly rescinding" that "arguable permission." 844 F.3d at 1067.

the context of a criminal prosecution, where the stakes are highest, sharpens the issues and ensures consistent application of the statute across the criminal and civil contexts. *Cf. United States* v. *U.S. Gypsum Co.*, 438 U.S. 422, 438-439 (1978) (noting that interpreting the Sherman Act primarily as a civil statute had rendered its scope "indetermina[te]").

Nevertheless, if this Court grants review in *Power Ventures*, Mr. Nosal respectfully requests that the Court grant this petition and consolidate the cases for argument. *See, e.g.*, *Exxon Mobil Corp.* v. *Allapattah Servs., Inc.*, 545 U.S. 546, 549-550 (2005) (consolidating and jointly disposing of two distinct cases presenting the same question of statutory interpretation). At the very least, this Court should hold this petition pending resolution of the *Power Ventures* case.

III. THE QUESTION IS IMPORTANT AND RECURRING

The question presented has far-reaching implications. The CFAA covers anyone "who uses a computer, smartphone, iPad, Kindle, Nook, X-box, Blu-Ray player or any other Internet-enabled device." *Nosal I*, 676 F.3d at 861. Every time a user loads a web page, checks his email, or logs into a social media account, he accesses computers owned or controlled by the publishers or providers of those services. *See id.* If the Ninth Circuit's decision is allowed to stand, whether that access is "authorized" or whether it is instead a federal crime will depend on "a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands"—precisely the result the Ninth Circuit

itself sought to avoid when it construed the statute's bar on exceeding authorized access in *Nosal I*. *Id.*

Password-protected user accounts are a ubiquitous means of controlling access to a vast array of online services. Often, these accounts exist as a way for companies to gain valuable marketing data. In other cases, account-based access protects *user* information such as emails, documents, or digital photographs. The use of these accounts is governed by private agreements, many of which expressly forbid password-sharing or impose other categorical prohibitions on who may access the website's services.[4]

The panel majority below insisted that "[t]his appeal is not about password sharing. Nor is it about violating a company's internal computer-use policies." Pet. App. 5a. And it paid lip service to *Nosal I*'s holding that "violating use restrictions *** is insufficient without more to form the basis for liability under the CFAA." Pet. App. 23a. But that is not consistent with a fair reading of the decision below, as the dissent explained. The majority held that a computer's owner "retain[s] exclusive discretion to issue or revoke" authorization within the meaning of

---

[4] *See, e.g.*, Facebook Statement of Rights and Responsibilities, effective January 30, 2015 ("You will not share your password *** [or] let anyone else access your account *** ."), *available at* https://www.facebook.com/legal/terms (last visited May 4, 2017); New York Times Terms of Service (effective November 17, 2015) ("You are not allowed to share your registration login credentials or give your login credentials to anyone else."), *available at* https://www.nytimes.com/content/help/rights/terms/terms-of-service.html (last visited May 4, 2017); Twitter Terms of Service, effective September 30, 2016 ("[Y]ou must be at least 13 years old to use the Services."), *available at* https://twitter.com/tos?lang=en (last visited May 4, 2017).

the Act. *Id.* at 19a. It thus affirmed a jury verdict based on an instruction that expressly defined "authorization" as permission from the computer's owner. *Id.* at 24a-25a. The inescapable import of the panel's holding is that accessing a computer in contravention of a use policy is a federal crime. *See Id.* at 60a-61a (Reinhardt, J., dissenting). After all, a policy that expressly bars sharing an account password, or that prohibits anyone under the age of 13 from opening an account can hardly be said to "grant * * * permission" to do those things. *Id.* at 18a (majority opinion); *see supra* n.4. And the panel explained that an account holder "ha[s] no mantle or authority to override [the owner's] authority to control access to its computers." Pet. App. 18a.

As the dissent and amici below explained, the panel majority's rule makes a crime out of such innocuous activities as "an office worker asking a friend to log into his email in order to print a boarding pass, in violation of the system owner's access policy; or * * * one spouse asking the other to log into a bank website to pay a bill, in violation of the bank's password sharing prohibition." Pet. App. 54a (Reinhardt, J., dissenting). It does the same for a husband who logs into his wife's Facebook account with her permission. *See* EFF *Amicus* Br. 17-18, *United States* v. *Nosal* (9th Cir. No. 14-10037), Doc. 14.[5]

[5] The decision below and the confusion among the Circuits have also attracted extensive academic commentary, including a recent symposium hosted by the George Washington Law Review devoted to the CFAA. *See* Symposium, *Hacking Into the Computer Fraud and Abuse Act: The CFAA at 30*, 84 G.W. L. Rev. 1437 (2016).

The very nature of networked computing compounds the problem: A person who logs into their Facebook account on a work computer is accessing both the employer's computer *and* Facebook's computers—not to mention the untold numbers of third-party computers that make the Internet possible. Under the majority's rule, a person who picks up his spouse's work-issued laptop and looks at her Facebook account has violated the CFAA *twice*—once by accessing the work-issued laptop without permission from his spouse's employer, and once by using a borrowed password to access Facebook's computers.

The majority's rule has broader social implications, too. It threatens to chill research carried out by journalists and scholars to uncover online discrimination and other abuses. *See* EFF & ACLU *Amicus* Br. in Support of Reh'g En Banc 15-18, *Nosal*, *supra*, Doc. 73. Audit testing has long been a valuable tool for ferreting out violations of civil rights laws. *See Havens Realty Corp.* v. *Coleman*, 455 U.S. 363, 373 (1982). The online equivalent of such testing may require accessing members' accounts with their permission or creating test accounts to see how users with different demographic profiles are treated. Under the majority's rule, a company need only prohibit such research in its terms of service to transform an essential means of enforcing the law into a crime itself.

Finally, the panel majority's anachronistic view of computer use threatens unintended consequences for the increasing trend towards so-called "cloud" computing. *See generally* BSA|The Software Alliance *Amicus* Br., *Nosal*, *supra*, Doc. 17. Computing services are increasingly provided online through remote servers referred to as the "cloud." *Id.* These

services permit users to store data and even use applications that are hosted remotely on hardware owned by the service provider. Remote hosting offers lower costs, better security, and enhanced flexibility. But it also departs from the traditional model of computing in which a user uses applications or data stored on a single machine or a local server. Instead, the account holder's work is both performed and stored on the service's computers. In such circumstances, sharing a password or account is not functionally different from choosing to share one's personal computer. But if the decision below stands, it is a federal crime without permission from the cloud service provider.

The panel majority claimed that such concerns "can be reserved for another day." Pet. App. 19a-20a. They cannot. The decision below creates a per se rule that applies throughout the Ninth Circuit: Access without permission from a computer's owner is access "without authorization" under the CFAA. This Court's review is needed now.

IV. THE NINTH CIRCUIT'S DECISION WAS INCORRECT

The panel majority thought that the CFAA "unambiguous[ly]" forbids accessing a computer without the owner's permission. Pet. App. 18a-20a, 24a. It does not. In fact, the statute says nothing whatsoever about *who* may authorize access to a computer. In light of the CFAA's text, purpose, and the rule of lenity, the better reading is that *either* the owner or an account holder can authorize access and that they must grant or revoke authorization unequivocally by establishing or removing technological access barriers.

1. The CFAA does not define "without authorization." *See* Pet. App. 12a. The meaning of that term "has proven to be elusive." *EF Cultural Travel*, 274 F.3d at 582 n.10. The panel majority, however, believed that "without authorization" is "unambiguous" because the word "authorization" is commonly defined as "permission." Pet. App. 17a-18a. Relying on this "straightforward meaning," it concluded that only a computer's owner—in this case, Korn/Ferry—could "authorize" access and that an account holder "had no mantle or authority" to do so on her own. Pet. App. 18a. That was quite a leap. Observing that "without authorization" means "without permission" does not even suggest, let alone establish unambiguously, that permission may come only from a computer's owner. Yet that was the extent of the panel majority's analysis of the central question in this case.

The Government did not dispute that Nosal's former assistant voluntarily shared her valid login credentials with his colleagues. *See, e.g.*, U.S. Br. 16-17, 20, *Nosal*, *supra*, Doc. 28-1. If they accessed Korn/Ferry's computers, they did so literally with "permission." Mr. Nosal's innocence or guilt of the password-sharing counts thus turns on whether that permission is sufficient under the CFAA.

From the face of the statute, there is no more reason to think that "without authorization" means "without the owner's permission" than there is to think it means "without an account holder's permission." Read in light of the statute's anti-hacking purpose, the most sensible conclusion is that *both* an owner and an account holder are valid sources of permission. That construction is not merely "possible to articulate," as the panel majority dismissively

suggested. Pet. App. 18a n.6 (quoting *Moskal* v. *United States*, 498 U.S. 103, 108 (1990)). It is consistent with the statutory text. *See United States* v. *Santos*, 553 U.S. 507, 513-514 (2008) (finding ambiguity where "all provisions of the *** statute are coherent; no provisions are redundant; and the statute is not rendered utterly absurd" under either of two possible interpretations). And it comports with Congress's stated intention to deter hackers from "breaking and entering" into computers. H.R. Rep. 98-894, at 20; *see* H.R. Rep. 99-612, at 5-6. By contrast, interpreting the CFAA to require an owner's permission risks "criminaliz[ing] a broad range of day-to-day activity"—a result Congress is highly unlikely to have intended. *Kozminski*, 487 U.S. at 949; *see supra* pp. 19-21.

The rule of lenity has particular bite where the broader reading of a statute threatens to turn every computer user in the country into an unwitting federal criminal. This Court has long required that Congress speak "in language that is clear and definite" before it will "choose the harsher" of two possible readings of a criminal statute. *Jones* v. *United States*, 529 U.S. 848, 858 (2000) (internal quotation marks omitted). Any "doubts are resolved in favor of the defendant." *United States* v. *Bass*, 404 U.S. 336, 348 (1971); *see Santos*, 553 U.S. at 514 ("Under a long line of our decisions, the tie must go to the defendant."). Under that rule, the Ninth Circuit was "bound to adopt the construction of [the] CFAA that criminalizes access only by those without permission from *either* an account holder *or* the system owner," Pet. App. 58a-59a (Reinhardt, J., dissenting), and to vacate Mr. Nosal's convictions.

None of this is to say that individuals who access computers for tortious or criminal purposes must go unpunished. Other state and federal laws provide ample civil remedies and grounds for criminal prosecution of wrongdoers. *See, e.g.*, *WEC Carolina*, 687 F.3d at 207 & n.4 (declining to adopt a broad construction of the CFAA "given that other legal remedies exist for these grievances"). The CFAA addresses one particular concern: hacking. Vindicating that purpose does not require adopting the Ninth Circuit's reading of the statute.

2. The panel majority also erred in rejecting Mr. Nosal's challenge to the jury instruction that "[w]hether a person is authorized to access the computers * * * depends on the actions taken by [the owner] to grant or deny permission to that person to use the computer." Pet. App. 24a.

If that instruction were correct, "the statute[] would provide almost no objective indication of the conduct or condition [it] prohibit[s]." *Kozminski*, 487 U.S. at 949-950. Whether access was illegal would depend instead on *private* contracts, policies, or communications. *See supra* pp. 17-19. And that "would fail to provide fair notice to ordinary people who are required to conform their conduct to the law." *Kozminski*, 487 U.S. at 949-950.

These concerns are best addressed by construing "authorization" in light of the CFAA's anti-hacking purpose. Hacking, as the Ninth Circuit explained in *Nosal I*, is "the circumvention of technological access barriers." 676 F.3d at 863. The panel majority thought the evidence in this case met that test because "[t]he password system adopted by Korn/Ferry is unquestionably a technological barri-

er." Pet. App. 26a. But the majority's conclusion does not follow from its premise. Real circumvention might involve technological attacks, such as computer programs designed to guess at thousands of possible passwords. *See Phillips*, 477 F.3d at 217 n.1, 220. Or it could involve obtaining legitimate credentials through fraud, such as "phishing." Indeed, the statute specifically prohibits "traffic[king] * * * in any password or similar information through which a computer may be accessed without authorization." 18 U.S.C. § 1030(a)(6). But a person who gains admission to a computer with a legitimately borrowed password does not "circumvent" a password system any more than a houseguest who uses his host's key "circumvents" a lock.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

THOMAS P. SCHMIDT
HOGAN LOVELLS US LLP
875 Third Avenue
New York, NY 10022

DENNIS P. RIORDAN
TED SAMPSELL-JONES
RIORDAN & HORGAN
523 Octavia Street
San Francisco, CA 94102

NEAL KUMAR KATYAL
Counsel of Record
EUGENE A. SOKOLOFF
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5600
neal.katyal@hoganlovells.com

Counsel for Petitioner

May 2017