No. 16-1105

IN THE

Supreme Court of the United States

POWER VENTURES, INC., ET AL.,

Petitioners,

v.

FACEBOOK, INC.,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF IN OPPOSITION

I. Neel Chatterjee
GOODWIN PROCTER LLP
135 Commonwealth Dr.
Menlo Park, CA 94025

Monte Cooper
Brian P. Goldman
Robert L. Uriarte
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025

Eric A. Shumsky
Counsel of Record
Hannah Garden-Monheit
ORRICK, HERRINGTON & SUTCLIFFE LLP
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400
eshumsky@orrick.com

Counsel for Respondent

QUESTION PRESENTED

Petitioners (Power Ventures and its CEO) operated a website, power.com, that harvested digital content from social networking sites like Facebook, and then republished it on their own website. Facebook repeatedly instructed them to cease and desist. When Petitioners refused, Facebook put up technological barriers to block Petitioners from accessing Facebook's computers. Petitioners then intentionally circumvented those measures by masking their computers' identity to continue accessing Facebook.

The question presented is whether Petitioners "intentionally access[ed] a computer without authorization," in violation of the Computer Fraud and Abuse Act, when they continued accessing Facebook's computers after Facebook clearly and repeatedly told them to stop and implemented technological barriers to block their access.

CORPORATE DISCLOSURE STATEMENT

Facebook, Inc. has no parent corporation, and no publicly held corporation owns 10% or more of Facebook, Inc.'s stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

This case involves a concededly splitless interpretation of the Computer Fraud and Abuse Act (CFAA), and a factbound application of that statute to activities that fall squarely within its heartland. Power Ventures committed computer trespass when it blatantly disregarded Facebook's express admonition to "keep out" of Facebook's computers, and then deliberately circumvented the digital fences that Facebook erected to enforce that command. The Court of Appeals' holding that Petitioners "intentionally access[ed] a computer without authorization" is correct and unremarkable. 18 U.S.C. § 1030(a)(2). A party is "without authorization" to access a computer when, as here, "permission has been revoked explicitly." Pet. App. 16a.

Most important for present purposes, no court has held otherwise, as Petitioners repeatedly acknowledge. Pet. 10, 14, 19. And that is why the best they can muster is an "abstract[]" connection to a circuit split concerning a *different* provision of the CFAA, which governs parties who *do* have authorization to access a computer but "exceed" the scope of that authorization. Pet. 24. But, as the Court of Appeals explained, "this case does not present the more nuanced question of exceeding authorization" because "Facebook explicitly revoked authorization for *any* access" to its computers. Pet. App. 20a.

The acknowledged lack of any circuit split on the question actually presented here provides ample reason to deny the petition. In addition, the petition suffers from multiple defects that make it an unusually

poor vehicle for considering the question presented. The first is an extraordinary case of waiver. Petitioners' principal argument is that "authorization" to interact with Facebook's system is not Facebook's to give or rescind because Facebook does not operate "protected computer[s]" within the meaning of the statute. *E.g.*, Pet. 8. That argument, however, was neither pressed nor passed upon below—or, indeed, at any point during the 8½ years this case has been pending. In addition, the question presented is not outcome-determinative. The Ninth Circuit affirmed Petitioners' liability under both the CFAA and a distinct state statute, the California Comprehensive Computer Data Access and Fraud Act (California Penal Code § 502), and the District Court's judgment imposes the same damages and relief under both provisions. Petitioners do not challenge that adequate and independent state-law ground for the decisions below, so a decision in their favor would have no effect on the outcome in this case.

For all of these reasons, the petition should be denied. And it should be denied outright, rather than held for any other pending petition. *Cf.* Pet. 11. Given Petitioners' waiver; the independent basis for the judgment; and critical differences with the other pending petition identified by Petitioners, there is no realistic possibility of the judgment here being affected.

STATUTORY PROVISIONS INVOLVED

In addition to the statutory provisions set forth in the petition, California Penal Code § 502(c)(2) supplied an independent ground for the judgment. It provides:

> (c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:
>
> ....
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

STATEMENT

1. Petitioners are a Cayman Islands corporation called Power Ventures and its CEO, Steven Vachani. In 2008, they wanted to break into the market for social networking websites. Pet. App. 6a. But Power did not want to build a network of its own. Instead, Petitioners conceived a business based on aggregating user information from, and co-opting the networks that users had built on, existing social media websites

like Facebook. *Id.* Thus, Petitioners developed a software program to collect (or "scrape") user information from such sites. Pet. App. 18a & n.4, 59a, 100a.

Scraping, however, puts users' privacy at risk. Once an outsider has harvested data from Facebook, Facebook cannot prevent the scraper from posting the data to other audiences, storing it insecurely, or otherwise compromising its security. ER180-81, SER379.[1] Scraping also can impair the proper functioning of the targeted website (i.e., Facebook's) by burdening the network and thereby slowing down Facebook's computer servers. ER180-81; SER482. For these reasons, Facebook forbids third-party developers from scraping information from its computers. SER379, 482. Instead, Facebook enables third-party developers to build applications that interact with Facebook in ways that ensure the security and privacy of Facebook user data. Pet. App. 7a-8a.

Because scraping was central to Power's business model, Power bypassed the approved secure channels for accessing Facebook. SER37, 372-73. Instead, Power solicited Facebook users' login credentials, and then used that access to scrape data from Facebook—including data not only from the users whose credentials Power had employed, but also the personal information and photographs of *other* Facebook users. Pet. App. 28a, 59a. In short, Power was taking and warehousing information about its users *and* its users'

[1] "ER" refers to the appellants' excerpts of record filed in the Court of Appeals, and "SER" refers to the appellee's excerpts of record. *Facebook, Inc. v. Power Ventures, Inc.*, No. 13-17154 (9th Cir.), ECF Nos. 18, 36.

friends. Power knew that Facebook and other social media websites would disapprove of this practice for security reasons, and "anticipated attempts to block [its] access by [those] network owners." Pet. App. 53a.

2. Power's prediction proved correct. In late 2008, Facebook detected Power's scraping software operating on its network. Pet. App. 8a, 35a. Expert analysis later revealed that Power's software was not only scraping private content, Pet. App. 6a, 35a, but also automatically sending tens of thousands of junk-mail messages to Facebook users asking them to join Power, such as "I am competing for the $100 prize in the 100x100x100 [Power] promotion and recommend you to participate too!" SER 382-83; *see* Pet. App. 8a, 40a-42a. Facebook immediately sent a letter informing Power that its access to Facebook was unauthorized and demanding that Power stop. Pet. App. 8a.

Undeterred, Vachani had informed his team that "we need to be prepared for Facebook to try to block us and the[n] turn this into a national battle that gets us huge attention." Pet. App. 18a. To that end, Petitioners designed and deployed "workaround solution 1"—their plan to use "proxy servers" to change Power's Internet Protocol (IP) address to circumvent Facebook's anticipated efforts to block its address—the digital equivalent of blocking an unwanted caller's telephone number. SER 88; Pet. App. 8a. Petitioners designed this "solution" for the express purpose of connecting to Facebook's computers through proxies that would conceal Power's identity, just as a harassing caller might route his phone calls through other telephone exchanges to mask their source. Pet. App. 48a-52a.

Thus, when Facebook eventually informed Power that it had blocked the company's access to Facebook by instituting an IP address block, SER305-06, Petitioners responded by changing their address, and then as Facebook promptly blocked each new IP address upon discovery, Petitioners changed the addresses again "in a game of cat and mouse." Pet. App. 50a. Finally, Petitioners adopted their "Amazon solution," SER292: switching to an IP address associated with the popular e-commerce website amazon.com, which Facebook could not block without also blocking its users' legitimate access to its system. SER399.

After weeks of this back-and-forth, Petitioners finally told Facebook what Vachani had been saying internally—they had no intention of complying. Petitioners had made the "business decision" to continue accessing Facebook, even though Petitioners knew "this is not your desired action." SER302. And Petitioners chided Facebook for the "serious strategic mistake" of trying to block Power. SER303. Power then used its unauthorized access to Facebook to engage in a massive marketing campaign, which involved co-opting users' accounts to send over 60,000 junk messages to the Power users' Facebook friends. Pet. App. 8a.

3. Having failed to stop Petitioners' trespasses with cooperative discussion, formal demands, or technical blocks, Facebook ultimately brought this civil suit under the CFAA, 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502.

The District Court granted summary judgment in favor of Facebook on both counts. Pet. App. 55a. It held that "the undisputed facts establish that Defendants circumvented technical barriers to access [the] Facebook site." Pet. App. 52a. The court relied on "Vachani's own statements," which "provide compelling evidence that he anticipated attempts to block access by network owners and intentionally implemented a system that would be immune to such technical barriers"—a system Power then "utilized ... to effectively circumvent these barriers." Pet. App. 53a. A second judge (to whom the case was reassigned) agreed, and denied a motion for reconsideration. Pet. App. 57a-109a. The court awarded compensatory damages equal to Facebook's cost of investigating and trying to stop Petitioners' actions. Pet. App. 36a. It also issued an injunction to prevent additional violations, citing Petitioners' clear willingness to keep violating the law in the face of repeated requests to stop. Pet. App. 104a.

4. The Court of Appeals unanimously affirmed that Power violated the CFAA as of the date of Facebook's cease and desist letter. Pet. App. 21a. The court explained that a party "can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." Pet. App. 15a-16a. Here, "Facebook expressly rescinded" any permission Power had to access Facebook's computers "when Facebook issued its written cease and desist letter" and "imposed IP blocks in an effort to prevent Power's continued access." Pet. App. 17a. Nor had this been a trap for the unwary; "Power knew that it no longer had authorization to access Facebook's computers, but continued

to do so anyway." Pet. App. 18a. Petitioners "deliberately disregarded the cease and desist letter and accessed Facebook's computers without authorization," and thus violated the CFAA. Pet. App. 19a.

In addition, the court unanimously affirmed liability as to Facebook's claim under California law. Pet. App. 21a-22a. Section 502, the court explained, "is 'different' than the CFAA."[2] Petitioners violated § 502 because "when Facebook sent the cease and desist letter, Power, as it conceded, knew that it no longer had permission to access Facebook's computers at all." Pet. App. 22a. "Power, therefore, knowingly accessed and without permission took, copied, and made use of Facebook's data." *Id.*

The Court of Appeals also affirmed the District Court's decisions to impose discovery sanctions on Power, and to hold Vachani personally liable for his central role in the misconduct. Pet. App. 22a-23a. Finally, it reversed the judgment against Petitioners with respect to Facebook's claim under the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, 15 U.S.C. § 7704(a)(1). Pet. App. 9a-13a. Accordingly, the court remanded for the District Court to consider how, if at all, remedies would have to be modified to exclude the reversed

---

[2] Pet. App. 21a (quoting *United States v. Christensen*, 801 F.3d 970, 994 (9th Cir. 2015), *amended on other grounds*, 828 F.3d 763 (9th Cir. 2016), *cert. denied*, 137 S. Ct. 628 (2017), *and cert. denied sub nom. Kachikan v. United States*, No. 16-8582, 2017 WL 1232848 (U.S. May 1, 2017)).

CAN-SPAM judgment, and to account solely for the CFAA and § 502 violations. Pet. App. 23a-24a.

5. Power and Vachani petitioned for panel rehearing or rehearing en banc with respect to the CFAA claim. No judge called for an en banc vote. Pet. App. 5a. The panel denied the petition for rehearing and concurrently issued an amended opinion on December 9, 2016. Pet. App. 4a-5a. Power and Vachani's petition to this Court followed.

6. In the meantime, the District Court moved forward with reassessing remedies. Judge Koh considered at length the parties' submissions on damages, and awarded $79,640.50 in compensatory damages under both the CFAA and § 502. *Facebook, Inc. v. Power Ventures, Inc.*, ___ F. Supp. 3d ____, No. 5:08-cv-05780-LHK, 2017 WL 1650608, at *1 (N.D. Cal. May 2, 2017); *see* Judgment at 1, No. 5:08-cv-05780-LHK (N.D. Cal. May 2, 2017), ECF No. 437.

The court also again assessed injunctive relief. And again it concluded that an injunction was warranted under both the CFAA and § 502. 2017 WL 1650608, at *13. Recounting the history of Petitioners' evasions, the court emphasized that "Defendants have frequently exhibited bad faith conduct that indicates that they will not be easily deterred from attempting to access Facebook's servers without authorization in violation of the CFAA and § 502." *Id.* at *13-14; *see also id.* at *14 ("[B]efore Facebook filed the instant suit, Defendants 'deliberately implemented … tactics to circumvent plaintiff's security measures,' and Defendants continued to illegally ac-

cess Facebook's computers even after Vachani 'repeatedly assured [Facebook's counsel] that the functionality of the Power website would be changed ….'" (internal citations omitted)). As of the filing of this brief, additional proceedings in that court remain ongoing, and Petitioners have appealed the District Court's reinstated judgment to the Ninth Circuit (No. 17-16161).

REASONS TO DENY THE PETITION

I. The Petition Should Be Denied Because There Is No Circuit Split On The Question Presented.

A. Petitioners acknowledge that there is an "absence of a circuit split" on the question whether conduct like theirs constitutes improper access "without authorization" under the CFAA. Pet. 14; *see also* Pet. 10, 19. And correctly so. A defendant who accesses a computer despite the fact that "he or she has no permission to [do so]," or that "such permission has been revoked explicitly," Pet. App. 16a, plainly does so "without authorization," 18 U.S.C. § 1030(a)(2)—and no court ever has held otherwise. That is because conduct like Petitioners' is a textbook violation of the CFAA. They continued to access Facebook's system even though "Power knew that it no longer had authorization to access Facebook's computers." Pet. App. 18a.

The lack of a circuit split is ample reason to deny the petition. Petitioners contend that the Court should grant certiorari "even in the absence of a circuit split," citing two cases in which the Court did so.

Pet. 19-20. But that of course is not the norm, and neither case is remotely analogous to this one. *White v. Woodall* was a petition brought by the Commonwealth of Kentucky seeking review of a Sixth Circuit decision granting habeas relief under the Antiterrorism and Effective Death Penalty Act in a capital case. 134 S. Ct. 1697 (2014). *Owasso Independent School District No. 1-011 v. Falvo* involved a school district's appeal of a decision that a common academic practice violated the Family Educational Rights and Privacy Act. 534 U.S. 426 (2002). Petitioners here are not government entities, and no comparable governmental interests or programs are constrained by the decision below. This is a civil dispute between private parties, involving egregious bad-faith conduct, and a decision that breaks no new ground.

B. The clearest indication that the petition does not merit review is that Petitioners seek to rely on a circuit split on a *different* provision of the CFAA—namely, the prohibition against "exceed[ing] authorized access" to a computer. Pet. App. 20a; *see* 18 U.S.C. § 1030(a)(2). But the statute makes plain, and this Court recently has recognized, that these are two distinct types of violations.[3] This case concerns the meaning of *unauthorized* access; it has nothing to do with any claim about *exceeding authorized* access. It should go without saying that the Court grants review

[3] *See Musacchio v. United States*, 136 S. Ct. 709, 713 (2016) ("The statute … provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly.").

to resolve circuit splits on issues that actually are presented by a case; it does not grant review to resolve questions presented on *other* issues in *other* cases. That is why—as Petitioners themselves put it—the "exceeds authorized access" provision that was not the basis for the decision below is relevant only "when framed at a high[] level of abstraction." Pet. 24. And, stranger still, it is why Petitioners suggest that the Court would itself have to "tweak[]" Petitioners' own Question Presented. *Id.*

It is no accident that a split has emerged over the "exceeds authorized access" provision, but not the "without authorization" provision at issue here. The former involves a subtle and fraught inquiry into when a computer user—who otherwise is authorized to use the computer—has *exceeded* that authorization by misusing the computer for unsanctioned purposes. Accordingly, some courts have adopted a narrowing construction of the "exceeds authorized access" provision because "[b]asing … [CFAA] liability on violations of private computer use polic[i]es c[ould] transform whole categories of otherwise innocuous behavior into federal crimes." *United States v. Nosal* (*"Nosal I"*), 676 F.3d 854, 860 (9th Cir. 2012) (en banc); *see* Pet. 24 (citing cases). Other courts, however, have held that employees "exceed[] authorized access" when they use an employer's computer or data for non-work purposes. *E.g.*, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir. 2001); *see* Pet. 24 (citing cases).

The "without authorization" provision, by contrast, has not divided the courts because it does not require difficult line-drawing. The sole question is

whether the defendant had authorization to access the computers *at all* (which here, Petitioners plainly did not have, as they undisputedly knew). Accordingly, as the Court of Appeals explained, "this case does not present the more nuanced question of exceeding authorization"—the only question that has divided the courts—because "Facebook explicitly revoked authorization for *any* access" to its computers. Pet. App. 20a; *see also* Pet. App. 21a ("[C]oncerns about overreaching or an absence of culpable intent simply do not apply here, where an individualized cease-and-desist letter is a far cry from the permission skirmishes that ordinary Internet users may face.").

C. At root, Petitioners' argument is that the owner of a computer system (here, Facebook) lacks the final say about "authorization" to access its system. But there is no conflict over that question. The Ninth Circuit has held that an account holder cannot authorize access to a computer it does not own, against the express wishes of the computer owner. Pet. App. 19a; *see also United States v. Nosal* (*"Nosal II"*), 844 F.3d 1024, 1037-38 (9th Cir. 2016). No other circuit has passed upon that question. Petitioners cite cases involving the "exceeds authorized access" provision—but in all of those cases, it was undisputed that the defendants' employers had authorized them to access a work computer or data, at least for certain purposes. The question whether someone else could have authorized their access was not presented. Pet. 24 (explaining that the "exceeds authorized access" split concerns situation "where the employee was entitled to access but did so for an unauthorized use").

This is why Petitioners acknowledge that there is no split on the actual question presented. The defendant in *Nosal II* has filed a petition for certiorari (which Petitioners seek to have this petition consolidated with or held for) that takes a different tack. *See* Petition for Writ of Certiorari, *Nosal v. United States*, No. 16-1344, 2017 WL 1832040 (U.S. May 5, 2017). We explain below (at 18) why there is no basis for a hold, but Nosal's argument that there is a split is wrong in any event. Nosal seeks to glean from dicta in the "exceeds authorized access" cases purportedly differing standards as to who can authorize access. *Id.* at *9-15. But that is just an artful effort to conflate the circuit split concerning "exceeds authorized access" with the distinct question presented here. Neither Nosal's approach, nor Petitioners' invitation to consider these distinct issues at a "high level of abstraction," can alter the fact that no circuit but the Ninth has passed upon the question whether (or when) an account holder can grant an otherwise-prohibited user "authorization" to access a protected computer it does not own.

II. The Petition Should Be Denied Because This Case Is An Especially Poor Vehicle To Address The Question Presented.

A. Petitioners waived the primary issue they now press as grounds for reversal.

The petition should be denied because Petitioners' central argument was waived below. According to Petitioners, the reason that Facebook has no right to deny Power authorization to connect to the computers owned and operated by Facebook is that "Facebook is

not a 'protected computer' as the term is defined and used in the 1986 statute." Pet. 8. For that reason, Petitioners contend, the "'authorization' the CFAA refers to is plainly that of the data owners and users," Pet. 8—that is, the individual Power users whose Facebook accounts Petitioners co-opted. According to Petitioners, the Court of Appeals' mistaken "belief that Power was accessing 'Facebook's computers'" was the linchpin of its "errant conclusion." Pet. 8; *see also* Pet. 18-19.

But Petitioners did not press their "protected computer" argument below. *See generally* Pet. C.A. Br. 28-29, 35-42; Pet. C.A. Reply Br. 5-12. The term "protected computer" was never discussed in Petitioners' briefs to the Ninth Circuit. Nor did they even cite 18 U.S.C. § 1030(e)(1) or (2), the provisions upon which Petitioners base this argument. Pet. 15, 19. Petitioners' failure to press this argument is why neither the District Court nor the Court of Appeals passed upon it. Although Petitioners did argue that individual users could authorize Power to access Power users' data on Facebook, Petitioners offered no justification for the unlikely proposition that a computer owner possesses no independent right to exclude.[4] Petitioners' new effort to close that gap by

[4] Even if Petitioners had preserved this argument, it is plainly without merit. As they concede, the CFAA "broadly" defines "protected computer" as a computer "'used in or affecting interstate or foreign commerce or communication.'" Pet. 19 (quoting 18 U.S.C. § 1030(e)(2)(B)). A website like facebook.com is a "protected computer" because a website resides on physical computers connected to the Internet—here, Facebook's servers. *See, e.g.*, *Reno v. ACLU*, 521 U.S. 844, 849-51 (1997) ("The Internet is an international network of interconnected computers. …

arguing that Facebook is not a "protected computer" comes far too late. The failure to preserve this issue is itself a sufficient basis to deny the petition. *See Taylor v. Freeland & Kronz*, 503 U.S. 638, 646 (1992) ("Ordinarily, this Court does not decide questions not raised or resolved in the lower courts.") (internal brackets and citation omitted).

B. Even if Petitioners prevailed, the judgment would remain intact.

Review also should be denied because the question presented makes no difference to the outcome of the case. Even if the CFAA claim were vacated, the judgment would not be affected. That is because the decision below rests on an "adequate and independent" state-law ground. *Michigan v. Long*, 463 U.S. 1032, 1038 (1983); *see Rice v. Sioux City Mem'l Park Cemetery*, 349 U.S. 70, 76 (1955) (dismissing certiorari as improvidently granted on federal constitutional questions where "in any other case arising under similar circumstances … one in petitioner's position would be entitled to recover damages in a civil action based on a violation of [a state] statute"). In addition to violating the CFAA, Petitioners' conduct violated California Penal Code § 502, and the Court of Appeals affirmed on both grounds. Pet. App. 21a-22a. And the District Court has since entered final judgment against Petitioners on both grounds as well. *See* Judgment at 1, No. 5:08-cv-05780-LHK (N.D. Cal. May 2, 2017), ECF No. 437.

[T]he World Wide Web … allows users to search for and retrieve information stored in remote computers[.]").

As the Court of Appeals explained, California Penal Code § 502 "is 'different' than the CFAA." Pet. App. 21a (quoting *Christensen*, 801 F.3d at 994). So while "the analysis under both statutes is similar in the present case" insofar as Petitioners' conduct fit easily within both, Pet. App. 21a-22a, Petitioners' argument here would affect only the CFAA and not § 502. That is because § 502 does not contain the "without authorization" language that is the subject of the question presented. *Compare* 18 U.S.C. § 1030(a)(2) *with* Cal. Penal Code § 502(c). Moreover, § 502's prohibitions are broader than the CFAA's. *See Christensen*, 801 F.3d at 994.

Petitioners do not challenge the judgment against them under § 502; they seek "review of the question of CFAA interpretation only." Pet. 8. Even if they had raised § 502, the meaning of a state statute is not a certworthy question. Section 502 authorizes all the relief awarded to Facebook, *see* Cal. Penal Code § 502(e)(1), and indeed, on remand, the District Court has already rested damages and the injunction on *both* the CFAA and § 502. 2017 WL 1650608, at *12-16; *see also* Judgment at 1, No. 5:08-cv-05780-LHK (N.D. Cal. May 2, 2017), ECF No. 437.

Because the resolution of the question presented "is irrelevant to the ultimate outcome of the case," the petition should be denied. Steven M. Shapiro et al., Supreme Court Practice 249 (10th ed. 2013); *see also id.* at 506; *see, e.g.*, *The Monrosa v. Carbon Black Exp., Inc.*, 359 U.S. 180, 184 (1959) ("[T]his Court decides questions … in the context of meaningful litigation.").

C. These fatal vehicle flaws mean that there is no reason to hold the petition.

Not only do Petitioners' waiver, and the adequate and independent state-law ground for the judgment, make this an unusually poor vehicle for addressing the question presented, they also make it unnecessary to hold this petition for the petition pending in *Nosal II*. *See* Pet. 11, 25-26 (requesting, in the alternative, a hold for *Nosal II* and consolidation). Even if this Court were to grant review in *Nosal II* (despite the absence of a circuit conflict on the "without authorization" provision), and then reverse, Petitioners would not benefit from that ruling because the judgment still would stand based on § 502.

In addition, Petitioners' extreme conduct means that they would lose even under the theory of the CFAA advocated by Nosal. Nosal's cert petition contends that the statute forbids "[h]acking[,] [which] … is 'the circumvention of technological access barriers.'" 2017 WL 1832040, at *24; *see also id.* at *7. That is exactly what Petitioners did here: purposefully circumvent technological barriers erected to keep them out of Facebook's computers. *Supra* 5-6; Pet. App. 8a; *see, e.g.*, SER88 (describing Petitioners' technical "workaround solution 1").

III. The Petition Should Be Denied Because The Decision Below Is Correct.

Finally, even if the Court did sit to correct errors, there is none to correct here: The Court of Appeals correctly applied the CFAA to Petitioners' egregious misconduct.

As the Court of Appeals explained, "[t]he CFAA prohibits acts of computer trespass." Pet. App. 13a; *see* S. Rep. No. 99-432, at 9-10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2487. Thus, the "without authorization" provision of the CFAA imposes liability for accessing a protected computer that the defendant has been prohibited from accessing. 18 U.S.C. § 1030(a)(2). Just as an intruder who jumps a fence or defies a direct order to "keep out" would be liable for trespass, *see* Model Penal Code § 221.2(2)(a),(c), the same is true in the digital domain—by ignoring a command to "keep out" of a computer, the intruder violates the CFAA.

To that end, as the court correctly explained, a defendant's access to a computer is "without authorization" under the CFAA "when … permission to access a computer … has been revoked explicitly." Pet. App. 16a. Every judge to have considered this case has agreed that that is precisely what occurred here. "Facebook expressly rescinded [Power's] permission [to access Facebook] when Facebook issued its written cease and desist letter to Power" and "then imposed IP blocks in an effort to prevent Power's continued access." Pet. App. 17a. "Nevertheless, Power continued to access Facebook's data and computers without Facebook's permission." Pet. App. 18a. It "deliberately disregarded" Facebook's targeted direction to keep out, and "[i]t circumvented [Facebook's] IP barriers that further demonstrated that Facebook had rescinded permission for Power to access Facebook's computers." Pet. App. 19a-20a.

The court also correctly rejected Petitioners' argument that their access to Facebook's computers was

authorized by Power users who gave Power access to their Facebook accounts. As the court explained, Power was like an individual attempting to access a friend's safe deposit box with the friend's permission, but who was ejected by the bank upon entering with a shotgun. Pet. App. 19a. The gun-toting borrower could not re-enter the bank on the theory that his friend's approval trumped the bank's right to control access to its premises. Here, likewise, whatever right Power might initially have had to access Facebook's computers, "[p]ermission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter." Pet. App. 19a. Facebook undisputedly told Petitioners to keep out. Thus, because "[t]he record shows unequivocally that Power knew that it no longer had authorization to access Facebook's computer," Petitioners violated the CFAA when Power "continued to do so anyway." Pet. App. 18a.

For these reasons, Petitioners are simply wrong that "this case has immense implications … across the nation … [for] [h]undreds of millions" of Internet users. Pet. 9-10. On the contrary, it serves as a modest and appropriate reminder to willful digital intruders who do things like deploying "workaround solutions" to scale digital fences that their trespasses violate state and federal law. The decision below was correct and merits no further review.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be denied.

Respectfully submitted,

Eric A. Shumsky
Counsel of Record
ORRICK, HERRINGTON &
SUTCLIFFE LLP
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400
eshumsky@orrick.com

June 13, 2017