No. 16-

IN THE

Supreme Court of the United States

POWER VENTURES, INC. AND STEVEN VACHANI,

Petitioners,

v.

FACEBOOK, INC.,

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 LEE
Counsel of Record
ANDREW SCHWENK
HUGHES HUBBARD & REED LLP
One Battery Park Plaza
New York, New York 10004
(212) 837-6000
thomas.lee@hugheshubbard.com

Counsel for Petitioners

MARCH 9, 2017

271720

QUESTION PRESENTED

Whether an online company given consent by users of an online social networking service to access data shared or stored by the users on the service, but is prohibited access by the service, "intentionally accesses a computer without authorization . . . and thereby obtains information from [a] protected computer" in violation of 18 U.S.C. § 1030(a)(2)(c) of the Computer Fraud and Abuse Act of 1986.

RULE 29.6 STATEMENT

Petitioner Power Ventures, Inc., states that it has no parent corporation and that no publicly held company owns 10% or more of its stock.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

RULE 29.6 STATEMENT ii

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES vi

OPINIONS BELOW 1

JURISDICTION 1

STATUTORY PROVISIONS INVOLVED 1

STATEMENT OF THE CASE 3

THE PROCEEDINGS BELOW 6

REASONS FOR GRANTING THE PETITION 8

I. THE NINTH CIRCUIT'S INTERPRETATION OF A FEDERAL STATUTE IMPLICATING A QUESTION OF NATIONAL IMPORTANCE IS CLEARLY ERRONEOUS AND SHOULD BE REVERSED. 14

II. THIS COURT SHOULD ALTERNATIVELY GRANT AND CONSOLIDATE WITH THE PENDING PETITION IN *NOSAL* TO GIVE GUIDANCE TO THE CIRCUITS IN CONFLICT OVER THE PROPER INTERPRETATION OF "WITHOUT

AUTHORIZATION" IN 18 U.S.C. § 1030(A)(2)(C) 23

III. THIS CASE IS A FLAWLESS VEHICLE FOR DECIDING THE QUESTION PRESENTED, WHETHER BY GRANTING THIS PETITION OR BY CONSOLIDATION. 26

CONCLUSION 27

TABLE OF APPENDICES

Page

APPENDIX A — ORDER AND AMENDED OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, DATED DECEMBER 9, 2016 ..... 1a

APPENDIX B — ORDER OF THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION, FILED FEBRUARY 16, 2012 ..... 25a

APPENDIX C — ORDER OF THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION, FILED SEPTEMBER 25, 2013 ..... 57a

TABLE OF AUTHORITIES

Page(s)

Cases

Butera & Andrews v. IBM Corp., 465 F. Supp. 2d 104 (D.D.C. 2006) 25

Calence, LLC v. Dimension Data Holdings, 2007 WL 1549495 (W.D. Wash. 2007).....25

Doe v. Dartmouth-Hitchcock Med.l Ctr., 2001 WL 873063 (D.N.H. 2001).....25

EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (CA1 2001) 24

Exxon Mobil Corp v. Allapattah Servs. Inc., 545 U.S. 546 (2005).....13, 26

Gonzaga University v. Doe, 536 U.S. 273 (2002).....10

Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418 (CA7 2006) 24

Musacchio v. United States, 136 S. Ct. 709 (2016).....23

Nosal v. United States, 844 F.3d 1024 (CA9 2016).....*passim*

Owasso Ind. Sch. Dist. No. 1-011 v. Falvo, 534 U.S. 426 (2002).....10, 19, 20

SBM Site Servs., LLC. V. Garrett, 2012 WL 628619 (D. Colo. 2012) 25

United States v. John, 597 F.3d 263 (CA5 2010) 9, 24

United States v. Nosal, 676 F. 3d. 854 (CA9 2012) (*en banc*) 11, 24

United States v. Rodriguez, 628 F.3d 1258 (CA11 2010) 24

United States v. Teague, 646 F.3d 1119 (CA8 2011) 9, 24

United States v. Valle, 807 F.3d 508 (CA2 2015) 20, 24

WEC Carolina Energy Sols. v. Miller, 687 F.3d 199 (CA4 2012) 24

White v. Woodall, 134 S. Ct. 1697 (2014) 20

Constitutional Provisions

Fourth Amendment 4

Statutes and Rules

18 U.S.C. 14

18 U.S.C. § 1030 ..... *passim*

28 U.S.C. § 1254(1) 1

28 U.S.C. § 1291 1

28 U.S.C. § 1367 ..... 1, 13, 26

28 U.S.C. § 2254(d)—a 21

California Penal Code § 502 6

Fed. R. Civ. Pro. 20 26

Fed. R. Civ. Pro. 20 and 23 ..... 13, 26

20 U.S.C. § 1232(g) 19, 20

Sup. Ct. R. 10(c) 10, 14

Sup. Ct. R. 12(4) 11, 25

Treatises and Periodical Materials

Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (Dec. 13, 2016) 4, 21

Aarti Shahani, *The Man Who Stood Up to Facebook*, NPR (Oct. 13, 2016) 22

Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*" 78 N.Y.U. L. Rev. 1586 (2003) 15

Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016) 23

Orin Kerr, *9th Circuit: It's a Federal Crime to Visit a Website After Being Told Not to Visit It*, Washington Post online (July 12, 2016) 23

Mark Lemley, *Place and Cyberspace*, 91 Calif. L. Rev. 521, 523–26 (2003) 18

Josephine Wolff, *The Hacking Law That Can't Hack It*, Slate.com (Sept. 27, 2016) 22

Power Ventures, Inc., and Steven Vachani respectfully petition this Court to grant a writ of *certiorari* to review the final decision of the U.S. Court of Appeals for the Ninth Circuit entered in this action on December 9, 2016.

OPINIONS BELOW

The Ninth Circuit panel's opinion is reported at 844 F.3d 1058 and is reproduced in Appendix A. The opinion of the District Court granting summary judgment is reported at 844 F. Supp. 2d 1025 and is reproduced in Appendix B. The opinion of the District Court denying reconsideration is unreported and is reproduced in Appendix C.

JURISDICTION

The panel (Graber, Wardlaw, Murguia) entered judgment on July 12, 2016. Petitioners timely filed for panel rehearing and rehearing *en banc*. Rehearing was denied on December 9, 2016; the panel entered an amended final judgment the same day. This Court's jurisdiction is invoked under 28 U.S.C. § 1254(1).

This civil action is one arising under federal law, over which the district court had subject matter jurisdiction under 28 U.S.C. § 1331 and § 1367 (supplemental California law claim). The Ninth Circuit had appellate jurisdiction under 28 U.S.C. § 1291.

STATUTORY PROVISIONS INVOLVED

18 U.S.C. § 1030(a)(2)(c) provides:

"Whoever—intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains—information from any protected computer . . . shall be punished as provided in subsection (c) of this section."

18 U.S.C. § 1030(e) defines key terms including:

> As used in this section –
>
> (1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device
>
> (2) the term "protected computer" means a computer—
>
> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States

18 U.S.C. § 1030(g) provides that:

"Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or equitable relief."

STATEMENT OF THE CASE

Petitioners are Power Ventures, Inc., and Steven Vachani, the CEO of Power Ventures, Inc. (collectively "Power"). From 2006 to 2011, Power operated an online communications, personal data management, and social networking aggregator hosted at the website www.power.com. Power offered registered users the capacity to access multiple online social networks (*e.g.*, LinkedIn, Twitter), messaging services (*e.g.*, Microsoft messenger—MSN), and email accounts (*e.g.*, Google mail) through a single, integrated online interface consisting of a digital dashboard and browser. This online interface also featured popular add-in applications like a unified address book and mailbox integrating all of a user's contacts, emails, social network messages, and instant messages in one place. The interface additionally enabled Power users to move files between different accounts with a click-and-drag function, like a user moves folders on an Apple Computer desktop or in Microsoft Windows. Power attracted more than ten million dollars of investment as a startup from noted Silicon Valley venture capital firms like Draper Fisher Jurvetson (who also invested in Hotmail, Skype, and Tesla) and registered more than twenty million users at its peak.

One key feature Power offered was the ability to transfer document files, address book contacts, in-

stant messages, emails, and photos easily from one online service to another. Because it is so time-consuming for people to move countless bits of data manually from one service provider to a competitor, online companies like Power that facilitate moving a user's data when one provider's terms of use are too onerous are indispensable to lives lived increasingly on line. The right of a user to readily move, copy, and transmit his or her own personal data between online service providers and storage devices is called "data portability." Data portability is a burgeoning policy concern of our time, as underscored by a recent report issued by the European Commission's Directorate General Justice and Consumers. (*See* Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (Dec. 13, 2016), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf).[1]

Respondent Facebook, Inc., is a publicly listed Delaware corporation founded in 2004 and presently headquartered in California. Facebook operates the now-ubiquitous social networking website www.facebook.com. Facebook activates accounts for its users (now numbering nearly two billion worldwide) who register with a unique username and password and agree online to "terms of use." Facebook users send "friend" requests to other friends

[1] Data portability may be seen as the modern digital analogue of the old freedom to dispose freely of one's possessions, papers, and effects, protected from government intrusion by the Fourth Amendment.

with Facebook accounts and post photos, observations, status and event updates, and links to interesting websites and articles for their Facebook friends. Each Facebook user may set the audience to which he or she wishes to post or share data like pictures and updates (*e.g.*, friends only, the public at large), and also the types of friends' updates for which they would like to receive notifications.

In November 2008, Power, which then had over five million users, began offering any user who had a Facebook account access to it through Power's online portal by entering his or her Facebook username and password. When these were entered, the Power user could access the Facebook website through Power's browser, similar to a computer user clicking on his or her programs through Microsoft Windows. (Google, LinkedIn, Microsoft Messenger, Twitter, and Myspace were already accessible via the Power portal in the same way.) Power users were also invited, as part of a launch promotion, to invite their own Facebook friends to enroll on Power via "event" or "status" updates that caused Facebook-generated emails to be sent to Facebook friends whose notifications filters were set to allow them.

Facebook objected that Power's access of its service was unauthorized and sent Power a "cease and desist" letter on December 1, 2008. Power responded that it had the Power users' consent to access data they had stored on Facebook, including their friends' contact information. Facebook insisted, however, that Power join "Facebook Connect," its program for third-party companies or websites to enroll for the right to access user profiles and data on terms that Facebook dictated (*e.g.*, without an easy way to move data). Facebook also unsuccessfully at-

tempted to block Power's IP (internet protocol) address. Settlement negotiations took place during the month of December 2008 but ultimately failed, and Facebook sued. Facebook was the only online social network provider to take legal action against Power. Google, Twitter, Myspace, LinkedIn, Microsoft, and others allowed their users who had Power accounts to access and freely move their personal data among their respective services via Power.

THE PROCEEDINGS BELOW

On December 30, 2008, Facebook filed a civil action against Petitioners in the federal district court for the Northern District of California. Facebook's complaint, which was amended on January 13, 2009, pled claims under the Computer Fraud and Abuse Act of 1986 ("CFAA"), 18 U.S.C. § 1030(a)(2)(C), as well as the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") and California Penal Code Section 502, among others. The statutory provision at issue in this case, 18 U.S.C. § 1030(a)(2)(C), authorizes criminal and civil liability against "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer." The district court granted summary judgment in Facebook's favor on the CFAA, CAN-SPAM and California Penal Code claims. App. 25a. It awarded statutory damages of $3,031,350 under CAN-SPAM, permanent injunctive relief, and held Vachani personally liable for Power's conduct. App. 109a.

Petitioners appealed. In a judgment originally filed July 12, 2016, and amended on December 9,

2016, the Ninth Circuit panel (Graber, Wardlaw, Murguia) reversed the district court on CAN-SPAM and invalidated the damages award (holding that the relevant invitation messages were not misleading). App. 13a, 23a. The appellate court affirmed the district court's ruling on Petitioner Vachani's personal liability. App. 22a. Respondent Facebook did not seek rehearing on the CAN-SPAM reversal, and Petitioners do not challenge the panel's affirmance of personal liability before this Court.

The Ninth Circuit also reversed in part and affirmed in part on the CFAA and California Penal Code claims, and, accordingly, remanded for consideration of appropriate remedies on those claims. App. 23a. The court held that Petitioners had only violated the CFAA (and state law) after Power received the cease-and-desist letter on December 1, 2008 and did not end its marketing campaign via Facebook users. App. 23a-24a. The court reasoned that because the Power users with Facebook accounts had consented to allow Power to access their Facebook contacts, "it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA." App. 17a. The court asserted, however, that liability under the statute changed after Facebook sent the cease-and-desist letter, regardless of the users' consent that it had held to have constituted "authorization" under the statute before the letter. App. 17a. "The consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission." App. 19a. The court accordingly held that "after receiving written notification from Facebook on December 1, 2008, Power accessed Facebook's comput-

ers 'without authorization' within the meaning of the CFAA and is liable under that statute." App. 20a.

Petitioners filed for panel rehearing and rehearing *en banc*, which was denied on December 9, 2016; the panel issued an amended judgment the same day. App. 1a. Hence this Petition, which seeks this Court's review of the question of CFAA interpretation only.

REASONS FOR GRANTING THE PETITION

Petitioners respectfully submit that the Ninth Circuit's interpretation of 18 U.S.C. § 1030(a)(2)(C) is clearly erroneous and unprecedented. It is unreasonable to conclude as the lower court did that users' consent for Power to access their Facebook data (*i.e.*, friends' photos and contact information) constitutes "authorization" under the CFAA at one point but does not at another. What led the court below to this errant conclusion was the belief that Power was accessing "Facebook's computers" when it reached out to the Facebook friends of Power users with the users' consent and invited them to join Power. But Facebook is not a "protected computer" as the term is defined and used in the 1986 statute: rather, it is a very modern online social network service provider that encourages nearly two billion users worldwide to join it and share personal data with friends and family. In this context, the "authorization" the CFAA refers to is plainly that of the data owners and users. If Facebook wanted Power to stop accessing this data, it could have asked the Power users who owned the data to withdraw the consent they had given to Power, or else cancel the users' accounts.

The Ninth Circuit panel's interpretation of 18 U.S.C. § 1030(a)(2)(C) to ground a private cause of action for an online social network like Facebook as against another online company accessing user data with the user's consent is not only unreasonable, it is unprecedented. Facebook, the party asserting a private right of action under the statute, has no authorship or ownership of the information accessed. Indeed, Facebook's very business model is to entice people—"users"—to share personal information about themselves on its website. This is in stark contrast to prior CFAA private claimants—typically employers or former employers whose computers and databases were hacked for sensitive information. Facebook is not a bank whose account manager pilfered its client-account database to make fraudulent charges, *see United States v. John*, 597 F.3d 263 (CA5 2010), or a government agency whose records (including then President Barack Obama's student loan records) were surreptitiously searched by a government contractor, *see United States v. Teague*, 646 F.3d 1119 (CA8 2011). Rather, Facebook is a digital scrapbook that enables users to curate their own online personae for friends, family, or even the public at large, and the data that Petitioners accessed were these very artifacts of the users' personal lives. Of course, Facebook's proprietary algorithms and confidential business records are its *own* information, and Facebook could surely seek CFAA liability if Petitioners had accessed that information. But that is not this case.

The court below's unreasonable and unprecedented interpretation of the CFAA in this case has immense implications not only in California—home of Silicon Valley, the cradle of modern technological innovation—but also across the nation. Hundreds of

millions (billions, worldwide) of people use Facebook and other social networking and "cloud" storage service providers like LinkedIn, Twitter, Google Docs, Skype, Dropbox, and Microsoft OneDrive to connect with friends and business associates; to store and share cherished photos, stories, and documents; and to post their observations on life's big and small questions. Facebook and other data controllers already have outsized influence over individual users as gatekeepers. Judicial decisions like the one below will aggrandize their power even more by handing them veto power over online entrepreneurs like Petitioners who seek to enable data portability for users.

Additionally, the lower court's interpretation is acutely pernicious because 18 U.S.C. § 1030(a)(2)(C) also grounds criminal liability under the CFAA of up to five years, *ibid.* § 1030(c)(2)(B). If Congress today decides that Petitioners' actions warrant such drastic criminal and civil liability, it can enact a new statute; the Ninth Circuit's creation of such liability by judicial fiat in overreading a 1986 statute is not the right way.

This Court has previously granted *certiorari* when a lower court erroneously interpreted a federal statute on an important national issue, even in the absence of a circuit split. *See, e.g.*, *Owasso Ind. Sch. Dist. No. 1-011 v. Falvo*, 534 U.S. 426 (2002); *cf.* Sup. Ct. R. 10(c) ("an important question of federal law that has not been, but should be, settled by this Court"). *Owasso* is particularly instructive because the Court granted and reversed the lower court's interpretation of a federal statute that it later held in the same Term did not even afford a private right of action. *See Gonzaga University v. Doe*, 536 U.S. 273 (2002).

With special regard to this case, the overwhelming presence of technology companies in California and Washington makes it highly unlikely that a split among the circuits on this precise issue will ripen.[2] Ninth Circuit precedents are often *de facto* the law of the land on cutting-edge social media issues owing to the circuit's hegemony over Silicon Valley.

Alternatively, if this Court were not inclined to grant this Petition as presenting a question of national importance on which it should rule, the Court could hold the Petition over and consolidate it with the soon-to-be pending petition in another Ninth Circuit case, *Nosal v. United States ("Nosal II")*, 844 F.3d 1024 (CA9 2016),[3] for which an extension was filed and granted by this Court until April 7, 2017 (No. 16A840). *Cf.* Sup. Ct. R. 12(4). *Nosal II* is a criminal case involving a charge under 18 U.S.C. § 1030(a)(4), a liability provision of the CFAA with the same "without authorization" language as § 1030(a)(2)(C). It applies to any person who "knowingly and with intent to defraud, accesses a protected

[2] In addition to Facebook, many of the most popular online social media providers like YouTube, Instagram, and Twitter, are based in California. Some of the largest cloud service providers are also in the Ninth Circuit's geographic jurisdiction: Apple, Dropbox, and Google Drive have headquarters in California, and Microsoft and Amazon are based in Washington state.

[3] An earlier case involved some of Nosal's colleagues at Korn/Ferry who downloaded confidential information from their employer in violation of company policies before jumping ship with Nosal to launch a competitive firm. *See United States v. Nosal ("Nosal I")*, 676 F. 3d. 854 (CA9 2012) (*en banc*).

computer without authorization … and by means of such conduct furthers the intended fraud and obtains anything of value." *Ibid.* § 1030(a)(4). Nosal, the defendant, accessed the confidential database of a former employer (the executive recruitment firm Korn/Ferry) by using the password of his former executive assistant who stayed on at Korn/Ferry at his request. The jury convicted Nosal of conspiracy to violate the "without authorization" provision of the CFAA under 18 U.S.C. § 1030(a)(4).

Nosal II and this case present the same issue of whether a third party (here, Petitioners; there, Nosal) who is denied authorization to access data (here, friends' contact information on Facebook; there, Korn/Ferry's confidential database) may do so with the consent of an authorized user (here, Power users with Facebook accounts; there, Nosal's ex-executive assistant). As the dissenting judge pointed out, because *Nosal II* involved a person (the assistant) who had authorization as a continuing Korn/Ferry employee to access its database but not for the "use" of enabling Nosal's conspiracy, it could be framed as implicating a 5-3 split among the circuits over whether "without authorization or exceeds authorized access" in the CFAA covers an impermissible use by an authorized person. *See Nosal II*, 844 F.3d. at 1048, 1048-49 (Reinhardt, dissenting).

Of course, there are also important differences between the Petitioners' novel case involving an online social network and *Nosal II*, which is a traditional case involving access to an employer's or former employer's computers or database. But in light of the similarities, the Court could hold over this Petition, grant the two petitions together and consolidate for argument, and issue a decision that will be

highly instructive to lower courts by distinguishing between the two factual contexts as it deems appropriate. *See, e.g., Exxon Mobil Corp v. Allapattah Servs. Inc.*, 545 U.S. 546 (2005) (simultaneously disposing of petitions from CA1 and CA11 regarding the application of the supplemental jurisdiction statute, 28 U.S.C. § 1367(a), to joinder of plaintiffs in diversity suits under Fed. R. Civ. Pro. 20 and 23, respectively).

In sum, this Court should grant *certiorari* in this case. The lower court's interpretation of the CFAA to extend liability to Petitioners as against a social networking website like Facebook is a question of national importance and is clearly erroneous and unprecedented. If uncorrected, the lower court's ruling will affect hundreds of millions of American (and a couple billion non-American) users of Facebook and other social network and cloud providers. Alternatively, this Court could hold over this petition and consolidate with the petition in *Nosal II*, which implicates a deep split regarding the scope of what "without authorization" means in the CFAA. Regardless of what this Court chooses to do, this case presents a flawless vehicle to decide the Question Presented.[4]

[4] Indeed, this case may arguably be a better vehicle than *Nosal II* because the defendant in that criminal case was also convicted of two counts of trade secret theft in violation of the Economic Espionage Act, 18 U.S.C. §§ 1832 (a). *See Nosal II*, 844 F.3d., at 1041.

I. THE NINTH CIRCUIT'S INTERPRETATION OF A FEDERAL STATUTE IMPLICATING A QUESTION OF NATIONAL IMPORTANCE IS CLEARLY ERRONEOUS AND SHOULD BE REVERSED.

The Ninth Circuit's unreasonable and unprecedented interpretation of 18 U.S.C. § 1030(a)(2)(C) of the CFAA to apply to an online social network service provider seeking to bar another online company acting with users' consent from accessing user data is clearly erroneous and risks mischief on hundreds of millions of internet users. Rule 10(c) of this Court explicitly provides that a lower court's decision of an "important question of federal law that has not been, but should be, settled by this Court" is a factor to be considered in granting *certiorari*. And, as elaborated below, this Court sometimes acts to correct a clearly erroneous interpretation of an important statute by a lower court, even in the absence of a circuit split, to prevent ripple effects or dire national consequences.

The CFAA, 18 U.S.C. § 1030, was initially enacted as part of the Comprehensive Crime Control Act of 1984. *See* Pub. L. No. 98-473, 98 Stat. 1837 (1984). The 1984 statute was substantially revised in 1986, with minor subsequent revisions. The CFAA has both criminal and civil liability provisions, with criminal sentences ranging from twenty years, *e.g.*,18 U.S.C. § 1030(c)(1)(B), to one year, *e.g.*, *ibid.* § 1030(c)(2). The statute's provision for a private right of action states that: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or equitable relief." *Ibid.* § 1030(g). Facebook brought its CFAA claim against Petitioners pursuant to this provision.

The specific provision of the CFAA that Facebook alleged Petitioners had violated was 18 U.S.C. § 1030(a)(2)(C), which provides: "Whoever—intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains—information from any protected computer . . . shall be punished as provided in subsection (c) of this section."[5]

18 U.S.C. § 1030(e)(1) defines "computer" to include not only "data processing devices" but also "any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(2) then defines a "protected computer" to mean a "computer":

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States

[5] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*" 78 N.Y.U. L. Rev. 1586 (2003).

A violation of this provision can result in a criminal sentence of up to five years. *Ibid.* § 1030(c)(2)(B).

Thus, Facebook's CFAA claim, which the Ninth Circuit adopted, was that Petitioners had accessed its website and servers—a "protected computer" under CFAA—and that it did so "without authorization" since Facebook had explicitly told them to desist. On Facebook's view, the authorization of the individual users whose Facebook data Petitioners accessed was irrelevant after Facebook had instructed Petitioners to stop: their authorization was no longer the "authorization" the CFAA required. Specifically, the court reasoned:

> Because Power had at least arguable permission to access Facebook's computers [from Power users with Facebook accounts], it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA. But Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power on December 1, 2008.

App. 17a.

The lower court's holding is unprecedented and unreasonable. Whatever confusion there was about what constituted "without authorization" among the circuits, *see infra* Part II, no court had held until now that the consent of the individual persons who generated, owned, stored, or shared the relevant data or information was irrelevant to the

"authorization" the statute required.[6] To be sure, if the controller or custodian of the data were a bank or a U.S. government agency, then the argument might seem at least superficially plausible. But in this case, Facebook is an online social network provider, with which people voluntarily *share* personal data and information precisely to disseminate it, not to lock it away in a vault or to submit sensitive information to apply for a government job or benefits. Nor is Facebook claiming that its own proprietary algorithms and business records were the information that Petitioners mined. At the very least, the users' authorization has to matter for something: the Ninth Circuit's decision renders it entirely irrelevant after Facebook denied access to Petitioners and gives Facebook the unitary veto power that it wanted with respect to its competitors like Power.

The obvious truth is that the court below was wrong to conclude the statute is meant to afford a private right of action for an online company with consent from its users to access their personal information shared with another online social networking service when the other service tells the company to stop.[7] In such a case, the company is not "intention-

---

[6] Facebook did not argue below that Petitioners exceeded the users' authorization of access to their data. In other words, there is no dispute that Petitioners acted within the consent provided by users with respect to the users' Facebook accounts.

[7] The court below analogized Petitioners' conduct to a person given permission to access jewelry in a friend's safe deposit box who walks into the bank with a shotgun to whom the bank refuses entry. *See* App. 19a. The analogy is inapt and misleading because Facebook's mission is not to secure the users' "property" (*e.g.*, photos, friends'

Footnote continued

ally access[ing] a computer without authorization or exceed[ing] authorized access" and "thereby obtain[ing] information—from any protected computer" in violation of 18 U.S.C. § 1030(a)(2)(C). It is unsurprising that no other circuit court has reached this conclusion, not only because it is an unreasonable construction of the statutory text, but also because this type of issue about the CFAA is likely to rise most commonly if not exclusively in California and portions of the West Coast within the Ninth Circuit's jurisdiction, where almost all U.S. social network and cloud computing service providers are headquartered.

Furthermore, although the lower court repeatedly referred to Petitioner's access to "Facebook's computers," *e.g.*, App. 5a, 14a, it is debatable whether Facebook and its servers are a "protected computer" for purposes of 18 U.S.C. § 1030(a)(2)(C). The

---

Footnote continued from previous page

contact information) in an online vault, but rather to share it with friends and family and sometimes the public at large. Furthermore, Power did not wield a figurative gun: its user-authorized entry into users' Facebook data was not even arguably coercive or dangerous, as evidenced by the fact that every other online service in Facebook's position (like Google and Microsoft) permitted it. As Judge Wardlaw noted during the oral argument below, physical property analogies are often unhelpful in the online context. *Facebook Inc. v. Power Ventures, Inc., et. al*, Oral Arg., 40:48-41:22, No. 13-17102 (CA9 Dec. 9, 2015), *available at* https://www.youtube.com/watch?v=4QUai3OmkdA; *see also* Mark Lemley, *Place and Cyberspace*, 91 Calif. L. Rev. 521, 523–26 (2003) ("[E]ven a moment's reflection will reveal that the analogy between the Internet and a physical place is not particularly strong.").

statute defines a "protected computer" as a computer or "data storage facility or communications facility" that performs a mission perceived as essential to protect against fraud in the 1980s, such as a computer "exclusively for the use of a financial institution or the United States Government," *see ibid.* §§ 1030(e)(1), 1030(e)(2)(A). True, 18 U.S.C. §1030(e)(2)(B)'s catchall reference to a computer "used in or affecting interstate or foreign commerce or communication" is broadly worded. But a social networking website that users access, primarily to stay in touch with friends and family, is far beyond the government mainframes, bank electronic accounts, and electronic trading exchanges that Congress and President Ronald Reagan envisioned when they passed the CFAA. This kind of vital regulation of the new economy should be ratified by a new Congress, not a Congress three decades ago that could not have even imagined a Facebook or a Google.

The Court has previously granted *certiorari* to correct a clear error in interpreting a federal statute likely to have broad repercussions if uncorrected, even in the absence of a circuit split. For example, in *Owasso Independent School District No. 1-011 v. Falvo*, 534 U.S. 426, there was no conflict among the circuits regarding the relevant question of statutory interpretation. Nevertheless, the Court unanimously reversed the Tenth Circuit's interpretation of the Federal Educational Records and Privacy Act of 1974 ("FERPA"), 20 U.S.C. § 1232(g), to reach student-on-student peer grading and reporting of test scores. The Court reasoned that this interpretation "would impose substantial burdens on teachers across the country." *Ibid.* at 435. "Indeed, the logical consequences of respondent's view are all but unbounded." *Ibid.*

Like the Tenth Circuit's erroneous decision in *Owasso* implicating educational privacy records, the Ninth Circuit's clearly erroneous decision regarding data privacy promises to have substantial adverse ripple effects if not corrected. Its interpretation "would impose substantial burdens," not on teachers, but rather on internet users "across the country" locked into their current social network service or cloud storage providers. Furthermore, internet startups like Petitioners would be constrained from offering services like data aggregation and relocation to enhance user freedom and online diversity. Indeed, the Ninth Circuit's error here is even more egregious because a violation of CFAA, unlike FERPA, can ground criminal liability of up to five years in this case, 18 U.S.C. § 1030(c)(2)(B), as well as private liability. As such, there are additional rule of lenity concerns for reversing the lower court's decision. *Cf. United States v. Valle*, 807 F.3d 508 (CA2 2015) (applying the rule of lenity to construe "authorized access" in CFAA narrowly).

Similarly, in *White v. Woodall*, 134 S. Ct. 1697 (2014), the Court granted *certiorari* and reversed a judgment from the U.S. Court of Appeals for the Sixth Circuit affirming the grant of a habeas petition because the Court determined the lower court had misinterpreted the federal habeas statute. Both the federal district and appellate courts held that the state court's refusal to issue a "no adverse inference from failure to testify" instruction to a jury in a death penalty sentencing hearing violated the defendant's due process rights. *Ibid.* at 1701. This Court explained that the federal habeas statute's "unreasonable application" language is only met when the state court's decision is "objectively unreasonable," *ibid.* at 1702, which the Court held was not

the case. Although the Sixth Circuit's application of the statute did not create a circuit split, this Court nonetheless reversed because the circuit "disregarded the limitations of 28 U.S.C. § 2254(d)—a provision of law that some federal judges find too confining, but that all federal judges must obey." *Ibid* at 1701.

The Ninth Circuit's erroneous decision has immense implications for users of online social media and cloud storage. As users create more online data, data portability among different service providers seeking to keep existing users locked in becomes a growing concern. New European Commission guidelines dictate that users must have "the right to transmit personal data from one data controller to another data controller *without hindrance*." (*See* Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, at 4 (Dec. 13, 2016) (emphasis added) (internal quotation marks omitted), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf). This ensures that users "can obtain and reuse, but also [] transmit the data they have provided to another service provider." *Ibid.* The Ninth Circuit has created civil and criminal liability for a company seeking to assist users—with their consent—fully to use, enjoy, and move their own data online as they choose.

By way of an example, consider a person who pays a monthly subscription to a hypothetical company called PhotoBook, an online cloud storage service, to organize and access family photos from any computer. Over years of creating and saving photos, the user amasses thousands of photos stored in PhotoBook. Then, because of financial need or practical considerations, the user wishes to transfer those

photos to another service or to a personal computer. The user may seek to hire a company such as Power—a digital mover—to transfer the photos because of a lack of time or technological knowhow. But under the Ninth Circuit's interpretation of the CFAA, PhotoBook may unilaterally deny the moving service access to the user's photos, even with the user's explicit consent. PhotoBook not only gains a power to lock-in its users (subject to increasingly onerous terms), it stifles innovation in the internet economy, all based on a clever but erroneous spin on a 1986 statute.

The importance of the Question Presented is underscored by the attention paid to it. The Electronic Frontier Foundation ("EFF"), a prominent internet rights non-profit organization, filed two amicus briefs at different stages of the district court proceedings. In the Ninth Circuit, the EFF again filed two amicus briefs. The latter of which, joined by the national American Civil Liberties Union ("ACLU") and the ACLU of Northern California, explained that the Ninth Circuit's decision risks creating liability for individual internet users, researchers, and journalists. *See* Amicus Brief of EFF et al., No. 13-17154, Dkt. 89 (CA9 Aug. 19, 2016), *available at* https://www.eff.org/document/facebook-v-power-ventures-eff-aclu-amicus-brief. The case and the Petitioners have been the subject of articles in major news organs like NPR, (Aarti Shahani, *The Man Who Stood Up to Facebook*, NPR (Oct. 13, 2016) *available at* https://goo.gl/UAXhVk), Slate, (Josephine Wolff, *The Hacking Law That Can't Hack It*, Slate.com (Sept. 27, 2016), *available at*

https://goo.gl/iXnxey), and by Professor Orin Kerr,[8] in the Washington Post online, (Orin Kerr, *9th Circuit: It's a Federal Crime to Visit a Website After Being Told Not to Visit It*, Washington Post online (July 12, 2016) *available at* https://goo.gl/rdc2Cu).

II. THIS COURT SHOULD ALTERNATIVELY GRANT AND CONSOLIDATE WITH THE PENDING PETITION IN *NOSAL* TO GIVE GUIDANCE TO THE CIRCUITS IN CONFLICT OVER THE PROPER INTERPRETATION OF "WITHOUT AUTHORIZATION" IN 18 U.S.C. § 1030(A)(2)(C)

The meaning of the words "without authorization or exceeds authorized access" in 18 U.S.C. § 1030(a)(2)(C) has sparked conflict among the lower courts and is ripe for guidance from this Court.[9] 18 U.S.C. § 1030(e)(6) defines "exceed authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter."

---

[8] Professor Kerr, a national expert on computer crime law issues, was joint counsel for Petitioners at the court below. *See also* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016).

[9] Last term, in *Musacchio v. United States*, 136 S. Ct. 709 (2016), this Court unanimously held that an erroneous jury instruction on 18 U.S.C. § 1030(a)(2)(C)—that the defendant had to have acted "without authorization *and* exceed authorized access"—did not offend due process, since it presented a tougher standard for conviction than the correct reading of the statute with a disjunctive "or". That decision, accordingly, did not address circuit conflict about the meaning of "without authorization" and "exceeded authorized access."

Because most CFAA cases arise in the context of an employee or ex-employee accessing an employer's computers or database, this definition would appear to foreclose civil and criminal liability in cases where the employee was entitled to access but did so for an unauthorized use. Three circuits have hewed to this narrow definition. *See United States v. Valle,* 807 F.3d 508 (CA2 2015) (New York City policeman not criminally liable for accessing criminal database for personal reasons); *WEC Carolina Energy Sols. v. Miller*, 687 F.3d 199 (CA4 2012); *United States v. Nosal* ("*Nosal I*"), 676 F.3d 854 (CA9 2012).

On the other hand, five circuits have held that employees or ex-employees who access computers to obtain data they have a right to access, but do so for an improper use or do so in violation of the employer's policies, violate the CFAA. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (CA1 2001) (former employee violated CFAA by using "scraper" technology to get price data from a former employer's public website); *United States v. John*, 597 F.3d 263 (CA5 2010); *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418 (CA7 2006); *United States v. Teague*, 646 F.3d 1119 (CA8 2011); *United States v. Rodriguez*, 628 F.3d 1258 (CA11 2010). This Court has not resolved this 5-3 circuit split between the narrow "no liability for improper use" view and broad "liability for improper use" views of the CFAA.

As described in detail above, the soon-to-be pending petition for *certiorari* in *Nosal II* can be framed as implicating this deep split, and, also, the same issue as this case when framed at a higher level of abstraction. This could be done, for example, by tweaking the Question Presented by this Petition to read: "Whether a third party given consent by a user

to access data on a 'protected computer' acts 'without authorization' in violation of 18 U.S.C. § 1030(a) of the Computer Fraud and Abuse Act of 1986."

Without speaking to the merits of *Nosal II*, Petitioners assert that this case independently warrants grant of *certiorari* because it presents a unique question of national importance about the applicability of the CFAA to online social media companies. This question has ramifications for hundreds of millions, if not billions, of internet users and burgeoning concerns about data portability. In this respect, it differs from the traditional CFAA cases in the lower courts involving access to an employer's or former employer's computers or database, which are usually fact-bound to the specifics of each case of less universal concern.

But if this Court were not inclined to grant this Petition, then Petitioners respectfully request that it hold the Petition over and consolidate it with the soon-to-be pending petition in *Nosal II*, for which an extension was filed and granted by this Court until April 7, 2017. *See Nosal v. U.S.*, No. 16A840 (Feb. 24, 2017); *Cf.* Sup. Ct. R. 12(4). On prior occasions, this Court has done so, to the profit and guidance of lower courts conflicted in similar but not identical applications of an enigmatic statute.[10] For instance,

[10] In fact, there is yet another burgeoning split among the lower courts regarding 18 U.S.C. § 1030(a)(2)(C). One federal district court has held that the new employer of a person who hacks into the computer of a former employer may also be liable under the CFAA. *See SBM Site Servs., LLC. V. Garrett*, 2012 WL 628619 (D. Colo. 2012). Three district courts have held that a new employer under these circumstances cannot be vicariously liable. *See Calence, LLC v. Dimen-*

Footnote continued

in *Exxon Mobil Corp v. Allapattah Servs. Inc.*, 545 U.S. 546 (2005), this Court issued a single opinion construing the supplemental jurisdiction statute, 28 U.S.C. § 1367, with respect to two different factual contexts involving the statute's application to complete diversity and amount-in-controversy requirements for class actions (Fed. R. Civ. Pro. 23) and simple joinder of plaintiffs (Fed. R. Civ. Pro. 20). The Court's decision in *Exxon Mobil* supplied welcome repose to lower courts and lawyers mired for decades in confusion about the statute's meaning. So, too, in the present case, any guidance from this Court on the application of the CFAA's "without authorization" language to different factual contexts such as in this case and *Nosal II* would be illuminating and welcome.

III. THIS CASE IS A FLAWLESS VEHICLE FOR DECIDING THE QUESTION PRESENTED, WHETHER BY GRANTING THIS PETITION OR BY CONSOLIDATION.

The facts relevant to this petition as articulated by the court below are undisputed and sharply frame the crucial question of statutory interpretation raised. Accordingly, the Court will be able to reach and decide the Question Presented without the risk

---

Footnote continued from previous page

sion Data Holdings, 2007 WL 1549495 (W.D. Wash. 2007); *Butera & Andrews v. IBM Corp.*, 465 F. Supp. 2d 104 (D.D.C. 2006); *Doe v. Dartmouth-Hitchcock Med.l Ctr.*, 2001 WL 873063 (D.N.H. 2001).

of an intervening disputed fact or procedural default. The challenged part of the decision below rests entirely on the Ninth Circuit's errant interpretation of 18 U.S.C. § 1030(a)(2)(C). The issue presented here was fully briefed and considered by the Court of Appeals in a reasoned opinion, and so this Court has the benefit of the Court of Appeals' views on the subject. The Question Presented by this Petition has generated national attention and implicates the future of data privacy and portability. It is ripe for a decision by this Court. Given that the lower court's decision on a question of national importance was clearly erroneous and unprecedented, this Court could summarily grant, reverse, and remand. But if the Court is disinclined to do so, Petitioners stand ready to brief and argue the merits of the case before the Court at its pleasure.

CONCLUSION

For the reasons set forth above, this Petition for a Writ of Certiorari should be granted.

Respectfully submitted,

Thomas Lee
Counsel of Record
Hughes Hubbard & Reed LLP
One Battery Park Plaza
New York, New York 10004
(212) 837-6000