NOS. 14-10037; 14-10275

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
PLAINTIFF-APPELLEE,

v.

DAVID NOSAL,
DEFENDANT-APPELLANT.

On Appeal From The United States District Court
for the Northern District of California
Case No. 3:08-cr-00237-EMC-1
Hon. Edward M. Chen, District Court Judge

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA IN SUPPORT OF DEFENDANT-APPELLANT'S PETITION FOR REHEARING *EN BANC*

Jamie L. Williams
Cindy Cohn
Andrew Crocker
Stephanie Lacambra
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
jamie@eff.org

Esha Bhandari
Rachel Goodman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2654

Counsel for Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Northern California
(Additional counsel on signature page)

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Northern California state that they do not have parent corporations, and that no publicly held corporation owns 10 percent or more of their stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Legislative Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect consumer interests, innovation, and free expression in the digital world. With over 26,000 active donors and dues-paying members, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF's interest in this case is in the principled and fair application of the Computer Fraud and Abuse Act ("CFAA") to online activities and systems, especially as it impacts Internet users, innovators, and security researchers. EFF has filed three *amicus* briefs in this case at the appellate level, including two when the case was previously before this Court.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with approximately 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU of Northern California is the geographic affiliate of the National ACLU that encompasses the Northern District of California, out of which this case arises. Founded in 1920, the ACLU has vigorously defended the First Amendment for nearly a century in state and federal courts across the

[1] Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except for undersigned counsel, has authored the brief in whole or in part, or contributed money towards the preparation of this brief. Both parties consent to this brief's filing.

country, including protecting valuable online research, journalism, and testing. It has also been at the forefront of efforts to ensure that the Internet remains a free and open forum for the exchange of information and ideas. The ACLU serves as counsel in a case challenging the constitutionality of a portion of the CFAA separate from the one at issue in this case, but raising related concerns. *See Sandvig v. Lynch*, No. 1:16-cv-01368-JDB (D.D.C. filed Jun. 29, 2016).

INTRODUCTION

The Ninth Circuit's two most recent decisions interpreting the meaning of access "without authorization" under the CFAA—the panel's decision in this case and the panel decision in *Facebook, Inc. v. Power Ventures, Inc*., No. 13-17102, 2016 WL 3741956 (9th Cir. July 12, 2016)—are inconsistent with Ninth Circuit precedent, are inconsistent with each other, and render the CFAA unconstitutionally vague. The two decisions, individually and together, lose sight of the CFAA's intended purpose of prohibiting breaking into computers in order to access or alter information, misconstruing this Court's prior decisions in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), and *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) ("*Nosal I*"). The majority's reasoning in this case, in particular—through subjecting to prosecution anyone who accesses someone else's online account without permission from the computer owner—criminalizes password sharing and thereby subjects millions of

innocent Americans to potential prosecution on the basis of routine online behavior. By failing to provide fair notice of what is unlawful, the panels' interpretations of the CFAA will also chill important computer security research and investigations of discriminatory practices online.

This Court should grant rehearing *en banc* in both cases to resolve the inconsistencies between the two panels' holdings and this Court's precedent, and to ensure that the CFAA is not transformed into a "sweeping [and unconstitutionally vague] Internet-policing mandate." *Id.* at 858.

ARGUMENT

En banc review is appropriate if "(1) necessary to secure or maintain uniformity of the court's decisions" or "(2) the proceeding involves a question of exceptional importance." Fed. R. App. P. 35. Both grounds are satisfied here.

I. THE COURT SHOULD GRANT *EN BANC* REVIEW TO SECURE UNIFORMITY OF THE COURT'S DECISIONS.

A. The Panel's Decision Conflicts With *Brekka* and *Nosal I*.

Ninth Circuit precedent in *Brekka* and *Nosal I* both prevented CFAA liability from reaching beyond its intended purpose—making it unlawful to break into computers in order to access or alter information. The panel's decision here conflicts with this precedent because it fails to assess whether the defendant broke into any computer. Instead, it finds that third parties who access a computer with authorization from someone with valid access credentials, but without

authorization from the computer owner, are violating the CFAA.

The CFAA makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C).[2] The statute defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter[.]" 18 U.S.C. § 1030(e)(6). But it does not define either "authorization" or "without authorization." A "protected computer" has been interpreted to include any computer connected to the Internet. *Nosal I*, 676 F.3d at 859. As Judge Reinhardt noted in his dissent, the CFAA does not indicate who must provide the requisite authorization to access a computer or website. *United States v. Nosal*, No. 14-10037, 2016 WL 3608752, at *22 (9th Cir. July 5, 2016) ("*Nosal II*") (Reinhardt, J., dissenting).

The statute's undefined and vague language has caused much confusion in the lower courts and has given rise to a circuit split over whether violations of computer use agreements (often called "terms of service" or "terms of use") trigger

[2] The specific CFAA section Nosal was charged with was 18 U.S.C. § 1030(a)(4), which requires an intent to defraud, but the interpretation of "without authorization" must apply equally to the statute's various subsections "pursuant to the 'standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning.'" *Nosal I*, 676 F.3d at 859 (quoting *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)).

CFAA liability. This Court, along with the Fourth and Second Circuits,[3] has found that they cannot, holding that the CFAA must be limited to the purpose intended by Congress—outlawing breaking into computers to obtain or alter information.

First, in *Brekka*, this Court held that the CFAA "was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives[.]'" 581 F.3d at 1130–31 (quoting H.R. Rep. 98–894, at 9, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984). *Brekka* rejected the theory that "a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer," such as violating an employer's computer use policies. *Id.* at 1135. Instead, the Court held that the CFAA's prohibition against accessing a protected computer "without

[3] *See WEC Carolina Energy v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *United States v. Valle*, 807 F.3d 508, 527–28 (2nd Cir. 2015). Four circuits have broadly interpreted "without authorization" and "exceeds authorized access" to include acts of disloyal employees who misuse their access to corporate information. *See, e.g., United States v. John*, 597 F.3d 263, 272–73 (5th Cir. 2010); *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582–84 (1st Cir. 2001); *United States v. Rodriguez*, 628 F.3d 1258, 1263–64 (11th Cir. 2010). But these courts' broad interpretation of the CFAA has been explicitly rejected by this circuit's decisions. *See Nosal I*, 676 F.3d at 862–63 (rejecting *John*, *Citrin*, and *Rodriguez* for failing to "construe ambiguous criminal statutes narrowly so as to avoid 'making criminal law in Congress's stead'") (quotation omitted); *Brekka*, 581 F.3d at 1135 ("[W]e decline to adopt the interpretation of 'without authorization' suggested by *Citrin*.").

authorization" covers individuals who have no rights to the computer system, while the prohibition against "exceed[ing] authorized access" is aimed at insiders who "ha[ve] permission to access the computer, but access[] information on the computer that the[y] [are] not entitled to access." *Id.* at 1133.

Three years later in *Nosal I*, this Court, *en banc*, reiterated that Congress's purpose in enacting the CFAA was to target "hackers" who "'intentionally trespass[ed] into someone else's computer files'" and obtained information, including information on "'how to break into that computer system.'" *Nosal I*, 676 F.3d at 858 (quoting S. Rep. No. 99–432, at 9, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487 (September 3, 1986)). The Court rejected the argument that the bounds of an individual's "authorized access" turned on use restrictions imposed by an employer, an interpretation of the statute that would have broadly criminalized violations of computer use policies and "transform[ed] the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id*. at 857. *Nosal* recognized that by targeting "hacking," Congress intended to target those who break into computers in order to access or alter information, not those who violate computer use restrictions. *Id.* at 863. In this way, Congress sought to address a narrow problem, not create "a sweeping Internet-policing mandate." *Id*. at 858.[4]

[4] Both the Fourth and Second Circuits, the two most recent federal circuit courts to interpret the CFAA's language, adopted this same narrow interpretation. *See WEC Carolina*, 687 F.3d at 207 (noting an "unwilling[ness] to contravene Congress's

The majority failed to assess whether David Nosal's associate, Becky Christian, broke into a computer when she accessed the Korn/Ferry company database at issue.[5] Indeed, she did not. Christian accessed the database with the legitimate login credentials of a current Korn/Ferry employee, "FH," who had voluntarily and consensually provided access to Christian and Nosal. Their own login credentials had been revoked when they left Korn/Ferry. To be sure, the act of sharing credentials violated company *policy*—which stated that anyone accessing any Korn/Ferry system or information needed "specific authority"—but it did not entail circumventing the ordinary technological means contemplated for accessing the system. In short, Christian's use of FH's credentials simply did not entail any kind of technological break-in.

The majority nevertheless held that these actions constituted a violation of the CFAA. The majority concluded that only the company—and not an employee with company-authorized login credentials—could provide an individual with "authorization" to access the computer: "Implicit in the definition of authorization

---

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"); *Valle*, 807 F.3d at 526 (a narrow interpretation was "consistent with the statute's principal purpose of addressing the problem of hacking, i.e., trespass into computer systems or data").

[5] Nosal was charged under the CFAA as an accomplice, liable for the actions of Christian and another former Korn/Ferry employee. *See Nosal II*, 2016 WL 3608752, at *2, n.1.

is the notion that someone, including an entity, can grant or revoke that permission. Here, that entity was [the computer owner,] and FH had no mantle or authority to give permission to former employees whose access had been categorically revoked by the company." *Nosal II*, 2016 WL 3608752, at *8. Thus, the majority held that the authorization granted by FH simply did not count for purposes of the CFAA. "Nosal had 'no possible source of authorization' since the company revoked his authorization and, while FH might have been wrangled into giving out her password, she and the others knew that she had no authority to control system access." *Id.* at *8, n.7

In short, because Nosal and his associates did not have permission directly from Korn/Ferry, their access to the Korn/Ferry database was without "authorization" under the CFAA and they were committing a crime. This holding rests *not* on whether Nosal and his associates broke into any computer, but on the fact that they lacked permission from the computer owner. As Judge Reinhardt recognized in his dissent, the test applied by the majority—whether authorization came directly from the computer owner—not only "loses sight of the [CFAA's] anti-hacking purpose" but it also "threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens." *Nosal II*, 2016 WL 3608752, at *19 (Reinhardt, J., dissenting). Indeed, there is no "workable line . . . separat[ing] the consensual password sharing in this case from the consensual password sharing

of millions of legitimate account holders, which may also be contrary to the policies of system owners." *Id.* at 20 (Reinhardt, J., dissenting).

Furthermore, while this case involves former employees whose access credentials had been revoked, computer owners commonly restrict password sharing in their terms of use. In such circumstances, the majority opinion appears to criminalize violations of computer use restrictions, muddying this Court's previously clear declaration that the CFAA does not impose criminal liability for violations of corporate policy governing how computers are used. *See Nosal I*, 676 F.3d at 863.

B. The Panel's Decision Conflicts With *Power Ventures*.

The panel's reasoning is also in tension with *Power Ventures*, 2016 WL 3741956, decided within a week of this case and also implicating password sharing as a CFAA violation.

In *Power Ventures*, Facebook users who wanted to manage multiple social media accounts employed the services of Power Ventures ("Power"), a social media aggregator. The users voluntarily shared their valid Facebook usernames and passwords with Power so that it could access their accounts to provide its service. Facebook sent Power a cease and desist letter that claimed Power was violating its terms of use. Facebook later also blocked an IP address Power had used in an attempt to force Power to comply with its terms. Power continued to use

the valid credentials shared by Facebook users to provide its services, and Facebook sued. *Power Ventures*, 2016 WL 3741956, at *2–*3.

In contrast with the holding here, *Power Ventures* rightly recognized that individual Facebook users (*i.e.*, account holders) *can* provide a third party with valid authorization to access their Facebook accounts. It held that prior to receipt of the cease and desist letter, "Power had at least arguable permission to access Facebook's computers" and thus "did not initially access Facebook's computers 'without authorization[.]'" *Id.* at *6. But the panel also held that the valid authorization provided by the individual Facebook users could be rescinded or overruled by Facebook, even if the authorization from users continued, stating: "[t]he 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."[6] *Id.* at *7.

Thus, under *Power Ventures*, an authorized computer user could give "authorization" to a third party, even if doing so was in violation of terms of service, at least until receipt of a cease and desist letter. Here, in contrast, the panel majority held that, under the circumstances of the case, authorization could *not*

[6] *Amici* filed an *amicus* brief in support of rehearing *en banc* in *Power Ventures*, explaining how the ambiguity created by the panel's failure to explain what is sufficient, under what circumstances, to constitute "revocation of permission" for purposes of the CFAA, raises significant unconstitutional vagueness concerns. *See Power Ventures, Inc.*, No. 13-17102, Dkt. 89.

come from an authorized computer user. *Nosal II*, 2016 WL 3608752, at *8. And as the dissent recognized, under a natural reading of the majority's reasoning that the only entity capable of granting "authorization" for purposes of the CFAA is the computer owner (and that FH thus lacked the power, as a mere employee, to provide Christian with authorization to access the Korn/Ferry database), any use of another person's password without the permission of the computer owner—even without an express prohibition on password sharing within the computer owner's terms of use—could constitute a CFAA violation. *See id.* at *8 & n.7.

These two cases conflict with respect to when, and under what circumstances, an individual with access to a computer may grant authorization to a third party against the wishes of the computer owner. This tension exacerbates the flaw that Judge Reinhardt identified in the decision in this case, that "[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." *Id.* at *25 (Reinhardt, J., dissenting).

Given the inconsistencies between the majority opinion here and the decision in *Power Ventures*, as well as the conflict with prior circuit precedent, this Court should grant rehearing *en banc* in both cases.

II. *EN BANC* REVIEW IS NECESSARY BECAUSE OF THE FAR-REACHING CONSEQUENCES OF THE PANEL'S DECISION.

There is a second, and independent, reason to grant *en banc* review: the panel's interpretation of the CFAA renders the statute unconstitutionally vague and threatens to chill important computer security and online discrimination research.

A. The Panel's Interpretation of the CFAA Renders the Statute Unconstitutionally Vague.

A criminal statute is void for vagueness if it fails to provide fair notice of what is criminal or threatens arbitrary and discriminatory enforcement. *Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). Due process requires that criminal statutes provide ample notice of what conduct is prohibited. *Connally v. Gen. Const. Co*., 269 U.S. 385, 390 (1926). Vague laws that do not "provide explicit standards for those who apply them . . . impermissibly delegate[] basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis." *Grayned v. Rockford,* 408 U.S. 104, 108–09 (1972).

As a result, the Rule of Lenity calls for ambiguous criminal statutes to be interpreted narrowly in favor of the defendant. *United States v. Santos*, 553 U.S. 507, 514 (2008)). The Rule of Lenity "ensures fair warning by so resolving ambiguity in a criminal statute as to apply [] only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997). The Rule of Lenity "not only

ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals." *Nosal I*, 676 F.3d at 863.

The competing interpretations of the CFAA outlined above demonstrate that the statutory language is ambiguous. Indeed, vagueness concerns were at the heart of this Court's decisions to adopt a narrow interpretation of the CFAA in both *Nosal I* and *Brekka*. *See Nosal I*, 676 F.3d at 862–64; *Brekka*, 581 F.3d at 1135. Here, the panel's interpretation renders the statute unconstitutionally vague because it turns millions of innocent Internet users into potential criminals on the basis of innocuous password sharing—something that individuals across the country do every day—simply because they did not have authorization directly from the computer owner. Under the majority's reasoning, nearly anyone who logs into someone else's online or computer account, even with their consent, is a potential criminal. But people living their everyday lives often give a password or other access credentials to a family member, caregiver, colleague, or other trusted person to allow them to send an email or electronic invitation, check their social networking information or contacts, send a tweet, pay a bill, or check a bank or credit card statement. The panel majority's decision threatens to turn all such

"agents" into criminals simply because such access has not been blessed by the computer owner.

For example, as noted by this Court in *Nosal I*, Facebook prohibits a user from sharing their username and password or from letting anyone else access their account.[7] *See id.* at 861. Under the panel majority's interpretation, a husband who—with his wife's permission—logs into her Facebook account or accesses her profile has acted without authorization and is guilty of a federal crime. The same would be true if the wife accessed a joint bank account through her husband's log-in credentials to pay family bills, or a paralegal accessed a lawyer's email account, in violation of policies against password sharing. *See Nosal II*, 2016 WL 3608752, at *25 (Reinhardt, J., dissenting).

Ultimately, the panel majority fails to tie its decision back to any alleged computer break-in, losing sight of the CFAA's intended purpose. The decision thus creates legal uncertainty, rendering ordinary people unable to understand what conduct is prohibited. *See United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007). As the public's use of online services requiring passwords and other forms

[7] Facebook's terms of service specifically state, "You will not share your password . . . [,] let anyone else access your account, or do anything else that might jeopardize the security of your account." Facebook, Statement of Rights and Responsibilities 4.8, last revised Jan. 30, 2016, available at https://www.facebook.com/legal/terms.

of authentication prior to access increases, the scenarios for serious criminal liability for innocuous behaviors do, too.

By expanding the scope of CFAA liability, the panel's decision also subjects an untold number of Internet users to prosecution, such that prosecutors can pick and choose which types of password sharing or account access "are so morally reprehensible that they should be punished as crimes[.]" *See United States v. Kozminski*, 487 U.S. 931, 949 (1988). By giving that inherently legislative power to prosecutors, the panel has "invit[ed] discriminatory and arbitrary enforcement." *See Nosal I*, 676 F.3d at 862. The Constitution, however, "does not leave us at the mercy of noblesse oblige" by the government. *United States v. Stevens*, 559 U.S. 460, 480 (2010). Rather, it requires that criminal statutes be clear. To avoid fatal vagueness problems, the CFAA must be narrowly applied to only the behavior Congress clearly intended to criminalize: breaking into computers in order to access or alter information.

B. The Panel's Decision Threatens to Chill Valuable Research and Journalism, Including Audit Testing for Online Discrimination.

The panel majority's broad reading of the CFAA also threatens to chill socially valuable research, journalism, and testing online, much of which is protected First Amendment activity. This includes not only computer security research, but also audit testing for online discrimination. While Judge Reinhardt's dissent lists examples of innocuous behavior that could be rendered criminal by an

expansive reading of the CFAA, *see Nosal II*, 2016 WL 3608752, at *21–22 (Reinhardt, J., dissenting), *Amici* wish to draw attention to a specific form of online activity that is critically important to holding companies accountable and that will be chilled by the panel majority's decision.

Robust investigative techniques employed by journalists and academic researchers to uncover online discrimination sometimes require violating specific company prohibitions on certain activities, and are often adversarial to a company's business interests. Nonetheless, the panel majority's interpretation of access "without authorization" could render it criminal for a researcher or journalist to access a website or gather information from that website where it is clear that the company has prohibited access by researchers for research purposes—or, specifically, sharing passwords for research purposes.

The chill imposed on researchers and journalists is of particular concern when it comes to ensuring compliance with federal and state anti-discrimination laws. Offline, audit testing has long been recognized as a crucial way to uncover racial discrimination in housing and employment and to vindicate civil rights laws, particularly the Fair Housing Act ("FHA") and Title VII's prohibition on employment discrimination. *Cf. Havens Realty Corp v. Coleman*, 455 U.S. 363, 373 (1982).

Online, there is growing evidence that proprietary algorithms are causing websites to discriminate among users, including on the basis of race, gender, and other characteristics protected under civil rights laws.[8] In order to uncover whether any particular website is treating users differently, researchers need to use a variety of techniques, such as creating test accounts that vary on the basis of race or gender and comparing the job advertising or housing offers that are displayed to, say, male versus female users. In the latter case, researchers may need to access the accounts of actual users to compare housing or job offers that are given to people of different genders or races. Such techniques are often adversarial to a company's interests. Pursuant to the panel's opinion, if a company disagrees with the purpose of a researcher's access to its website, it can render that research criminal by merely stating in terms of use or by letter that researchers are not authorized to access its website, or that individual users are not allowed to share their access credentials with researchers or journalists. Websites could therefore shut down any unwanted anti-discrimination research or testing, even where the researcher did not break into a computer. Under the panel opinion, the company's choice to prohibit such research could be enforceable as a criminal CFAA violation. As a result, many researchers and journalists will likely refrain from conducting their socially

[8] *See*, *e.g.*, Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (May 2016), https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

valuable and constitutionally protected research to avoid the threat of criminal prosecution.

CONCLUSION

For the reasons discussed herein, this Court should grant *en banc* review of the panel decisions in both this case and *Power Ventures*.

Dated: August 26, 2016

By: */s/ Jamie L. Williams*

Jamie L. Williams
Cindy Cohn
Andrew Crocker
Stephanie Lacambra
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
jamie@eff.org

Esha Bhandari
Rachel Goodman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2654

Linda Lye
Nicole Ozer
Matthew T. Cagle*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437
**admission pending*

Attorneys for Amici Curiae
Electronic Frontier Foundation,
American Civil Liberties Union,
and American Civil Liberties
Union of Northern California

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(a)(7)

Pursuant to Fed. R. App. P. 32(a)(7), I certify as follows:

1. This *Amicus Curiae* Brief of Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Northern California in Support of Defendants-Appellants' Petition for Rehearing *En Banc* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,194 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: August 26, 2016

By: */s/ Jamie L. Williams*
Jamie L. Williams

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on August 26, 2016.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: August 26, 2016

By: */s/ Jamie L. Williams*
Jamie L. Williams