NOS. 13-17154, 13-17102

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FACEBOOK, INC.,

PLAINTIFF-APPELLEE,

V.

POWER VENTURES, INC. AND STEVEN VACHANI,

DEFENDANTS-APPELLANTS.

On Appeal From The United States District Court
for the Northern District of California
Case No. 5:08-cv-05780-LHK
Honorable Lucy H. Koh, District Court Judge

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AND AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA IN SUPPORT OF DEFENDANTS-APPELLANTS' 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 Foundation, and American Civil Liberties Union of Northern California

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 Foundation, 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 both Internet users and innovators who improve user experience. EFF filed *amicus* briefs in this case at both the district court and appellate level and argued as *amicus* before the Ninth Circuit panel. EFF has also served as counsel or *amicus* in various other CFAA cases.

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

[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. Neither party opposes the filing of this brief.

First Amendment for nearly a century in state and federal courts across the 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's decision in *United States v. Nosal*, No. 14-10037, 2016 WL 3608752 (9th Cir. July 5, 2016) ("*Nosal II*")—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 *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) ("*Nosal I*"), and *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), and effectively holding the defendants liable for a violation of a company's terms of service. The decisions make potential criminals out of millions of ordinary Americans on the basis of

innocuous online behavior. And 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. Under these decisions, researchers will fear that violating corporate policies forbidding research on public websites will subject them to CFAA liability.

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." *Nosal I*, 676 F.3d 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 a computer in order to access or alter information. *Power Ventures* conflicts with this precedent because it fails to assess whether the defendants broke into any computer and instead finds that a violation of corporate policy is sufficient to give

rise to CFAA liability, at least in cases where authorized users have permitted a third-party to access their accounts on their behalf.

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). This provision is also privately enforceable through a civil suit for damages or injunctive relief. 18 U.S.C. § 1030(g). 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 *Nosal II* dissent, the CFAA does not indicate who must provide the requisite authorization to access a computer or website. *See Nosal II*, 2016 WL 3608752, at *22 (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

CFAA liability. This Court, along with the Fourth Circuit and Second Circuit,[2] has found that they cannot, holding that the CFAA must be limited to the purpose intended by Congress—outlawing breaking into computers and then obtaining or altering 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

[2] *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*.").

CFAA's prohibition against accessing a protected computer "without 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.[3]

The panel in *Power Ventures* failed to assess whether defendants Steven Vachani and Power Ventures (collectively "Power") broke into a computer when they accessed Facebook's website. Indeed, Power did not. Power's access came from Facebook users whose valid accounts allowed them access to Facebook. Because these users wanted to more easily manage multiple social media accounts, they employed the services of a social media aggregator, Power. The users voluntarily shared their Facebook usernames and passwords with Power so that it could access their accounts in order to provide its service to them. Facebook sent Power a cease and desist letter that claimed violations of 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.

Importantly, Facebook never did the one thing that would have enforced its terms of service on Power: it never revoked the login credentials of any of the Facebook/Power users.

[3] Both the Fourth Circuit and Second Circuit, 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 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 (holding that 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").

Power continued to use the valid user credentials to provide its services to its willing customers, and Facebook sued. Yet, since the basis for the cease and desist letter and the attempted block of Power's IP address was Facebook's perception that Power was violating its terms of service, Power's continued use amounted to a mere violation of Facebook's corporate use policy.

The panel nevertheless found Power liable for violating the CFAA. The panel rightly recognized that individual Facebook users (*i.e.*, account holders) can provide a third party such as Power with valid authorization to access their Facebook accounts on their behalf. 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[.]'" *Facebook v. Power Ventures*, 2016 WL 3741956, at *6 (2016). 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: "[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."[4] *Id.* at *7.

[4] As explained in Section II *infra*, the ambiguity created by the panel's failure to explain what is sufficient, under what circumstances, to constitute "revocation of

According to the panel, after receipt of the cease and desist letter, and despite having ongoing authorization from Facebook's users and valid credentials, Power was no longer accessing Facebook's computers with "authorization" under the CFAA and was thus committing a crime. This holding rests *not* on whether Power broke into any computer system; it rests on whether Power's ongoing permission for access from users was still valid despite Facebook's notice of terms of service violations and an attempted IP block to enforce them—essentially the same type of "computer use" restriction that this Court, *en banc,* considered in *Nosal I* and found insufficient to render access unauthorized within the meaning of the CFAA.

B. The Panel's Decision Conflicts With *Nosal II*.

The panel's reasoning is also in tension with *Nosal II*, 2016 WL 3608752, decided only a week before this case and also involving password sharing.

In *Nosal II*, a company employee shared her legitimate login credentials for accessing a corporate database with former employees whose own credentials had been revoked. The *Nosal II* panel majority concluded that only the company—and not the employee with legitimate login credentials—could provide an individual with "authorization" to access the computer. According to the majority: "Implicit in the definition of authorization is the notion that someone, including an entity,

---

permission" for purposes of the CFAA raises significant concerns of unconstitutional vagueness.

can grant or revoke that permission. Here, that entity was [the company and computer owner] and [the current employee] 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.

But in this case, the panel held that—at least initially—Power had not violated the CFAA by gaining access to Facebook through the login credentials of individual Facebook users, even though Facebook had terms of use that made it clear that third parties such as Power were not free to access user accounts in this manner. *See Power Ventures*, 2016 WL 3741956, at *6.

It is difficult to articulate a standard from these two cases regarding when, and under what circumstances, an individual with access to a computer may grant access to a third party against the wishes of the computer owner. *See Nosal II*, 2016 WL 3608752, at *25 (Reinhardt, J., dissenting) ("It 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."). Given the inconsistencies between the panel opinion in this case and *Nosal II*, as well as its conflict with prior circuit precedent, this Court should grant rehearing *en banc* in both this case and *Nosal II*.

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.

Although this is a civil case, the underlying statutory prohibition against accessing a computer "without authorization" is criminal. Constitutional constraints on criminal statutes therefore apply. 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 at 862–64; *Brekka*, 581 F.3d at 1135. Here, the panel's interpretation renders the statute unconstitutionally vague because it is unclear when a computer user or website visitor's access becomes access "without authorization," and because the statute may give rise to arbitrary and discriminatory enforcement.

Significantly, the panel opinion fails to provide computer and website users with fair notice of what conduct is criminal. In particular, the decision fails to explain when a user is on notice that its conduct is "without authorization." *Power Ventures* held that Power was "plainly put . . . on notice" that its access to Facebook was unwanted because it had received a cease and desist letter alleging violations of terms of service. *See Power Ventures*, 2016 WL 3741956, at *7 n.2.

But the decision does not explain why similarly clear and explicit terms of use would not be sufficient notice. The panel's reassurance that "[v]iolation of . . . terms of use, without more, would not be sufficient to impose liability[,]" *id.*, creates *more* ambiguity rather than less around what constitutes lack of authorization, and why a cease and desist letter should be treated differently from other forms of written policy restrictions. At root, the panel fails to tie its decision back to any alleged computer break-in, losing sight of the CFAA's intended purpose. In so doing, the decision threatens to turn innocent Internet users into criminals on the basis of password sharing—something that individuals across the country do every day.

A few examples suffice to demonstrate this ambiguity. Suppose a bank website creates a pop-up notice warning that only credentialed users, not family members, are allowed to access the bank's computer system. Has the person who nonetheless continues to log in with her spouse's legitimate credentials to pay a bill, at the spouse's behest, been given "notice" that her access is "without authorization" under the CFAA? Similarly, could this rule criminalize using a partner's online video streaming account or Amazon account with their permission, if the company started prominantly displaying a notice upon each visit to its website that only registered users were allowed to stream videos or order goods, while third parties were not authorized to do so? What about logging into an airline

account to print a boarding pass, or paying a bill directly on a utility or credit card website, on behalf of another person? What if the website sent an individual email stating its terms of use? What if it sent a registered letter?

The panel's decision does not make clear which factor is dispositive in rendering access unauthorized, whether it is the critical factor of notice (in which case, prominently displayed website or computer policy restrictions such as those described above might count), or whether it is an individualized use restriction (such as through a cease and desist letter), or something else. And it is silent on the central act that could clarify when access is revoked: revocation of access credentials themselves.

These scenarios each involve a third party accessing a website as an agent or proxy of a legitimate account holder. This is commonplace online: people living their everyday lives often give a password or other access credentials to a family member, caregiver, or other trusted person to allow them to send an email or evite, check their Facebook or other social networking information or contacts, send a tweet, pay a bill, or check a bank or credit card statement. The panel's decision threatens to turn all such "agents" into criminals simply because a computer owner provides some—as yet unclear—level of notice that it does not want unregistered individuals accessing its computers.

The panel's 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 of authentication prior to access increases, the scenarios for serious criminal liability for innocuous behaviors do, too. And by basing CFAA liability on whether or not a company provided notice that a particular access was unwanted, the panel decision repeats the problem this Court has specifically sought to avoid: imposing criminal liability for violations of corporate policy governing how computers are used. *See Nosal I*, 676 F.3d at 863 ("[T]he CFAA does not extend to violations of [a company's or website's computer] use restrictions.").

By expanding the scope of CFAA liability in this way, 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 legislsative 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'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 *Nosal II* 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'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's interpretation of access "without authorization" would 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, such as if a website explicitly requires that account holders not use their accounts 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.[5] 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. Such techniques are often adversarial to a company's interests, and websites often prohibit the creation of test accounts in their terms of use. Pursuant to the panel's opinion, if a company disagrees with the

[5] *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.

purpose of a researcher's access to its website, it can make that prohibition clear and thereby shut down any unwanted anti-discrimination research or testing, even where the researcher did not break into a computer but merely accessed an otherwise-public website. Under the panel opinion, the company's choice to prohibit such research is enforceable as a criminal CFAA violation. As a result, many researchers and journalists will likely refrain from conducting their socially 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 *Nosal II*.

Dated: August 19, 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 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 Foundation, 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 Foundation, 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 4,193 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 19, 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 19, 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 19, 2016

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