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

REPLY BRIEF IN SUPPORT 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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

IN THE
Supreme Court of the United States

No. 16-1344

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

REPLY BRIEF IN SUPPORT OF CERTIORARI

INTRODUCTION

Every day, hundreds of millions of Americans log in to computers that belong to someone else using passwords or other personalized credentials. Under the rule adopted by the Ninth Circuit in this case, sharing those credentials is a federal crime absent permission from the computer's owner. That is not the case in five other circuits, which have taken a number of different approaches to determining *who* may authorize access under the CFAA.

The Government does not seriously dispute that the circuits are divided over who may authorize access under the CFAA. Rather, it argues (at 12) that no split is "implicated" in this case. The Government is wrong. The Government claims (at 12-

13) that the Second and Fourth Circuits have not dealt with the same facts. But it fails to explain what difference those facts would make. The Government contends (at 14-17) that the First, Fifth, and Seventh Circuits' interpretations of the CFAA would not change the outcome here. But in light of the jury instructions in this case, adopting any one of those interpretations would require vacating the convictions. The conflict is real, outcome-determinative, and urgently in need of resolution.

The Government's effort to downplay the sweeping implications of the panel majority's reasoning is no more persuasive. The Government insists (at 10) that the Ninth Circuit did not did not adopt a general rule that gives computer owners exclusive discretion over access in all cases. But the panel majority reasoned that another person can authorize access *only* if the owner allows it. The Government repeats (at 11) the panel majority's claim that this case "is not about password sharing." Pet. App. 5a. But the conduct punished as a violation of the CFAA in this case was, after all, the use of a password that had been freely shared to gain access to a computer.

The *amici* have warned that the Ninth Circuit's decision fuels longstanding uncertainty over the scope of the CFAA and threatens to criminalize a broad range of innocuous password sharing and socially valuable research. *See* EFF *Amicus* Br. 16-18; Bratus, et al. *Amicus* Br. 18-21. That cannot be what Congress intended when it passed the CFAA to combat computer hacking. This case is the ideal vehicle for this Court to finally address the question that has divided the circuits and restore the CFAA to its intended purpose. This Court should grant review.

ARGUMENT

I. THE DECISION BELOW DEEPENS LONGSTANDING CONFUSION AMONG THE CIRCUITS

The Ninth Circuit's decision exacerbates a 4-2 circuit split over who may authorize access under the CFAA. The Government's effort to dispel that split rests on immaterial distinctions and untenable assumptions.

1. Start with the Ninth Circuit's break with the Second and Fourth Circuits. The Ninth Circuit held that whether access is "authorized" turns on the subjective intentions, preferences, and policies of the computer's owner; the Second and Fourth Circuits have found such factors irrelevant. *See* Pet. 9-11. The Government does not dispute the petition's characterization of the split. Instead, it argues (at 12) that "no circuit conflict is implicated here" because neither *WEC Carolina* nor *Valle* "involved post-revocation surreptitious access." That distinction makes no difference.

The fact that Nosal's colleagues may have used a borrowed password "surreptitiously" is plainly irrelevant under the Fourth Circuit's decision in *WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F.3d 199 (4th Cir. 2012). The court in that case was "unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy." *Id.* at 207. Nor is the fact that Korn/Ferry had "revoked" their access dispositive. Circumventing that revocation by borrowing a password might violate a use policy that forbids sharing

passwords and it may suggest bad faith, but those are two things the Fourth Circuit has expressly declined to place within the statute's ambit.

The Government's distinction is no more persuasive with respect to the Second Circuit's decision in *United States* v. *Valle*, 807 F.3d 508 (2d Cir. 2015). Indeed, the court there expressly rejected the reading of the CFAA the Government imputes (at 10) to the Ninth Circuit here. The Second Circuit found that letting CFAA liability depend on "whether the applicable authorization" in a given case "was clearly defined and whether the abuse of computer access was intentional" would not address "the risk of criminalizing ordinary behavior inherent in [a] broad construction" of the statute. *Id.* at 528. The Second Circuit would thus have found the purportedly "stark revocation" and "[un]sympathetic access through an authorized third party" in this case irrelevant. U.S. Br. 10 (quoting Pet. App. 19a-20a).[1]

2. The Government does not seriously dispute the petition's characterization of the divergent approaches to "authorization" taken by the First, Fifth, and Seventh Circuits, either. *See* Pet. 11-15. Rather, it contends that the rules those courts apply would not change the outcome in this case. The Government is wrong. If the CFAA defined "authorization" as the First, Fifth, or Seventh Circuits have, Nosal's convictions would have to be vacated.

---

[1] The Government also notes (at 13) that *Valle* squarely addressed only the CFAA's prohibition on "*exceed[ing]* authorized access," not the "without authorization" prong at issue here. 807 F.3d at 523 (emphasis added). But that makes no difference to the question *who* may authorize access.

The District Court instructed the jury 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 and the person uses the computer anyway." C.A. E.R. 109 (emphasis added). The verdict form did not distinguish between the authorization and revocation theories. *See* Jury Verdict, *United States* v. *Nosal* (N.D. Cal. No. 3:08-cr-00237), Doc. 408.

Under the First, Fifth, or Seventh Circuits' rules, simply accessing a computer without having "received permission from Korn/Ferry," C.A. E.R. 109, would "fail[] to come within the statutory definition of the crime." *Griffin* v. *United States*, 502 U.S. 46, 59 (1991). And accessing a computer after the owner's authorization was revoked would violate the statute only if the jury found facts as to which it received no instructions at all. The jury was never instructed about the existence or scope of any duty Nosal's former assistant may have owed Korn/Ferry, about what might constitute Korn/Ferry's "reasonable expectations," or about the relevance of any "confidentiality agreement" Nosal's former assistant may have signed. The Government does not suggest otherwise.

Because adopting the approaches taken by any of these other circuits would make it impossible to conclude "beyond a reasonable doubt" that the jury had not "convicted [Nosal] for conduct that is not unlawful," his convictions would have to be vacated. *McDonnell* v. *United States*, 136 S. Ct. 2355, 2375

(2016) (quoting *Neder* v. *United States,* 527 U.S. 1, 16 (1999)).[2]

II. REVIEW IS ESSENTIAL BECAUSE THE DECISION BELOW DRAMATICALLY AND UNPREDICTABLY EXPANDS THE SCOPE OF A FEDERAL CRIMINAL STATUTE

The Ninth Circuit held that a person violates the CFAA any time he logs into a computer without permission from its owner. As *amici* point out, that holding potentially criminalizes a wide range of innocuous password sharing and account access. *See* EFF *Amicus* Br. 16-18; Bratus, et al. *Amicus* Br. 17-18; *see also* Pet. App. 62a-64a (Reinhardt, J., dissenting).

1. The Government insists that the decision below is narrower. It argues (at 10) that the panel majority did not create a blanket rule that gives computer owners exclusive discretion over access in all cases, and it leans heavily (at 11) on the panel majority's claim that this case "is not about password sharing." Pet. App. 5a. The Ninth Circuit's reasoning cannot bear those limitations.

For starters, the decision below is plainly not confined to the "circumstances of this particular case,"

---

[2] The Government contends (at 6, n.*) that it preserved the argument that Nosal's convictions on the conspiracy and trade-secrets counts would survive reversal on the CFAA counts. Not so. As the petition explained, and the dissent below observed, the Government did not dispute Nosal's argument that the convictions would fall together. *See* Pet. 7. A footnote in the Government's opposition to Nosal's petition for rehearing en banc could not resurrect that argument.

as the Government contends (at 10). Under the Ninth Circuit's reasoning, the owner *always* and *necessarily* retains exclusive discretion over access because only the owner can give others permission to share access. Indeed, the reason the panel majority concluded that Nosal's former assistant could not confer "authorization" by sharing her password was that she "had no mantle or authority to override Korn/Ferry's authority to control access to its computers." Pet. App. 18a; *see id.* at 19a & n.7.

Nor can there be any doubt that this case *is* about password sharing. Nosal was convicted of violating the CFAA on the basis of his colleagues' use of his former assistant's password on three occasions. It is undisputed that Nosal's former assistant freely gave Nosal's colleagues permission to use her valid login credentials so that they could access Korn/Ferry's computers. U.S. C.A. Br. 16-17, 20. That is the definition of password sharing.

The Government stresses (at 12) that Nosal's colleagues acted "surreptitiously by purporting to be" Nosal's former assistant "precisely because they lacked authorization to access" Korn/Ferry's computers "themselves." But that does not make this case any less about password sharing. Nosal's colleagues did not trick his former assistant or act without *her* permission. The Ninth Circuit's decision can only mean one thing: Accessing a computer with a shared password is a federal crime unless the computer's *owner* approves.

2. The *amici* have warned that the Ninth Circuit's expansive reading of the statute vests prosecutors with discretion to bring federal criminal charges for conduct that the vast majority of Americans would

not recognize as wrong, let alone unlawful. *See* EFF *Amicus* Br. 17-18; Bratus, et al., *Amicus* Br. 17-18; *see also* Pet. 19-21 (citing amicus briefs filed below).

As the dissent below explained, "[i]t is impossible to discern from the majority opinion what principle distinguishes authorization in Nosal's case from one in which a bank has clearly told customers that no one but the customer may access the customer's account, but a husband nevertheless shares his password with his wife to allow her to pay a bill." Pet. App. 63a (Reinhardt, J., dissenting).

And the consequences of the Ninth Circuit's decision sweep beyond even these innocuous private instances of password sharing. The uncertainty and confusion created by a broad reading of the CFAA threaten to chill important computer security research—ironically weakening defenses against the very hackers the CFAA was meant to punish. *See* Bratus, et al. *Amicus* Br. 19. Audit testing for online discrimination and academic research are also at risk. EFF *Amicus* Br. 18-21.

The Government suggests (at 10-11) that such hypothetical situations would not violate the CFAA because they presumably do not involve individuals who received "particularized notice" that they were not authorized to access a computer. Pet. App. 19a. But if *scienter* is the Government's limiting principle, then it is hopelessly vague.

The Ninth Circuit's opinion left open whether some "less stark revocation" would be insufficient to trigger liability. Pet. App. 19a. And that uncertainty is not resolved by the Ninth Circuit's decision in *Facebook, Inc.* v. *Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), which conflates authorization with *scien-*

ter by suggesting that a person may use a shared password until the owner expressly says otherwise. *See id.* at 1067. On the contrary, as the Second Circuit observed in *Valle*, fact-specific inquiries into the clarity of an owner's wishes or the intent of the user do not address the risk of over-criminalization. *See* 807 F.3d at 528. This Court's review is badly needed.

III. THIS CASE IS THE IDEAL VEHICLE TO DECIDE THE QUESTION PRESENTED

The Government asserts (at 12) that certiorari should be denied because "this case involves a fact pattern of clearly unlawful activity." But the Government identifies no obstacle to this Court's review of the question presented. Nosal's convictions would have to be vacated under the interpretations of the CFAA adopted in five other circuits. And the circumstances of this case do not diminish the importance or urgency of the question.

This Court's "concern is not with tawdry tales" of surreptitious access to Korn/Ferry computers; "[i]t is instead with the broader legal implications of the Government's boundless interpretation of the" CFAA. *McDonnell*, 136 S. Ct. at 2375. This criminal prosecution, which involves the use of a freely shared password, throws those broader implications into sharp relief. Granting review here would allow the Court to finally address the question who may authorize access under the CFAA on a factual record that is squarely within the heartland of the statute.

As explained in the petition, that makes this case a better vehicle for resolving the question presented than the petition pending in *Power Ventures*, a civil case involving a novel fact pattern that does not

purport to implicate a circuit conflict. *See* Pet. 15-17. Nevertheless, if the Court is inclined to grant certiorari on the closely related question in *Power Ventures*, Mr. Nosal respectfully requests that this petition be granted and consolidated with that case for argument or, at the very least, held pending a decision.

IV. THE DECISION BELOW IS WRONG

Although the Government insists Nosal is guilty, it offers only a fleeting defense of the reasoning the panel majority relied on to affirm his conviction. It is that deeply flawed reasoning that now defines the scope of the CFAA in the Nation's largest circuit.

The Government repeats (at 9) the panel majority's observation that "the 'ordinary' and 'common-sense meaning' of 'authorization' is 'permission or power granted by an authority.'" (quoting Pet. App. 17a (internal quotation marks omitted)). But, as the dissent noted below, "[t]he question that matters is not what authorization *is* but who is entitled to give it." Pet. App. 56a (Reinhardt, J., dissenting).

Like the panel majority, the Government is unable to identify a statutory basis to conclude that an authorized user cannot also be "an authority" who may grant "permission" by sharing her password. Rather, the Government argues (at 9-10) that, in *this* case, a confidentiality agreement purportedly prohibited such password sharing. But that runs headlong into the "[s]ignificant notice problems [that] arise if [courts] allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read." *See United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) ("*Nosal I*").

Nor does the Government explain why the Court should not resolve the question presented and avoid any potential notice problems by construing the CFAA consistent with its anti-hacking purpose to require "the circumvention of technological access barriers." *Id.* at 863. The Government asserts (at 17) that the judgment below would still be affirmed under that interpretation because Korn/Ferry's password system was a "technological access barrier." But Nosal's colleagues did not "circumvent" the password system; they used a valid, freely shared password.

As the *amici* explain, the CFAA was meant to outlaw "serious technological intrusion" such as "breaking into a computer system for the purpose of accessing or altering information." EFF *Amicus* Br. 6-7; *see* Bratus, et al. *Amicus* Br. 14. Interpreting "without authorization" to require the technological equivalent of "breaking and entering," H.R. Rep. No. 98-894, at 3706 (1984), would require reversal.

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

SEPTEMBER 2017