No. 10-10038

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

DAVID NOSAL,

Defendant-Appellee.

Appeal from the United States District Court
for the Northern District of California, San Francisco
in Case No. CR-08-0237 MHP (Hon. Marilyn Hall Patel)

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLEE'S PETITION FOR REHEARING EN BANC

Marcia Hofmann
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, California 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Amicus Curiae
Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

State Statute

Federal Rules

Other Authorities

Legislative Materials

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

Pursuant to Federal Rule of Appellate Procedure 26.1, amicus Electronic Frontier Foundation, a 501(c)(3) non-profit corporation incorporated in the Commonwealth of Massachusetts, makes the following disclosures:

1. Amicus is not a publicly held corporation or other publicly held entity.
2. Amicus has no parent corporations.
3. No publicly held corporation or other publicly held entity owns 10% or more of amicus.

STATEMENT OF AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at www.eff.org.

As part of that mission, EFF serves as counsel or amicus curiae in key cases addressing computer crime, and the Fourth Amendment as applied to the Internet and other new technologies. EFF is particularly interested in ensuring the proper application of the Computer Fraud and Abuse Act and state computer crime laws, as well as maintaining constitutional protections for criminal defendants. Toward this end, EFF has filed amicus briefs in cases such as United States v. Cioni, --- F.3d ---, 2011 WL 1491060 (4th Cir. 2011), United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009), Facebook v. Power Ventures Inc., 2010 WL 3291750 (N.D. Ca. Jul. 20, 2010), and the panel proceeding in this case.

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 Counsel for Appellant the United States of America nor Appellee David Nosal oppose the filing of this brief.

INTRODUCTION

In one fell swoop, the panel opinion creates a new theory of criminal liability under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, that gives employers the discretion to define what is and is not a federal crime. The panel misconstrued this Court's prior decision in LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), ignored the text and purpose of the CFAA, and inadvertently extended another provision of the CFAA to make criminals out of millions of ordinary Americans. The panel purported to do this on the basis of the word "so" in the text of § 1030(e)(6). Because the panel's decision expands the CFAA dramatically, the Court should grant rehearing *en banc*.

STATEMENT OF THE CASE

A. The Facts

The facts are simple and not in dispute. Appellee David Nosal was an executive at Korn/Ferry executive search firm. United States v. Nosal, --- F.3d ---, 2011 WL 1585600 at *1 (9th Cir. 2011). Korn/Ferry maintained a computer database with contact information for potential executive candidates. Id. at *2. In an effort to maintain the confidentiality of the information in the database, Korn/Ferry employees had unique usernames and passwords to access the database. Id. Moreover, all employees were

required to sign agreements acknowledging that the information in the database could only be used for Korn/Ferry business. Id. Any time an employee accessed the database, a pop-up banner warned, "[t]he computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution." Id.

Nosal decided to leave the firm to start his own company and asked two Korn/Ferry employees to access information from the database. Id. at *1. It was undisputed that the employees had authority to access the database because they were still employed by Korn/Ferry at the time they accessed the database. Id. at *3-4.

The government charged Nosal under § 1030(a)(4), which makes it a crime to "knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access, and by means of such conduct further[] the intended fraud and obtain[] anything of value." The term "exceeds authorized access" is defined in § 1030(a)(6) as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

Because the employees were authorized to access the database, the government's theory was that Nosal's accomplices "exceed[ed] authorized access" when they obtained information from the database they were allowed to access, but intended to use that information for an unauthorized *purpose*.

The district court granted Nosal's motion to dismiss on the basis of this Court's decision in Brekka, which held that "exceeds authorized access" in the CFAA refers to an individual who "has permission to access the computer, but accesses information on the computer that the person is not entitled to access." 581 F.3d at 1133. The district court found that since Nosal's accomplices had authority to access the database as current Korn/Ferry employees, they had not "exceed[ed] authorized access" regardless of their fraudulent intent. Nosal, 2011 WL 1585600 at *4.

B. The Panel Opinion

The government appealed, arguing the word "so" in § 1030(a)(6) "clarifies that the accesser might have been entitled to obtain the information *in some circumstances*, but not in the way he did – *i.e.*, he was 'not entitled so to obtain' the information." Gov. Reply Brief at 8 (quoting § 1030(e)(6)) (emphasis in original). As a result, Nosal could be held liable because "someone exceeds authorized access by obtaining information in a

prohibited manner, even if the accesser might be entitled to obtain the same information under other circumstances." Gov. Reply Brief at 9.

The panel agreed with the government. Relying on Webster's Dictionary's definition of "so" as meaning "in a manner or way that is indicated or suggested," the panel ruled "an employee exceeds authorized access under § 1030(e)(6) when the employee uses that authorized access 'to obtain or alter information in the computer that the accesser is not entitled [in that manner] to obtain or alter.'" 2011 WL 1585600 at *4. The panel believed Brekka held "it is the *employer's* actions that determine whether an employee acts without authorization to access a computer in violation of § 1030" and therefore "the *only* logical interpretation of 'exceeds authorized *access*' *is that the employer has placed* limitations on the employee's 'permission to use' the computer and the employee has violated – or 'exceeded' – those limitations." Nosal, 2011 WL 1585600 at *5-6 (emphasis in original).

Responding to Nosal's concern that "our decision will make criminals out of millions of employees who might use their work computers for personal use," the panel claimed § 1030(a)(4)'s requirement that criminal liability only attaches if a defendant has both the intent to defraud and his unauthorized access furthers the fraud and obtains something of value meant

"simply using a work computer in a manner that violates an employer's use restrictions, without more, is not a crime under § 1030(a)(4)." 2011 WL 1585600 at *7.

District Judge Campbell, sitting by designation, dissented. 2011 WL 1585600 at *8 (Campbell, D.J., dissenting). She noted that while the intent to defraud was required in § 1030(a)(4), the majority failed to take into account that the phrase "exceeds authorized access" also appears in § 1030(a)(2)(C). That section of 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." Id. Section 1030(a)(2)(C) has no intent requirement aside from "intentionally accessing a computer without authorization or exceed[ing] authorized access[.]" Id. Thus, the majority did precisely what it claimed not to do: make a criminal out of any employee who might use her work computer for personal use in violation of her employer's computer policy. Id.

Judge Campbell feared that such an interpretation would not only make the CFAA unconstitutionally vague, but also lead to arbitrary enforcement. Id. at *9. As for the majority's belief that the word "so" in § 1030(a)(6) required such an interpretation, she noted "so" was likely

"added for emphasis alone," as in § 1030(a)(1), which prohibits theft of government secrets by someone "with reason to believe that *such information so obtained* could be used to the injury of the United States." Id. at *10 (quoting § 1030(a)(1)) (emphasis in original). That would conform with the CFAA's purpose of combatting hacking by individuals never authorized to access a particular computer. See Nosal, 2011 WL 1585600 at *10 (Campbell, D.J., dissenting) (citing S. Rep. No. 99-432 (1986) reprinted in 1986 U.S.C.C.A.N. 2479).

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 of these prongs are satisfied here.

A. The Court Should Grant En Banc Review Because the Panel Decision Conflicts With LVRC Holdings LLC v. Brekka.

Brekka was concerned with interpreting the term "without authorization" in §§ 1030(a)(2) and (4). Finding that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it," the Court confirmed that "without authorization" applies to a situation when an employee "has not received permission to use that computer for *any* purpose . . . or when the employer

has rescinded permission to access the computer and the defendant uses the computer anyway." Brekka, 581 F.3d at 1133, 1135.

Relevant to the panel's discussion of the key term here – "exceeds authorized access" – was Brekka's observation that "an individual who is authorized to use a computer for certain *purposes* but goes beyond those *limitations* is considered by the CFAA as someone who has 'exceed[ed] authorized access.'" Id. at 1133 (emphasis added). The panel seized upon this language to conclude that its decision "that an employer's use restrictions define whether an employee 'exceeds authorized access' is simply an application of Brekka's reasoning." Nosal, 2011 WL 1585600 at *6.

But the panel missed Brekka's key point: that "a person who 'exceeds authorized access,' has permission to access the computer, but *accesses information* on the computer that the person is not entitled to access." Brekka, 581 F.3d at 1133 (quoting § 1030(a)(6)) (emphasis added) (citation omitted). In other words, the "limitations" discussed in Brekka concerned restrictions on *access* to information, not subsequent *use* of that information.

That is how Brekka made "without authorization" and "exceeds authorized access" co-exist: one covers a situation where a person never had access rights at all ("without authorization"), and the other covers a situation

where the person had rights to access some information, but goes beyond these rights to access information she is not authorized to obtain ("exceeds authorized access"). Neither situation defines access in terms of *how* that information is ultimately used. The majority of courts interpreting the phrase "exceeds authorized access" have reached the same conclusion.[1]

Thus, it is clear that an individual "exceeds authorized access" only when she is not granted full access to information on a computer, but access that information anyway by exceeding the *limitations* placed on her access.

[1] See, e.g., Koch Industries, Inc. v. Does, 2011 WL 1775765 *8 (D. Utah May 9, 2011) (citing Brekka and stating "plaintiff's claim was really a claim that a user with authorized access had used the information in an unwanted manner, not a claim of unauthorized access or of exceeding authorized access. A majority of courts have concluded that such claims lie outside the scope of the CFAA."); Orbit One Communications, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (holding CFAA does not "encompass an employee's misuse or misappropriation of information to which the employee freely was given access."); see also Lewis-Burke Associates, LLC. v. Widder, 725 F. Supp. 2d 187 (D.D.C. 2010); Clarity Services v. Barney, 698 F. Supp. 2d 1309, 1316 (M.D. Fla. 2010); Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d 1267 (M.D. Ala. 2010); ReMedPar, Inc. v. AllParts Medical, LLC, 683 F. Supp. 2d 605, 611 (M.D. Tenn. 2010); Black & Decker (US) Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008); Diamond Power International, Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); International Association of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Maryland 2005); Nat'l City Bank, N.A. v. Republic Mortgage Home Loans, LLC, 2010 WL 959925 (W.D. Wash. Mar. 12, 2010) (unpublished); Jet One Group v. Halcyon Jet Holdings, Inc., 2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009) (unpublished); Brett Senior & Associates, P.C. v. Fitzgerald, 2007 WL 2043377 (E.D. Pa. July 13, 2007) (unpublished); Lockheed Martin Co. v. Kelly, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006) (unpublished).

Stated differently, a CFAA "violation does not depend upon the defendant's unauthorized use of *information*, but rather upon the defendant's unauthorized use of *access*." Diamond Power International, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (emphasis in original).

This scenario is not hard to envision. As the district court noted, "if a person is authorized to access the 'F' drive on a computer or network but is not authorized to access the 'G' drive of that same computer or network, the individual would 'exceed authorized access' if he obtained or altered anything on the 'G' drive." Nosal, 2011 WL 1585600 at *3. This is what Brekka meant when it explained that "a person who 'exceeds authorized access,' [] has permission to access the computer, but accesses information on the computer that the person is not entitled to access." Brekka, 581 F.3d at 1133 (citation omitted).

This interpretation comports with the plain text of § 1030(e)(6), which states the term "'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." The statute clearly punishes the act of accessing, not misusing, information. As one district court has noted, if Congress wanted to capture within the definition

of "exceeds authorized access" those who misuse information they are otherwise entitled to access, it would have written § 1030(a)(4) "without any reference to 'authorization.'" Lockheed Martin Corp., 2006 WL 2683058 at *6.

To the extent Congress did intend to capture those employees who misuse their authority to access, the CFAA does that *not* in the term "exceeds authorized access," but in the provision of § 1030(a)(4) that explicitly requires fraudulent intent. See 18 U.S.C. § 1030(a)(4) (requiring a defendant to do an act "knowingly and with intent to defraud" which "furthers the intended fraud and obtains anything of value").

But by "looking to an offender's motivation in accessing information in determining whether the unlawful access requirement has been met," the panel "seeks to collapse these independent requirements into a single inquiry: whether the offender intended to use impermissibly the information obtained." Brett Senior & Associates, 2007 WL 2043377 at *4. That, in turn, makes the fraudulent intent language in § 1030(a)(4) superfluous. And as even the panel noted, "one of the most basic interpretive canons is that a statute should be construed so that effect is given to all of its provisions, so that no part will be inoperative or superfluous, void or insignificant." Nosal,

2011 WL 1585600 at *4 (quoting Corley v. United States, --- U.S. ---, 129 S. Ct. 1558, 1566 (2009)) (brackets omitted).

In short, the panel lost sight of the fact that § 1030 is concerned with "access," and that an individual "exceeds authorized access" only when she accesses things she is not permitted to access, not when she misuses the information. This Court should grant *en banc* review to reconcile the panel's opinion with Brekka.

B. The Panel's Erroneous Interpretation of "Exceeds Authorized Access" in § 1030(a)(6) Merits *En Banc* Review Because It Turns a Vast Number of Employees Into Criminals.

There is a second compelling reason to grant *en banc* review: the panel dramatically expanded the CFAA to cover millions of employees who violate their employers' computer use restrictions every day. The panel turned the CFAA on its head by allowing employers to unilaterally decide what will become criminal activity. It also exposes individuals to abusive litigation and selective enforcement of the law by prosecutors.

The panel claimed that it did "not dismiss lightly" the possibility that its decision could criminalize the mundane, everyday behavior of employees who read personal email or check the score of a college basketball game in violation of their employers' computer use policies. Nosal, 2011 WL 1585600 at *7. However, the panel believed that § 1030(a)(4)'s requirement

that an employee must have an "intent to defraud" was enough to protect employees under these circumstances. Id.

But as Judge Campbell wrote in her dissenting opinion, the term "exceeds authorized access" does not appear only in section § 1030(a)(4), which, as noted above, requires fraudulent intent. See Nosal, 2011 WL 1585600 at *8-9. It also appears in § 1030(a)(2)(C), which imposes criminal penalties on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer." Nothing more is required.[2] And since "identical words used in different parts of the same statute are generally presumed to have the same meaning," IBP, Inc. v. Alvarez, 546 U.S. 21, 34 (2005), the panel's interpretation of the CFAA allows employers to determine what behavior is not "authorized," and therefore a serious federal crime under § 1030(a)(2)(C).

[2] See Ninth Circuit Model Criminal Jury Instruction 8.79 (liability under § 1030(a)(2)(C) requires only (1) intentionally accessing without authorization or exceeding authorized access to a protected computer; and (2) obtaining information from the computer). The term "protected computer" includes any computer connected to the Internet. See 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as one that "is used in or affecting interstate or foreign commerce or communication"); see also United States v. Tello, 600 F.3d 1161, 1165 (9th Cir. 2010) (Internet is "instrumentality of interstate commerce").

This concern is hardly hypothetical. In a recent lawsuit in Florida, a woman sued her former employer for wrongfully terminating her employment after she became pregnant. Lee v. PMSI, Inc., 2011 WL 1742028 (M.D. Fla. May 6, 2011). The company retaliated with a counterclaim alleging that the plaintiff violated § 1030(a)(2)(C) by making personal use of the Internet at work in violation of company policy. Id. at *1. While the court ultimately dismissed the counterclaim, the panel's troubling interpretation of the CFAA offers new fodder for those who would make similar overreaching and abusive arguments under § 1030(a)(2)(C).

The panel's interpretation also renders the CFAA unconstitutionally vague. "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." Grayned v. City of Rockford, 408 U.S. 104, 108-109 (1972). One needs to look no further than the government's brief to see an example of the potential for abuse:

> For example, an employer could grant an employee access to all information on its computer system, but it could restrict that access authority in various ways. It may tell the employee, "You have permission to access any medical records on the computer system, but only between the hours of 9:00 a.m. and 5:00 p.m., only with the written approval of a supervisor, and only when a doctor has specifically requested the records." When these circumstances are not present, the employee is no

> more entitled to obtain the medical records than is another employee who is prohibited from accessing the medical records at all. And if the first employee accesses a medical record in a way that violates any of these specific restrictions, that employee would not be entitled "so to obtain" that medical record and would have exceeded authorized access under the CFAA.

Gov. Reply Brief at 8-9.

Under the government's rationale, it would be a crime to access a record at, for instance, 6:30 p.m. Nobody would imagine that she could be prosecuted under the CFAA for such an infraction of corporate policy. Indeed, it is this potential for abuse that has led most courts to reject the panel's interpretation of "exceeds unauthorized access."[3]

Nor does such a sweeping interpretation of the CFAA create the potential for draconian results only in the employment context. The panel's belief that a person "exceeds authorized access" anytime she violates a written policy regarding the use of a computer she is otherwise authorized to access could be extended to an Internet user who accesses a website in

[3] See, e.g., Brett Senior & Associates, 2007 WL 2043377 at *4 (finding it "unlikely that Congress, given its concern 'about the appropriate scope of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract") (quoting S. Rep. 99-432, at 3 (1986); Lockheed Martin Corp., 2006 WL 2683058 at *7 ("In addition to broadening the doorway to federal court, the 'adverse interest' inquiry affixes remarkable reach to the statute – a reach that is not apparent by the statute's plain language . . . would checking personal email on company time without express permission . . . give rise to CFAA liability? It might.").

violation of a written terms of service. Unsurprisingly, the government has argued precisely that in other cases, claiming that an Internet user's breach of a website terms of service is a criminal CFAA violation. See United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009); United States v. Lowson, No. 10-CR-00144 (D. N.J. filed Feb. 23, 2010). The panel's expansive reading of the statute opens the door to turning millions of Internet users into criminals for typical, routine Internet activity.

This is particularly troubling because companies often forbid common or mundane uses of the Internet in their terms of use. For example, Google's terms of service state, "You may not use the Services and may not accept the Terms if (a) you are not of legal age to form a binding contract with Google."[4] And Facebook's terms of service require users to "not provide any false personal information on Facebook" and to "keep your contact information accurate and up-to-date."[5] But under the panel's view, a minor who uses Google to research a high school history assignment has just committed a felony. So too the Facebook user who lies about her age or fails to immediately update her account when she moves to a different city.

[4] Google Terms of Service § 2.3, http://www.google.com/accounts/TOS (last modified Apr. 16, 2007) (last accessed June 21, 2011).

[5] Facebook Statement of Rights and Responsibilities § 4.1, 4.7, http://www.facebook.com/terms.php (last modified October 4, 2010) (last accessed June 21, 2011).

The panel surely did not intend to criminalize these routine, everyday activities under § 1030(a)(2)(C), but its opinion threatens to create that absurd result.

It also gives private parties the power to decide what will be a crime. As law professor Orin Kerr notes, "granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner." Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1650-51 (2003). This concern is particularly acute because companies can change their terms of service at any time. "Users of computer and internet services cannot have adequate notice of what actions will or will not expose them to criminal liability when a computer network or website administrator can unilaterally change the rules at any time and are under no obligation to make the terms of use specific or understandable to the general public." Facebook v. Power Ventures Inc., 2010 WL 3291750, *11 (N.D. Ca. Jul. 20, 2010) (unpublished). It is the duty of Congress to decide what conduct to criminalize, but the panel decision lets private parties make those decisions instead.

The panel's reading of the statute also gives prosecutors enormous discretion to arbitrarily enforce the law. As one district court noted, imposing liability for violating terms of service "would create a constitutionally untenable situation in which criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use." Facebook, 2010 WL 3291750 at *11 (analyzing California's computer crime law, Cal. Penal Code § 502). Another district court has warned that

> utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime . . . makes the website owner-in essence-the party who ultimately defines the criminal conduct. This will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers.

Drew, 259 F.R.D. at 465.

For these reasons, Facebook and Drew refused to criminalize violations of terms of service. But both of these opinions were issued *before* the panel's opinion. If the panel's opinion becomes the law of this circuit, then CFAA liability under § 1030(a)(2)(C) may extend not only to every hard-working employee who strays from her work duties for a few minutes, but also to the scores of individuals who never read a website's terms of service and unknowingly have become federal criminals. Because the

CFAA was never intended to apply so broadly, this Court should grant rehearing *en banc* to narrow the reach of a law that now has few boundaries.

CONCLUSION

The CFAA was "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.'" Brekka, 581 F.3d at 1130-31 (quoting H.R. Rep. 98-984, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)). The panel's opinion loses sight of this purpose and misinterprets Brekka in a way that expands the CFAA to allow employers to determine whether or not their employees can be sent to prison based on little more than checking their personal email on company time. Because the CFAA was not intended to apply so broadly, this Court should grant *en banc* review.

Respectfully submitted,

June 23, 2011

By: */s/ Hanni Fakhoury*

Hanni Fakhoury
Marcia Hofmann
Attorneys for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE

I hereby certify as follows:

1. The foregoing Brief of Amicus Curiae complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B). The brief is printed in proportionally spaced 14-point type, and there are 4,064 words in the brief according to the word count of the word-processing system used to prepare the brief (excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii)).

2. The brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5), and with the type style requirements of Federal Rule of Appellate Procedure 32(a)(6). The brief has been prepared in a proportionally spaced typeface using Microsoft Office Word 2011 in 14-point Times New Roman.

June 23, 2011 By: */s/ Hanni Fakhoury*

Hanni Fakhoury
Marcia Hofmann
Attorneys for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that on June 23, 2011, 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.

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.

June 23, 2011 By: */s/ Hanni Fakhoury*
Hanni Fakhoury