NOS. 16-16832 & 16-16905

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ORACLE USA, INC. et al.,

PLAINTIFFS-APPELLEES,

v.

RIMINI STREET, INC., a Nevada corporation; SETH RAVIN, an individual,

DEFENDANTS-APPELLANTS.

On Appeal from the United States District Court
for the District of Nevada (Las Vegas)
Case No. 10-cv-00106-LRH

The Honorable Larry R. Hicks, District Court Judge

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANTS-APPELLANTS

Jamie Williams
Aileen Nguyen (on the brief)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: jamie@eff.org
Telephone: (415) 436-9333

Counsel for Amicus Curiae
Electronic Frontier Foundation

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, Amicus Curiae Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization working to protect consumer interests, innovation, and free expression in the digital world. With over 34,000 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 arises from its ongoing efforts to encourage the principled and fair application of computer crime laws, including not only the federal computer crime statute—the Computer Fraud and Abuse Act ("CFAA")—but also state computer crimes statutes, such as California's Computer Data Access and Fraud Act, Cal. Penal Code § 502, and Nevada's computer crime law, Nev. Rev. Stat. § 205.4765. EFF is specifically concerned with how the application of computer crime statutes impacts Internet users, innovators, and security researchers. In that regard, EFF has served as counsel or amicus in key cases addressing the CFAA and/or Cal. Penal Code § 502. *See United States v. Nosal*, __F. Supp. 3d__, No. 14-10037, 2016 WL 7190670 (9th Cir. Dec. 8, 2016) ("*Nosal II*") (amicus); *Facebook, Inc. v. Power Ventures, Inc.*, __F. Supp. 3d__, No. 13-

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

17102, 2016 WL 7190690 (9th Cir. Dec. 9, 2016) (amicus); *United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015) (amicus); *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (appellate co-counsel); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) ("*Nosal I*") (en banc) (amicus); *United States v. Cioni*, 649 F.3d 276 (4th Cir. 2011) (amicus); *Craigslist, Inc. v. 3Taps, Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (amicus); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus). EFF has also served as amicus in *State v. Nascimento*, 379 P.3d 484 (Or. 2016), a case involving the interpretation of Oregon's computer crime statute, Or. Rev. Stat. § 164.377.

INTRODUCTION

The district court in this case created a new theory of criminal liability under California's Computer Data Access and Fraud Act, Cal. Penal Code § 502, and Nevada's computer crimes law, Nev. Rev. Stat. § 205.4765—one that turns millions of ordinary Internet users into criminals on the basis of routine online behavior. Under the district court's reading of these two criminal statues—which apply when an individual knowingly accesses and takes, uses, or copies data from a computer "without permission," *see* Cal. Penal Code § 502(c)(2), (3), or accesses, uses, or copies data from a computer "without authorization," *see* Nev. Rev. Stat. § 205.4765(1), (3)—a violation of a website's terms of use now gives rise to criminal liability.

This court rejected this very outcome in the context of the federal computer crime statue, the Computer Fraud and Abuse Act ("CFAA"), and it should reject it here. *See United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) ("*Nosal I*") (en banc). Websites' terms of use cover everything from prohibitions on password sharing to real name requirements, and violations of these provisions are an everyday occurrence online. By criminalizing violations of corporate terms of use policies, the district court's interpretation of the California and Nevada computer crime statutes not only transforms ordinary Internet users into criminals on the basis of innocuous and routine online behavior, but it also renders both statutes

unconstitutionally vague. Consistent with the rule of lenity, this Court should reject the district court's overbroad interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765—and reverse its holding that Defendants Rimini Street, Inc. and Seth Ravin (collectively, "Rimini") violated these statutes through breaching the Terms of Use of Oracle's website.

ARGUMENT

I. ALLOWING LIABILITY UNDER EITHER CAL. PENAL CODE § 502 OR NEV. REV. STAT. § 205.4765 FOR TERMS OF USE VIOLATIONS TURNS A VAST NUMBER OF ORDINARY INDIVIDUALS INTO CRIMINALS.

California's computer crime law prohibits "[k]nowingly access[ing] and *without permission* tak[ing], cop[ying], or mak[ing] use of any data from a computer, computer system, or computer network, or tak[ing] or cop[ying] any supporting documentation." Cal. Penal Code § 502(c)(2) (emphasis added). Nevada's statute prohibits "knowingly, willfully and *without authorization* . . . Us[ing], . . . Cop[ying]" or "Obtain[ing] or attempt[ing] to obtain access to" a computer or data stored on a computer. *See* Nev. Rev. Stat. § 205.4765(1)(e), (j), (k) & (3)(i), (h), (k) (emphasis added).[2]

[2] Pursuant to this Court's recent holding in *Nosal II*, the phrases "without authorization" and "without permission" are synonymous. *United States v. Nosal*, __F. Supp. 3d__, No. 14-10037, 2016 WL 7190670, at *2 (9th Cir. Dec. 8, 2016) ("*Nosal II*"), ("[W]e conclude that 'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means . . . without permission[.]"); *see also United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)

Neither statute on its face applies to bare violations of a website's terms of use—such as when a computer user has permission *and* authorization to access *and* use the computer or data at issue, but simply accesses or uses the information in a manner the website owner does not like. That is exactly what happened here: Rimini at all times had permission and authorization to individually access, take, copy, and use support materials from Oracle's website for the purpose of assisting clients, the very purpose for which it sought access.[3] Rimini simply accessed the materials via an automated script that Oracle disapproved of in its Terms of Use.

("[T]o 'authorize' ordinarily means 'to give official approval to or permission for[.]'").

[3] Oracle attempted to block Rimini's IP address, but the cease and desist letter Oracle sent Rimini refers to the blocks as a "temporary" method to enforce its terms of use and did not withdraw Rimini's—or Rimini's clients'— authorization to generally access, download, or use materials from Oracle's website. *See* Joint Opening Brief for Appellants Rimini Street, Inc. and Seth Ravin, Dkt. 34, p. 9; ER1374–75. This cease and desist letter was thus very different than the one sent by the plaintiff in *Facebook, Inc. v. Power Ventures, Inc*., __F. Supp. 3d__, No. 13-17102, 2016 WL 7190690, at *6, n.3 (9th Cir. Dec. 9, 2016), which "plainly put Power on notice that it was no longer authorized to access Facebook's computers." Unlike in that case, the cease and desist letter here, referencing a "temporary" IP address block, was far from unequivocal. Indeed, as has been noted by law professor and CFAA scholar Orin Kerr, instituting even a *permanent* IP address block should not be viewed as an access barrier or revocation of authorization; because "circumventing an IP block does not violate trespass norms" governing the Internet, IP address blocks are a form of provider-imposed restriction or limit that should be viewed as "at most speed bumps (that cannot trigger trespass liability)[.]" Kerr, Orin S. Kerr, *Norms of Computer Trespass*, 116 Columbia Law Review 1143, 1164, 1169 (2016), available at https://ssrn.com/abstract=2601707. A *temporary* IP address block thus surely should not be viewed as a revocation of authorization, let alone an unequivocal one.

Yet, the district court nevertheless found that Rimini acted "without permission" *and* "without authorization" when it "used, or caused to be used, automated downloading tools on Oracle America's website in violation of the website's Terms of Use[.]" *Oracle USA, Inc. v. Rimini St., Inc.*, __F. Supp. 3d __, 2016 WL 3344377, *7 (D. Nev. 2016). By reading the California and Nevada statues to include terms of use restrictions governing the *manner* in which an authorized computer user can access and use a computer system, the lower court extended the reach of both statutes—to the detriment of all Internet users.

As this Court recognized *en banc* when interpreting the scope of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, basing criminal liability on the violation of corporate terms of use would transform "millions of ordinary citizens" into criminals. *Nosal I*, 676 F.3d at 862. In *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015), *cert. denied*, 2017 WL 69212 (Jan. 9, 2017), this Court noted that there are textual differences between the CFAA and Cal. Penal Code § 502: "the CFAA criminalizes unauthorized access" while § 502 criminalizes "unauthorized taking or use of information." But regardless of these slight textual differences, one thing at least is true for both statutes—in addition to Nev. Rev. Stat. § 205.4765 and *any other* computer crime statute regardless of its language[4]—"[b]asing criminal liability on violations of private computer use

[4] *See, e.g., State v. Nascimento*, 379 P.3d 484, 491 (Or. 2016) (rejecting the

policies can transform whole categories of otherwise innocuous behavior into . . . crimes simply because a computer is involved." *See Nosal I*, 676 F.3d at 860.

For instance, as this Court has noted, Google's terms of service used to forbid minors from using its services.[5] Under the district court's interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765, a vast number of teens and pre-teens under the age of 18 would have been transformed into juvenile delinquents—and their parents and teachers into delinquency contributors—just for using a Gmail account or conducting a Google search, as doing so would have been in violation of Google's policy. *See id.* at 861.

Furthermore, to this day many social media websites and dating websites prohibit lying about or otherwise misrepresenting personal information. *See id.* at 861.[6] But people routinely take a few years off their age, a few pounds off their

---

government's contention that Oregon's computer crime statute, Or. Rev. Stat. § 164.377(4)—which makes it a crime to use, access, or attempt to access a computer or computer network "without authorization"—covered violations of corporate terms of use, in part because of the unintended consequences of such an interpretation: "it is a stretch to suggest that an employee who uses her work computer to send a private email during the work day—or check Facebook or buy a movie ticket—contrary to her employer's policy against personal use, has 'accessed' or 'used' the computer 'without authorization,' although she may have violated her employer's policy.").

[5] *See* Google, Terms of Service, § 2.3 (effective Apr. 16, 2007 – Mar. 1, 2012), http://www.google.com/intl/en/policies/terms/archive/20070416 ("You may not use the Services and may not accept the Terms if . . . you are not of legal age to form a binding contract with Google[.]").

[6] *See, e.g.,* Facebook, Statement of Rights and Responsibilities, § 4.1 (last updated

weight, or otherwise describe themselves more optimistically than accurately. And there are legitimate reasons to register an online account with something other than a real name; it can protect against online harassment and discrimination.[7] But under the lower court's interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765—just as was the case with regard to an overbroad reading of the CFAA—using an alternative name or nickname, or "describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit." *See id.* at 862.

The same is true for violating eBay's terms of use, which prohibits posting an item for sale in an inappropriate category. *See id* at 861–62.[8] Users undoubtedly

---

Jan. 30, 2015), https://www.facebook.com/legal/terms ("You will not provide any false personal information on Facebook[.]"); Match.com, Terms of Use Agreement, § 9 (last updated Dec. 14, 2016), http://www.match.com/registration/membagr.aspx ("You represent and warrant that all information that you submit upon registration is accurate and truthful and that you will promptly update any information provided by you that subsequently becomes inaccurate, misleading or false.").

[7] *See* J. Nathan Matias, *The Real Name Fallacy*, The Coral Project (Jan. 3, 2017), https://blog.coralproject.net/the-real-name-fallacy/; *see also* Jacob Davidson, *Facebook's Zuckerberg Defends Controversial 'Real Name' Policy*, Money (Jul. 1, 2015), https://time.com/money/3942997/facebook-real-name-policy/ ("[Facebook's] real name policy, which requires users to go by their real names on the site, has been criticized by domestic violence survivors, Native Americans, drag queens, and trans users, who say the rule discriminates against their identity and in some cases puts them at risk of physical harm.").

[8] *See* eBay, User Agreement (last updated Sept. 29, 2016), http://pages.ebay.com/help/policies/user-agreement.html ("[Y]ou will not: post, list or upload content or items in inappropriate categories[.]").

do this—sometimes accidentally and sometimes purposefully, because they think their posting will get more traffic. In either case, under the lower court's interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765, these users would be guilty of a crime.

Just as this Court noted in the context of the CFAA, if the California and Nevada legislatures "meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect [them] to use language better suited to that purpose." *See id*. at 857. Neither used such language, and this Court should reject Oracle's attempt to expand the scope of both statutes so as to cover the conduct at issue here. *See United States v. Bass*, 404 U.S. 336, 348 (1971) ("Because of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislature and not courts should define criminal activity.").

The district court relied on *Christensen* to conclude that Cal. Penal Code § 502—and thus also Nev. Rev. Stat. § 205.4765, which "covers the same conduct," *Oracle*, 2016 WL 3344377 at *6—criminalizes violations of a website's terms of use. But the district court's reading takes *Christensen* too far. That case involved behavior that is a far cry from the mere terms of use violation at issue here. *Christensen* involved a "widespread criminal enterprise" with employees

using their login credential to access information for illegal purposes, *i.e.*, helping to set up illegal wiretaps or otherwise assisting an illegal private investigation service. *See Christensen*, 828 F.3d at 775. By contrast, this case involves an entity that had authorization and permission to access, copy, and use the materials at issue, and indeed did so for the very purpose authorized, just in a manner the computer owner (here, Oracle) did not approve of.

To avoid transforming millions of computer users into criminals on the basis of innocuous online activity, this Court should reject not only the district court's expansive interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765, but also its overbroad reading of *Christensen*—a case that should be limited to its stark facts.

II. THE LOWER COURT'S BROAD READING OF CAL. PENAL CODE § 502 AND NEV. REV. STAT. § 205.4765 RENDERS THE STATUTES UNCONSTITUTIONALLY VAGUE.

A criminal statute can be void for vagueness if it (a) fails to provide fair notice as to what is criminal, or (b) has the potential to lead to arbitrary and discriminatory prosecutions. *Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). As a result, the rule of lenity calls for ambiguous criminal statutes—particularly those that also impose civil liability—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). Critically, the "rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that [lawmakers] have fair notice of what conduct its laws criminalize." *Nosal I*, 676 F.3d at 863.

Constitutional vagueness concerns were at the heart this Court's decision to exclude violations of computer use restrictions from federal computer crime liability and to instead limit such liability to violations of access restrictions. *See id.* at 862–64; *see also United States v. Valle,* 807 F.3d 508, 527–28 (2nd Cir. 2015)*; WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012). The same concerns apply to the state computer crime statutes at issue here. Namely, if this Court were to uphold the lower's court's interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765 as criminalizing terms of use violations, the statutes would be invalidated as vague—both for failing to give adequate notice and for risking arbitrary enforcement.

A. Terms of Use Do Not Provide Sufficient Notice of What Conduct Is Prohibited.

Due process requires that criminal statutes provide ample notice of what conduct is prohibited. *See Connally v. Gen. Const. Co*., 269 U.S. 385, 390 (1926). But basing criminal liability on policies instituted by private entities confers on these entities the power to outlaw any conduct they wish without the clarity and

specificity required of criminal law. As this Court has previously recognized, "allow[ing] criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read" creates "[s]ignificant notice problems[.]" *Nosal I*, 676 F.3d at 860.

The central problem with basing criminal liability on terms of use restrictions, such as the one at issue in this case, is that such liability would permit a private party to manipulate the company-consumer relationship—a relationship traditionally governed by tort and contract law—"into ones policed by the criminal law." *Id.* This would grant website owners the power to unilaterally "transform whole categories of otherwise innocuous behavior into . . . crimes." *Id.* Website's terms of use agreements are drafted to address concerns far beyond the purpose underlying computer crime statutes like Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765—to target malicious actors who break into computer systems to cause damage or steal information. Premising liability on violations of use restrictions would allow the contours of criminal law to turn on market forces and the whims of private entities.

Further, because website owners retain the right to modify their policies or terms of use at any time, without notice,[9] "behavior that wasn't criminal yesterday

[9] *See, e.g.*, Amazon, Conditions of Use (last updated June 21, 2016), https://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088 ("We reserve the right to make changes to our site, policies,

can become criminal today without an act of [the legislature] . . . and without any notice whatsoever." *Nosal I*, 676 F.3d at 862. This result gives everyday Internet users "insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1586 (2010).

The notice problems inherent in premising criminal liability on terms of use agreements are exacerbated by the language and length of these agreements. One study of 30 terms of use agreements of popular websites—including Facebook, LinkedIn, Pinterest, Google+, Wikipedia, Twitter, Craigslist, and IMDB—found that most were written at a college reading level and contained thousands of words, and that reading all 30 would take a total of eight hours.[10] Indeed, as noted, this Court has acknowledged that terms of use agreements are lengthy, opaque, and seldom read. *Nosal I*, 676 F.3d at 860 (also noting that access to smart phones, iPads, Kindles, Nooks, X-boxes, Blu-Ray players and other Internet-enabled devices is "governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands"). In one example, an online gaming store modified its terms of use on April Fool's Day to

---

Service Terms, and these Conditions of Use at any time.").

[10] Casey Fiesler & Amy Bruckman, *Copyright Terms in Online Creative Communities*, Georgia Institute of Tech. (2014), http://www.chi.gatech.edu/2014/giving-it-away/.

state that purchasers agreed to grant to the company a claim to their "immortal soul"; only 12 percent of purchasers clicked on a hyperlink that allowed them to nullify the soul transfer and instead receive a coupon.[11]

Attaching criminal punishment to violations of vague, constantly changing, boilerplate-filled, and largely unread terms of use agreements would make it impossible for Internet users to know what conduct is criminally punishable at any given time.

B. Basing Liability on Violations of Terms of Use Restrictions Would Permit Capricious Enforcement by Prosecutors.

The district court's interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765 is unconstitutionally vague for a second reason: it risks arbitrary enforcement. As the Supreme Court has stated, "if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them." *Grayned v. Rockford*, 408 U.S. 104, 108 (1972). "A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application." *Id*. at 108–09.

By expanding the scope of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765 to cover millions of ordinary individuals who violate terms of use

[11] *See, e.g.*, Catharine Smith, *7,500 Online Shoppers Accidentally Sold Their Souls to Gamestation*, Huffington Post (June 17, 2010), http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html.

restrictions via innocuous and routine online behaviors, the lower court's decision permits arbitrary and discriminatory enforcement. Namely, by interpreting these statutes in a way that would "criminalize a broad range of day-to-day activities," the lower court subjects Internet users to prosecution at the whim of prosecutors, who can pick and choose which violations they wish to penalize. *See United States v. Kozminski*, 487 U.S. 931, 949 (1988). Such broad statutory interpretation "delegate[s] to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes" and "subject[s] individuals to the risk of arbitrary or discriminatory prosecution and conviction." *Id*. at 932. Here, by giving that much power to prosecutors, the lower court has "invit[ed] discriminatory and arbitrary enforcement." *See Nosal I*, 676 F.3d at 862. Under the lower court's interpretation of the statutes, just as for the CFAA, in the context of violating a terms of use prohibition against misrepresenting personal characteristics, "[t]he difference between puffery and prosecution may depend on whether you happen to be someone [a prosecutor] has reason to go after." *Id. at* 862.

As the Supreme Court has noted, the Constitution "does not leave us at the mercy of *noblesse oblige*" by the government. *United States v. Stevens,* 559 U.S. 460, 480 (2010); *see also Nosal I*, 676 F.3d at 862. Thus, while the government might promise that it would not prosecute an individual for trivial matters, such as

claiming on a dating site that one is taller than one actually is, the fact is that pursuant to the lower court's holding, it could—under either statute. And as the Second Circuit recently held in rejecting an interpretation of the CFAA that included terms of use violations, "we are not at liberty to take prosecutors at their word in such matters." *Valle*, 807 F.3d at 528. As the Second Circuit stated, "[a] court should not uphold a highly problematic interpretation of a statute merely because the Government promises to use it responsibly." *Id*. (citing *Stevens*, 559 U.S. 460, 480 (2010)). In order to avoid fatal vagueness problems, this Court must reject the district court's interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765 as criminalizing violations of a website's terms of use.

CONCLUSION

For the reasons discussed herein, this Court should overrule the district court's expansive interpretation of Cal. Penal Code § 502 and Nev. Rev. Stat. § 205.4765.

Dated: January 26, 2017

By: /s/ Jamie Williams
Jamie Williams
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
jamie@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

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

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

1. This Brief of Amici Curiae Electronic Frontier Foundation In Support of Defendants-Appellants complies with the type-volume limitation, because this brief contains 3,934 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: January 26, 2017

By: /s/ Jamie Williams
Jamie Williams

Counsel for Amicus Curiae
Electronic Frontier Foundation

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 January 26, 2017.

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: January 26, 2017

By: /s/ Jamie Williams
Jamie Williams

Counsel for Amicus Curiae
Electronic Frontier Foundation