No. 10-10038

IN THE 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
District Court No. CR 08-0237 MHP

PETITION FOR REHEARING EN BANC

Dennis P. Riordan (SBN 69320)
Donald M. Horgan (SBN 121547)
Ted Sampsell Jones (MN SBN 034302X)
Riordan & Horgan
523 Octavia Street
San Francisco, CA 94102
Telephone: (415) 431-3472

Counsel for Appellee
DAVID NOSAL

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

Table of Authorities continued

MISCELLANEOUS

STATEMENT PURSUANT TO FED. R. APP. P. 35(b)

Pursuant to Federal Rule of Appellate Procedure 35(b), David Nosal hereby petitions for rehearing en banc of the panel decision in this matter. That published decision, by a 2-1 vote, reversed the district court's decision to dismiss several counts alleged under the Computer Fraud and Abuse Act (CFAA). 18 U.S.C. § 1030. *See United States v. Nosal*, – F.3d –, No. 10-10038 (9th Cir. April 28, 2011). En banc review is necessary both to maintain uniformity of this Court's decisions and to resolve questions of exceptional importance.

QUESTION PRESENTED

I. DOES AN EMPLOYEE VIOLATE THE COMPUTER FRAUD AND ABUSE ACT WHEN HE IS PERMITTED TO USE COMPANY COMPUTERS BUT DOES SO IN A MANNER THAT VIOLATES COMPANY POLICIES?

INTRODUCTION

This Court grants en banc review extremely rarely, but there are panel decisions that plainly require consideration by a broad cross-section of the members of this Court. This is such a case. The ruling of a divided panel has called into question the continuing validity of an earlier panel opinion on a legal issue of enormous social significance.

In passing the CFAA in 1986, Congress acted "to curb computer hacking."

Nosal, slip op. at 5538 (citing S. Rep. No. 99-432 at 2-3) (Campbell, J., dissenting). The question presented by this case is whether Congress not only intended the CFAA to penalize hacking, but also to impose criminal sanctions on an employee who, having been granted access to his employer's computers, violates company restrictions on their use. The divided three-judge panel now has held the CFAA does indeed sweep so broadly.

The expansive interpretation of the CFAA applied by the panel majority subjects a wide range of employee conduct to both civil and criminal liability. Moreover, the panel's decision has implications beyond the employment context. By extension, it creates liability for any violation of contracts limiting authorized computer usage, including standard-form terms of service for all kinds of websites.

The question presented here is thus an exceptionally important one, and it is also a difficult one. It has divided federal courts around the country.[1] In fact, in a ruling on essentially the same issue only two years ago, a unanimous three-judge panel of this Court consciously created a circuit split by adopting a narrow construction of the CFAA. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th

[1] *See Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 & nn. 65-66 (S.D.N.Y. 2010) (discussing the division of authority among federal circuit and district court cases interpreting the CFAA).

Cir. 2009) (Ikuta, McKeown, Selna (D.J.)).

This case has already received an unusual amount of attention. Even before the panel issued the *Nosal* decision, academic commentators recognized the importance of the issues presented here.[2] After the panel issued its ruling, the opinion sparked a flurry of reaction in the press and blogosphere.[3] In fact, the implications of the decision in this case have already been discussed in Congressional testimony.[4]

---

[2] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1585-87 (2010) (discussing the *Nosal* prosecution); Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization under the Computer Fraud and Abuse Act*, 52 Wm & Mary L. Rev. 1369, 1381-82 (2011) (same).

[3] *See, e.g.*, David Kravets, *Appeals Court: No Hacking Required to Be Prosecuted as a Hacker*, Wired, Apr. 29, 2011, http://www.wired.com/threatlevel/2011/04/ no-hacking- required/; *Ninth Circuit Reverses Course on Computer Fraud and Abuse Act*, Posting of John D. McLachlan to Non-Compete and Trade Secrets Blog, http://www.noncompetenews.com/post/2011/05/16/Computer-Fraud-Abuse-Act-Ninth-Circuit-Rerverses-Course.aspx (May 16, 2011); *When the Right Interpretation of the Law is a Scary One (CFAA Edition)*, Posting of Michael Risch to PrawfsBlawg, http://prawfsblawg.blogs.com/prawfsblawg/2011/04/ when-the-right-interpretation-of-the-law-is-a-scary-one-cfaa-edition.html (Apr. 28, 2011).

[4] *Cybersecurity: Innovative Solutions to Challenging Problems, Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of the H. Comm. on the Judiciary*, 112th Cong. (2011) (statement of Leslie Harris, President and CEO, Center for Democracy and Technology).

By reversing the course set by *Brekka*, the panel majority here both created a conflict within this circuit and decided an a question of exceptional importance. Whatever the merits of the majority's interpretation of the CFAA, the question merits en banc consideration, and the conflict with *Brekka* must be resolved.

STATEMENT OF THE CASE

The indictment in this case centers on allegations that defendant-appellee David Nosal and his accomplices misappropriated proprietary information from their employer. Mr. Nosal worked at Korn/Ferry International, an executive recruiting firm. He left Korn/Ferry with several other employees to start his own competing firm. The indictment alleges that the other employees, acting as Mr. Nosal's accomplices, obtained confidential and proprietary information from Korn/Ferry computers to use for their competing business.

At the time they obtained the information, the accomplices were still Korn/Ferry employees — they still had valid passwords to access Korn/Ferry databases, and they were still entitled to access the proprietary information. However, by allegedly using the information to help start a competing business, the employees violated Korn/Ferry corporate policies, which stated (among other things) that the proprietary databases could only be used for "legitimate Korn/Ferry business." (Indictment at ¶ 10.)

On June 28, 2010, the government filed an indictment against Mr. Nosal and one of his accomplices. The indictment alleged several crimes, including conspiracy, mail fraud, theft of trade secrets — and violations of the CFAA. Prior to trial, Mr. Nosal moved to dismiss the CFAA counts. He argued that the CFAA does not cover acts of misappropriation. The district court initially denied the motion. After this Court issued its decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), however, Mr. Nosal filed a motion to reconsider, and the district court dismissed some (but not all) of the CFAA counts.[5]

The government appealed. On April 28, a divided three-judge panel of this Court reversed the district court's ruling and reinstated the dismissed CFAA counts. Judge Trott authored the opinion, joined by Judge O'Scannlain. District Judge Campbell, sitting by designation, dissented.

REASONS FOR GRANTING REVIEW

A. Review is Necessary to Resolve an Intra-Circuit Conflict

Review is necessary to resolve the conflict between the holding in this case and this Court's prior holding in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127

[5] The district court dismissed the CFAA counts alleging that a Korn/Ferry employee entitled to access the Korn/Ferry computers had done so for an impermissible purpose, but refused to dismiss the CFAA counts which alleged the access had been accomplished by a person no longer employed by Korn/Ferry.

(9th Cir. 2009). The CFAA forbids persons from accessing computers and obtaining information *either* without authorization *or* in excess of their authorization. *See* 18 U.S.C. § 1030(a)(1)-(4). In this circuit, there are now two different definitions of the "exceeds authorized access" prong of the CFAA. There is the definition adopted by the majority in this case, and then there is the different definition adopted by the three-judge panel in *Brekka*.

Brekka was a unanimous opinion authored by Judge Ikuta. According to *Brekka*:

> [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.

581 F.3d at 1133. Under the *Brekka* definition, Mr. Nosal could not be found guilty of the relevant counts, because his accomplices had permission to access the information that they allegedly misappropriated.

Apparently dissatisfied with the *Brekka* definition, the majority in this case created a new definition:

> [T]he 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.

Slip op. at 5531. Under the majority's new definition, Mr. Nosal could be found

guilty, because his accomplices allegedly violated the limitations on the use of information that they obtained.

Of course, the CFAA contains its own definition of "exceeds authorized access." It states that "exceeds authorized access" means to "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." 18 U.S.C. § 1030(e)(6). The *Brekka* definition closely tracks the statutory definition. The majority's definition in this case, by contrast, imports a misappropriation theory of liability into the statutory definition. The majority's definition is dubious as a matter of statutory interpretation,[6] but merits aside, the more important point is simply that the majority's definition creates an intra-circuit conflict.

---

[6] The majority imported a misappropriation theory into the statute through a single two-letter word in § 1030 (e)(6): "so."

According to the majority, the word "so" in § 1030(e)(6) means "in a manner or way that is indicated or suggested." Slip op. at 5528 (quoting *Webster's Third New Int'l Dictionary* 2159 (Philip Babcock Gove, ed. 2002)). But the word "so" has many other meanings. It can mean "thus" or "in this way," or it can simply function as an "introductory particle," or it can be "used to add emphasis" or "used to strengthen or confirm a previous statement." *See* XV *Oxford English Dictionary* 886-88 (2d ed. 1989). The majority never explained why it chose one definition of "so" and ignored all other possibilities. To support its desired result, the majority simply engaged in "cherry-pick[ing] dictionary definitions." *Silveira v. Lockyer*, 328 F.3d 567, 573 (9th Cir. 2003) (Kleinfeld, J., dissenting from denial of rehearing en banc).

The majority here did not seriously attempt to reconcile its definition with *Brekka's* definition. Rather, it contended that its definition was consistent with *Brekka's* "core rationale." Slip op. at 5532. According to the majority, *Brekka's* "core rationale" was that employers had some ability to define the scope of access. But what the majority here ignored was the actual holding of *Brekka* — namely, that employers can define the permissible scope of *access* to information, but not the permissible scope of *subsequent use* of that information. In short, the majority's decision was not consistent with *Brekka's* ultimate holding.

En banc review is therefore necessary to resolve the conflict and maintain uniformity of this Court's decisions.

B. Review is Necessary to Clarify the Scope Not Just of Section 1030(a)(4), But Also of Section 1030(a)(2)

Uniformity of precedent aside, review is appropriate to settle an important issue of law. The majority endorsed an extraordinarily broad theory of civil and criminal liability under the CFAA. The majority held that an employee who violates her employer's limitations on computer use "exceeds authorized access" under the CFAA. Given that employers routinely limit authorized computer use to official company business only, the majority's construction of the CFAA gives the statute a frighteningly vast reach.

The majority responded to such concerns this way:

> We do not dismiss lightly Nosal's argument that our decision will make criminals out of millions of employees who might use their work computers for personal use, for example, to access their personal email accounts or to check the latest college basketball scores. But subsection (a)(4) does not criminalize the mere violation of an employer's use restrictions. . . . The requirements of a fraudulent intent and of an action that furthers the intended fraud distinguish this case from the Orwellian situation that Nosal seeks to invoke. 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).

Slip op. at 5533-34.

Given the broad legal definition of "fraudulent intent," however, the majority's response to what it agrees is an "Orwellian" prospect does not put that specter to rest. Worse yet, the majority utterly ignored the implications of its decision for other provisions of the CFAA, especially § 1030(a)(2).

1. The Scope of Section 1030(a)(2).

Like subdivision (a)(4), subdivision (a)(2) of the CFAA makes it a crime to obtain information from a computer by exceeding authorized access. Unlike subdivision (a)(4), subdivision (a)(2) contains no requirement of fraudulent intent. Subdivision (a)(2) simply states that anyone who "exceeds authorized access" and

obtains information from a protected computer[7] is guilty of a crime.

Thus, under the majority's definition of "exceeds authorized access," simply using a work computer in a manner that violates an employer's use restrictions, without anything more, *is* a crime under the CFAA. Under the majority's construction of the statute, literally tens of millions of employees who use their work computers to access personal email accounts or check basketball scores are now guilty of a federal crime under § 1030(a)(2).

It is true that unlike violations of subdivision (a)(4), violations of subdivision (a)(2) are — for the moment[8] — sometimes only misdemeanors. *See* 18 U.S.C. § 1030(c)(2)(A). But violations of subdivision (a)(2) are felonies any time that the person accessed the computer for "private financial gain." *Id*. § 1030(c)(2)(B)(i). Thus, if an employer states that a computer may only be used for company business, and an employee uses it to participate in an NCAA pool, the employee is guilty of a felony. Violations of subdivision (a)(2) are also felonies

---

[7] For the purposes of the CFAA, a "protected computer" is any computer involved in interstate commerce.

[8] The Obama Administration recently proposed amendments to the CFAA that would, among other things, make all (a)(2) violations felonies. Office of Mgmt. & Budget, Executive Office of the President, OMB Letter, Law Enforcement Provisions Related to Computer Security (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

anytime that the defendant accessed the computer "in furtherance of any . . . tortious act." *Id*. § 1030(c)(2)(B)(ii). Thus, to convert a garden-variety CFAA violation into a felony, the government need only find some theory of tort liability. The majority's interpretation of "exceeds authorized access" creates both civil and criminal liability for a wide variety of innocuous behavior.

These concerns are not merely theoretical. In a recent federal civil case in Florida, for example, a woman named Wendi Lee sued her employer for discrimination. The employer filed a counterclaim under the CFAA, alleging that the Ms. Lee violated company policy because she checked Facebook and sent personal email with her company computer. *Lee v. PMSI, Inc.*, No. 8:10–CV–2904, 2011 WL 1742028 (M.D. Fla., May 6, 2011). The district court in Florida wisely dismissed those counterclaims, relying in part on this Court's ruling in *Brekka*. *Id*. at *2. But now, in this Circuit, Wendi Lee's "excessive internet usage" would not only be actionable in a civil case — it would also constitute a federal crime.

Nor are the implications of this case limited to the employment context. If violating an employer's limitations on use constitutes exceeding authorized access, then violating a website operator's limitations on use also constitutes exceeding authorized access. Thus, under the majority's rationale, any person

who violates the (often highly restrictive) Terms of Service for a website also violates the CFAA. In this Circuit, Lori Drew was prosecuted for cyber-bullying on just such a theory. The charges against Drew were dismissed, *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), but after the decision in this case, terms of service cases are now actionable, both civilly and criminally, under the CFAA.

It is thus remarkable that the majority never discussed, or even mentioned, the implications of its ruling for subdivision (a)(2) of the CFAA. Its interpretation of "exceeds authorized access" applies just as much to that provision as it does to subdivision (a)(4). And the majority's interpretation could subject literally tens of millions of citizens to civil and criminal liability. Such an important ruling deserves greater consideration.

2. The Scope of Section 1030(a)(4)

Moreover, even for subdivision (a)(4), the limitation to cases involving "fraudulent intent" is cold comfort to anyone concerned about the potentially vast scope of the CFAA. As this Court's model jury instructions state, an "intent to defraud" is simply "an intent to deceive or cheat." Ninth Circuit Manual of Model Jury Instructions — Criminal § 3.16 (2010). Nothing more is required. When employees close their office doors to secretly use their company computers for forbidden personal purposes, they deceive their employers. When employees turn

in time sheets for eight hours of work on a day when they spent sixty minutes of office time on You Tube, their false statement deprive their employers of something of monetary value — namely, an hour's wages.[9] Even in a post-*Skilling* world, such conduct easily could be alleged to constitute fraud.[10] If the government does not pursue such a theory in this case, it no doubt will do so soon.

For better or worse, this Court has always "construed fraud broadly." *United States v. Jones*, 472 F.3d 1136, 1140 n.3 (9th Cir. 2007). In the employment context, this Court long ago held that "employee disloyalty can constitute a violation of the mail fraud statute." *United States v. Bohonus*, 628 F.2d 1167, 1172 (9th Cir. 1980). Shortly before the Supreme Court's decision *Skilling*, this Court stated that an employee commits fraud when he "deprives his employer of its right to have its affairs conducted 'free from deceit, fraud, dishonesty, conflict of interest, and self-enrichment,' and consistent with the employee's fiduciary duties to the employer." *United States v. Kincaid-Chauncey*,

---

[9] An estimate, reported in, among other publications, the New York Times, Washington Post, and Boston Globe, by John A. Challenger, CEO of Challenger, Grey, and Christmas, put the cost of lost wages caused by internet viewing of the 2006 NCAA "March Madness" tournament at 3.8 billion dollars.

[10] *Cf.* Alex Kozinski & Misha Tseytlin, *You're (Probably) a Federal Criminal*, *in* In the Name of Justice 43, 46 (Timothy Lynch, ed. 2009) ("Have you ever violated your employee code of conduct? Maybe you should reach into your desk drawer and take a look.").

556 F.3d 923, 939 (9th Cir. 2009).

While this line of cases has been limited by *Skilling*, it is unclear what the exact nature of those limitations will be. At least some judges on this Court have recognized that "not every breach of contract," employment or otherwise, can constitute fraud. *United States v. Milovanovic*, 627 F.3d 405, 413-15 (9th Cir. 2010) (Fernandez, J., dissenting). But this Court has never fashioned any limiting principle that would prevent easy application of fraud concepts to garden-variety employee misconduct. After all, if any employee deceives in any way his employer in order to keep getting a salary — that is, in order to keep obtaining money or property — he has committed fraud.

In sum, the majority's broad interpretation of "exceeding authorized access" has wide-reaching ramifications, in both civil and criminal cases, for several provisions of the CFAA. The proper scope of those provisions is a question of exceptional importance that merits en banc review.

C. Review is Necessary to Clarify the Mens Rea Requirement

Perhaps in an attempt to limit the stunning reach of its ruling, the majority almost off-handedly appeared to create a new mens rea requirement for the crime. After discussing the scope of the CFAA and the meaning of "exceeds authorized access," the majority offered this conclusion:

> Therefore, *as long as the employee has knowledge of the employer's limitations on that authorization*, the employee "exceeds authorized access" when the employee violates those limitations. It is as simple as that.

Slip op. at 5530 (emphasis added). The majority thus apparently held that a defendant's knowledge of an employer's limitations is essential — that knowledge is an essential element of the offense. The majority, in other words, created a new mens rea element.

That holding is problematical for several reasons. First, while a mens rea requirement limiting the reach of the CFAA might make sense, it is not mentioned in the text of the statute, and it does not find substantial support in the existing case law. It had not been briefed or argued by either party.

More importantly, the majority's casual creation of a new mens rea element will create countless difficulties for future cases. Among other things: (a) it is unclear whether the mens rea requirement applies to criminal cases only, or also to civil cases; (b) it is unclear whether a computer user must simply know that use limitations exist, or whether she must also know the content of those limitations — it is unclear, for example, whether an employee who checks a box stating "I accept the terms of use" without reading those terms is deemed to have knowledge; (c) it is unclear what steps, if any, a computer owner must take to

communicate use restrictions to a user;[11] (d) it is unclear how jury instructions should describe the mens rea requirement.

Furthermore, in this case, the indictment did not contain an allegation of knowledge. If this case returns to the district court in its present posture, Mr. Nosal will once again move to dismiss the indictment for failure to allege an essential element of the offense — namely knowledge of the employer's limitations. The government will no doubt argue that no such element exists. It will argue that the majority's suggestion about the necessity of an employer's knowledge was merely an aside, an ill-considered digression, a bit of dicta.

In short, for this case, and for all future CFAA cases, it is not even clear whether there is a knowledge requirement, much less what that knowledge requirement might mean. Because the majority's mens rea requirement was derived from the definition of "exceeds authorized access" itself, it would apply not just to cases brought under subdivision (a)(4), but also to cases brought under subdivisions (a)(1) and (a)(2). It would thus affect many cases, civil and criminal. The existence and scope of the knowledge requirement is another exceptionally

---

[11] In this case, the majority noted that the employer had "placed clear and conspicuous restrictions on the employees' access" to computers and databases. Slip op. at 5531. The factual basis for this statement is unclear, since the nature of the restrictions was not described in the indictment. More importantly, as a legal matter, it is unclear whether "clear and conspicuous restrictions" are required.

important question, which merits en banc review.

D. Review is Necessary to Consider the Constitutionality of the CFAA

In his briefing to the three-judge panel, Mr. Nosal argued, as a matter of statutory interpretation, that a narrower interpretation of the CFAA was proper. In addition, Mr. Nosal also presented a constitutional argument. He argued that a broad interpretation of "exceeds authorized access" would render the CFAA unconstitutionally vague.

Other courts and commentators have recognized the serious constitutional problems that a misappropriation or misuse theory of the CFAA would create. *See, e.g.*, *United States v. Drew*, 259 F.R.D. 449, 463-68 (C.D. Cal. 2009) (holding that the statute violates the vagueness doctrine); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1585-87 (2010) (arguing that the vagueness doctrine requires rejection of the misappropriation theory of employee liability under the CFAA).

The dissent found these constitutional objections meritorious. "If every employee who used a computer for personal reasons and in violation of her employer's computer use policy were guilty of a federal crime, the CFAA would lend itself to arbitrary enforcement, rendering it unconstitutionally vague." Slip

Op. at 5537. The majority, however, did not address Mr. Nosal's constitutional arguments. The constitutionality of the CFAA is an exceptionally important question, which merits en banc review.

CONCLUSION

For the reasons stated, rehearing en banc should be granted.

Dated: June 13, 2011

Respectfully submitted,

RIORDAN & HORGAN

DENNIS P. RIORDAN
DONALD M. HORGAN
TED SAMPSELL-JONES

By /s/ Dennis P Riordan
DENNIS P. RIORDAN
Attorneys for Defendant
DAVID NOSAL

CERTIFICATION REGARDING BRIEF FORM

I, Dennis P. Riordan, hereby certify that the foregoing brief is proportionately spaced, has a typeface of 14 points, and contains 3,958 words.

Dated: June 13, 2011

/s/ Dennis P. Riordan
DENNIS P. RIORDAN

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the
Appellate CM/ECF System

I hereby certify that on June 13, 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.

Signature: /s/ Jocilene Yue
Jocilene Yue

****

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the
Appellate CM/ECF System

I hereby certify that on_____, 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.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature: _____
Jocilene Yue

No. 10-10038

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

DAVID NOSAL,

Defendant-Appellee.

OPPOSITION TO PETITION FOR REHEARING EN BANC

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
DISTRICT COURT NO. 08-CR-00237-EMC

LANNY A. BREUER
Assistant Attorney General
U.S. Department of Justice
Criminal Division

JENNY C. ELLICKSON
Trial Attorney
U.S. Department of Justice
Criminal Division
Computer Crime & Intellectual
Property Section
1301 New York Ave., N.W. Suite 600
Washington, DC 20530
Phone: (202) 305-1674

MELINDA HAAG
United States Attorney

BARBARA J. VALLIERE
Chief, Appellate Division
Assistant United States Attorney

KYLE F. WALDINGER
Assistant United States Attorney
450 Golden Gate Ave., 11th Floor
San Francisco, CA 94102
Phone: (415) 436-6830

Attorneys for Plaintiff-Appellant
UNITED STATES OF AMERICA

Dated: July 20, 2011

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

STATUTES AND RULES

OTHER SOURCES

OPPOSITION TO PETITION FOR REHEARING EN BANC

A grand jury has charged David Nosal with several violations of 18 U.S.C. § 1030(a)(4), a provision of the Computer Fraud and Abuse Act ("CFAA") that makes it a crime to knowingly and with intent to defraud exceed authorized access and by means of such conduct further the intended fraud and obtain anything of value. The panel correctly concluded that an employee "exceeds authorized access" when he violates the employer's restrictions on his computer access, as the government alleges that Nosal's accomplices did in this case. The panel's decision is consistent with the Court's prior decisions, and it is correct as a matter of statutory interpretation. Furthermore, the panel properly rejected Nosal's constitutional vagueness argument as applied to Nosal and properly declined to speculate about how its decision would apply to hypothetical cases. Because Nosal has failed to demonstrate that en banc review is necessary to maintain uniformity of this Court's decisions or to resolve a question of exceptional importance, the Court should deny his petition for rehearing en banc.

BACKGROUND

In 2008, a federal grand jury returned a 20-count superseding indictment that charges Nosal with violating several criminal statutes. Counts 2 through 9 of the indictment allege that Nosal's accomplices – and Nosal himself, as an aider and abettor – violated 18 U.S.C. § 1030(a)(4) when they accessed the computer system

of their employer, Korn/Ferry International ("Korn/Ferry"), for the purpose of defrauding Korn/Ferry and helping Nosal set up a competing business, in violation of a computer use policy that restricted their access both to the system in general and to Korn/Ferry's proprietary database in particular. *United States v. Nosal*, 642 F.3d 781, 782-83, 787 (9th Cir. 2011). Before trial, Nosal moved to dismiss the indictment, arguing in part that his accomplices could not have "exceeded authorized access" within the meaning of the CFAA because they had permission to access Korn/Ferry's computer systems, including the information at issue, under certain circumstances. *Id.* at 783. The district court ultimately agreed with Nosal as to Counts 2 and 4-7 and dismissed these counts. *Id.* at 784.

The government filed an interlocutory appeal, and on April 28, 2011, the panel issued a 2-1 published decision reversing the district court's dismissal of Counts 2 and 4-7 and reinstating those counts for trial. The panel explained that the question on appeal was whether Nosal's accomplices "could have *exceeded* their authorized access by accessing information that they were entitled to access only under limited circumstances." *Id.* (emphasis in original). The panel answered this question in the affirmative, holding that "an employee 'exceeds authorized access' under § 1030 when he or she violates the employer's computer access

restrictions – including use restrictions." *Id.* Nosal now petitions the Court for rehearing en banc.

ARGUMENT

Rehearing en banc is warranted only to maintain uniformity among Circuit decisions or to address questions of exceptional importance. Fed. R. App. P. 35(a); Ninth Cir. R. 35-1. En banc hearings are disfavored, *United States v. Wylie*, 625 F.2d 1371, 1378 n.10 (9th Cir. 1980), and should be "rare exceptions." *United States v. Burdeau*, 180 F.3d 1091, 1092 (9th Cir. 1999) (Tashima, J., concurring in order denying rehearing en banc). Here, the panel's decision is consistent with the Court's recent decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), and Nosal does not identify any other decision from the Supreme Court, this Court, or any other court of appeals that conflicts with the panel's decision. Moreover, the issues involved are not of exceptional importance: the panel considered and correctly rejected Nosal's argument that § 1030(a)(4) is unconstitutional, and it properly refrained from deciding issues that are not presented by this case. Accordingly, the Court should deny Nosal's petition for rehearing en banc.

I. The Panel's Determination Is Consistent With This Court's Decision in *LVRC Holdings LLC v. Brekka*

The panel properly held that an employee "exceeds authorized access" under 18 U.S.C. § 1030 when he or she violates the employer's computer access restrictions. *Nosal*, 642 F.3d at 785. In so doing, the panel rejected Nosal's claim that a computer user could exceed authorized access only by accessing information that he or she is completely prohibited from accessing under any circumstances. The panel therefore resolved a question left unanswered by *LVRC Holdings LLC v. Brekka*, and did so in a way that was wholly consistent with *Brekka*. Because there is no conflict between the panel's decision and *Brekka* or any other decision of this Court, en banc review is not necessary to maintain uniformity of the Court's decisions.

As the panel recognized, there is "a substantial factual distinction" between this case and *Brekka*. *Nosal*, 642 F.3d at 787. In this case, the government alleges that Nosal's accomplices were subject to "clear and conspicuous restrictions" on their computer access, and that they violated those restrictions. *Id.* In *Brekka*, by contrast, the defendant-employee "had unfettered access to the company computer" and therefore "had not acted in a way that violated any access restrictions." *Id.*; *see also Brekka*, 581 F.3d at 1129, 1133, 1135. Instead, the plaintiff in *Brekka* argued that the defendant lost any authority to access the plaintiff's computers once he

breached his implicit duty of loyalty to the plaintiff, thereby rendering his subsequent accesses "without authorization" for purposes of the CFAA. *See id.* at 1133-34.

The *Brekka* panel rejected the plaintiff's "without authorization" argument and held that, under the plain language of the CFAA, "'authorization' depends on actions taken by the employer," and does not turn on whether the defendant breached a state duty of loyalty to an employer. *Id.* at 1135. The *Brekka* panel further held that "a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose . . . , or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id.* at 1135. Although Nosal claims that "the actual holding of *Brekka*" is that "employers can define the permissible scope of *access* to information, but not the permissible scope of *subsequent use* of that information," Pet. 8 (emphasis in original), *Brekka* does not include such a holding. In fact, *Brekka* does not even discuss employer restrictions on the subsequent use of information, perhaps because the employer in *Brekka* had imposed no such restrictions. *See Brekka*, 581 F.3d at 1129 (no prohibitions on emailing company documents to personal computers); *id.* at 1132

(no evidence that employee had agreed to keep documents confidential, or to return or destroy those documents).

Because there were no access restrictions in *Brekka*, and no allegations that the defendant had exceeded authorized access, *Brekka* did not address the question before the panel in this case: "whether [computer users] could have *exceeded* their authorized access by accessing information that they were entitled to access only under limited circumstances." *Nosal*, 642 F.3d at 785 (emphasis in original). Accordingly, the panel correctly began its analysis of this question by examining the definition of "exceeds authorized access" in 18 U.S.C. § 1030(e)(6). *See id.* As discussed in Part II, *infra*, the panel correctly found that the plain language of § 1030(e)(6) resolved the question on appeal in the government's favor, but it did not end its analysis there. Instead, the panel discussed *Brekka* at length and concluded that its decision in this case was "simply an application of *Brekka*'s reasoning." *Id.* at 787.

In particular, *Brekka* explained that the employer's actions determine the scope of an employee's authorization to access a company computer, holding that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee *permission to use* it."[1] *Brekka*, 581 F.3d at

---

1 To the extent that Amicus argues that employer actions should not define the scope of authorization under the CFAA, *see* Amicus Br. at 1, 11, 12, 16, 18,

1133 (emphasis added). The panel quoted this language from *Brekka* and then held that "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*, 642 F.3d at 787 (emphasis in original). This holding is wholly consistent with *Brekka*.

Despite the panel's extensive reliance on *Brekka*, Nosal argues that the panel's decision conflicts with *Brekka* because of *Brekka*'s statement 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." Pet. 6 (quoting *Brekka*, 581 F.3d at 1133). However, this sentence is consistent with the panel's decision in this appeal. When an employee violates or "exceeds" limitations that the employer has placed on her authority to access a computer, any information that the employee obtains during that computer access is "information on the computer that the person is not entitled to access." *Brekka*, 581 F.3d at 1133. The hypothetical possibility that the employee might have been entitled to access the same information in other circumstances – *e.g.*, when she had a legitimate business purpose for doing so – does not mean that she is entitled to

---

Amicus appears to be asking the Court to overturn both *Brekka* and the panel's decision.

obtain this information when she accesses her employer's computer in violation of the employer's access restrictions.

Nosal also argues that the panel's decision conflicts with what he claims is "the actual holding of *Brekka*" – "that employers can define the permissible scope of *access* to information, but not the permissible scope of *subsequent use* of that information." Pet. 8 (emphasis in original). As discussed above, *Brekka* does not include such a holding. However, even if it did, there would be no conflict between that holding and the panel's decision in this appeal. The government is not arguing that Nosal and his co-conspirators exceeded authorized access because they misused computer data that they had been authorized to obtain. *See* Gov't Reply at 2-3. Accordingly, the panel did not discuss whether Nosal and his co-conspirators could have exceeded authorized access by accessing information with authorization and then subsequently using that information for a prohibited purpose.[2] Instead, the panel found that Nosal's accomplices could have exceeded

---

2 Nosal's belief that the panel's decision is based on restrictions on the subsequent use of information, rather than restrictions on access, may stem from the panel's repeated references to "use restrictions." *See, e.g.*, *Nosal*, 642 F.3d at 784, 785. However, the panel simply used the term "use restrictions" to reference the type of access restrictions at issue here – *i.e.*, restrictions that allow employees to access certain information on their work computers only for legitimate business purposes, and not for other uses. *See id.* at 784 ("The district court stated that intent is irrelevant . . . , even if an employee's access to the computer is expressly limited by the employer's use restrictions."); *id.* at 785 (referring to "the employer's computer access restrictions – including use restrictions"). Furthermore, to the

authorized access by violating Korn/Ferry's access restrictions, which "placed clear and conspicuous restrictions on the employees' access both to the system in general and to the Searcher database in particular." *Nosal*, 642 F.3d at 787.

For all of these reasons, the panel's decision is consistent with *Brekka*. The panel's decision does not disturb the reasoning in *Brekka* at all, nor would it require a different outcome in a case that presents the same facts as *Brekka*. Nosal identifies no other decisions of this Court, the Supreme Court, or any other circuit that conflict with the panel's decision. Therefore, en banc review is not necessary to maintain uniformity of this Court's decisions.

II. The Panel Correctly Interpreted 18 U.S.C. § 1030(e)(6)

The panel's decision correctly interprets the plain text of 18 U.S.C. § 1030(e)(6), which 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 accesser is not entitled *so* to obtain or alter." 18 U.S.C. § 1030(e)(6) (emphasis added). Before the panel, Nosal argued that this definition encompasses only situations where the accesser has obtained information that the

---

extent that the panel occasionally employs "use" as a synonym for "access," its terminology is consistent with *Brekka*, which held that "to access a company computer" means "to use it." *See Brekka*, 581 F.3d at 1133 ("[A]n employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it.").

accesser is *never* entitled to access, under any circumstances. *See* Def. Resp. at 10-11. However, the panel rejected Nosal's argument and correctly held that an employee exceeds authorized access "when that access violates the employer's access restrictions," including restrictions that give the employee limited access to information on the computer.[3] *Nosal*, 642 F.3d at 789.

In reaching this conclusion, the panel noted that Nosal's interpretation of § 1030(e)(6) would render superfluous the word "so" in the statutory definition. *Id.* at 785-86. The panel explained that, in context of § 1030(e)(6), the word "so" means "in a manner or way that is indicated or suggested," which in turn means that an employee exceeds authorized access by using her authorized access "to obtain or alter information in the computer that the accesser is not entitled [in that manner] to obtain or alter." *Id.* (alteration in original).

Neither the dissent nor Nosal offers a convincing alternative interpretation of "so." The dissent suggests that this word "could have been added for emphasis alone." *Id.* at 791. However, this interpretation gives "so" no independent meaning or significance, which improperly renders this word superfluous or

---

3 As the panel observed, its interpretation of "exceeds authorized access" is consistent with decisions from the Fifth and Eleventh Circuits. *See Nosal*, 642 F.3d at 788 (citing *United States v. John*, 597 F.3d 263 (5th Cir. 2010), and *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010)).

insignificant. *See Corley v. United States*, 129 S. Ct. 1558, 1566 (2009). Furthermore, it is difficult to see how the word "so" adds emphasis either to § 1030(e)(6) or to § 1030(a)(1), another CFAA provision that the dissent invokes to support its interpretation. Indeed, "so" has the same meaning in § 1030(a)(1) as it does in § 1030(e)(6) – the phrase "so obtained" in § 1030(a)(1) plainly means "in that manner obtained." 18 U.S.C. § 1030(a)(1).

Nosal does not embrace the dissent's interpretation of "so" and instead observes that the word has "many" possible meanings. Pet. 7 n.6. However, two of the alternative definitions that Nosal mentions – "thus" or "in this way" – are essentially the same as the panel's definition, and the other three make no sense in the context of the statute.[4] *See id.* The mere existence of multiple dictionary definitions for "so" does not render this word ambiguous in § 1030(e)(6), particularly because its context in the statute favors the panel's definition. *See*

---

4 *Compare* Pet. 7 n.6 (citing XV *Oxford English Dictionary* 886-88 (2d ed. 1989)) (". . . ['so'] can simply function as an 'introductory particle,' or it can be 'used to add emphasis' or 'used to strengthen or confirm a previous statement."), *with Oxford English Dictionary* (2d ed. 1989), *available at* http://www.oed.com (providing examples of "so" as an introductory particle, including: "So, let me see: my apron," and "So, so, ma'am! I humbly beg pardon."), *and id.* (explaining that "so" can be "[u]sed to add emphasis to a statement contradicting a negative assertion made by the previous speaker," as in the exchange "'You don't know anything about it!' 'I do *so*!'") (emphasis in original), *and id.* (providing examples where "so" is "[u]sed to strengthen or confirm a previous statement," including "My father's birthday? Why, so it is!" and "You wanted my love – is that much true? And so I did, love, so I do.").

Ayres v. Prudential Ins. Co. of America, 602 F.2d 1309, 1311 (9th Cir. 1979) ("To find that a word or phrase isolated from its context is susceptible to more than one meaning, or that a word or phrase in its context is susceptible to one reasonable and one unreasonable meaning, does not spell ambiguity.").

Finally, although the panel addressed only the statutory definition of "exceeds authorized access," the legislative history of the CFAA also confirms the plain meaning of this statutory text. Congress added this term and definition to the CFAA to "simplify the language" of the existing statute by substituting "exceeds authorized access" for a "more cumbersome" phrase from the 1984 statute: "or having accessed a computer with authorization, uses the opportunity such access provides *for purposes* to which such authorization does not extend." S. Rep. No. 99-432, pt. 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486 (emphasis added). In making this substitution, Congress expressed no desire to change the reach of the original language, which would plainly encompass the charged conduct in this case. *See* Gov't Br. at 16-18; Gov't Reply at 10-14. This additional justification for the panel's decision also militates against granting rehearing en banc.

III. The Panel Properly Rejected Nosal's Constitutional Arguments As Applied To § 1030(a)(4), And En Banc Review Is Not Necessary To Clarify The Scope Of This Provision

Before the panel, Nosal argued that the government's interpretation of "exceeds authorized access" would render the CFAA unconstitutionally vague because "the statute would cover a remarkably broad range of conduct, including conduct that is not seriously culpable." Def. Resp. at 18. Nosal now claims that the panel did not address this constitutional argument, and that en banc review is warranted because the constitutionality of the CFAA is an exceptionally important question. Pet. 18. However, the panel did consider Nosal's constitutional argument and properly rejected it as applied to § 1030(a)(4), the provision with which Nosal has been charged. *Nosal*, 642 F.3d at 788-89. Because the panel was required to consider Nosal's vagueness challenge "as applied to the particular facts at issue," *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2719 (2010), the panel properly declined to consider Nosal's vagueness challenge as applied to § 1030(a)(2), a provision with which Nosal has not been charged.

With respect to § 1030(a)(4), the panel rejected Nosal's constitutional argument because it concluded that this provision does not have the broad reach that Nosal claimed. In particular, the panel noted that § 1030(a)(4) "does not criminalize the mere violation of an employer's use restrictions," but instead

requires that an employee exceed authorized access with fraudulent intent and thereby further the intended fraud and obtain something of value. *Nosal*, 642 F.3d at 788; *see also* 18 U.S.C. § 1030(a)(4). Because Nosal's vagueness argument was therefore based on a faulty premise, the panel had no need to decide whether there was merit to Nosal's claim that a statute would be unconstitutionally vague if it criminalized "a remarkably broad range of conduct, including conduct that is not seriously culpable." Def. Resp. at 18.

Nosal now argues that § 1030(a)(4)'s fraudulent intent requirement is so broad that § 1030(a)(4) could theoretically criminalize "garden-variety employee misconduct." Pet. 14. As an initial matter, Nosal cites no legal authority for the proposition that a statute may not criminalize "garden-variety employee misconduct," nor is it clear that § 1030(a)(4) would even cover such misconduct. More importantly, Nosal does not argue – nor could he – that the alleged conduct in this case is "garden-variety employee misconduct" akin to watching a YouTube video behind closed doors. Instead, the indictment alleges that Nosal and his accomplices accessed Korn/Ferry's proprietary database of executive candidates and obtained information about at least 1,500 executives for the purpose of furthering Nosal's competing business. *See* Gov't Excerpts of Record ("ER") 29-31. Because Nosal's argument about the scope of § 1030(a)(4) is therefore based

on hypothetical applications of § 1030(a)(4), rather than the facts of his own case, his vagueness argument must fail. *See Humanitarian Law Project*, 130 S. Ct. at 2721 (declining to address plaintiffs' hypothetical arguments about the meaning of "training" and "expert advice or assistance" because plaintiffs "cannot seek refuge in imaginary cases").

In the alternative, Nosal argues that en banc review is necessary to clarify the panel's statement that an employee must know about the employer's limitations on authorization in order to be liable for "exceeding authorized access" under the CFAA. *See* Pet. 14-17. Nosal does not explain why this clarification, if needed, would require rehearing en banc, rather than rehearing by the panel, which Nosal does not request. In any event, there is nothing novel about the panel's recognition that the CFAA imposes liability only on employees who knowingly or intentionally exceed authorized access, notwithstanding Nosal's claim that the panel's statement about knowledge "created a new mens rea element." *Id.* at 15. In fact, the plain text of § 1030(a)(4) requires that a defendant exceed authorized access "knowingly," 18 U.S.C. § 1030(a)(4), and the indictment in this case already alleges this knowledge.[5] *See* ER 31 (". . . the defendants . . . did knowingly

---

5 The other two CFAA provisions that use the term "exceeds authorized access" also require that a defendant do so knowingly or intentionally. *See* 18 U.S.C. § 1030(a)(1) (requiring knowledge); 18 U.S.C. § 1030(a)(2) (requiring intent).

. . . access a protected computer belonging to Korn/Ferry, . . . by exceeding authorized access . . .”). The panel’s decision simply recognized this existing knowledge requirement and did not, as Nosal claims, “create a new mens rea requirement.”[6] Pet. 14. Accordingly, en banc review is not necessary to clarify the scope of the knowledge requirement in § 1030(a)(4).

IV. En Banc Review Is Not Warranted To Clarify How The Panel’s Decision Would Apply To 18 U.S.C. § 1030(a)(2), A Provision With Which Nosal Has Not Been Charged

Even though the panel’s decision is clear as applied to Nosal and his co-conspirators, Nosal argues that this Court should rehear his § 1030(a)(4) case in order to “clarify the scope” of § 1030(a)(2). Pet. 8. But this case includes no § 1030(a)(2) charge. Nosal does not explain how “clarifying” § 1030(a)(2) would affect the outcome of his case, nor does he cite any law to support his suggestion that en banc review is necessary to clarify the scope of an uncharged statute. In short, Nosal does not show that *this* proceeding presents an exceptionally important question about the scope of § 1030(a)(2), *see* Fed. R. App. P. 35(b)(1)(B), or even an Article III case or controversy involving this uncharged provision. *See Alvarez v. Smith*, 130 S. Ct. 576, 580-81 (2009) (“[A] dispute solely

---

6 Neither party raised the scope of § 1030(a)(4)’s knowledge requirement before the district court or the panel. *See Lassiter v. City of Bremerton*, 556 F.3d 1049, 1054 n.5 (9th Cir. 2009) (declining to consider argument that was not raised in the district court).

about the meaning of a law, abstracted from any concrete actual or threatened harm, falls outside the scope of the constitutional words 'Cases' and 'Controversies.'"). Accordingly, Nosal has no standing to ask the Court to "clarify" § 1030(a)(2), just as he cannot ask the Court to issue an advisory opinion about the scope of the bank fraud statute or any other statute with which he has not been charged.

The panel properly declined to consider hypothetical § 1030(a)(2) cases suggested by Nosal and Amicus that are designed to test the limits of "exceeds authorized access." "Whatever force these arguments might have in the abstract, they are beside the point here." *Humanitarian Law Project*, 130 S. Ct. at 2721. Indeed, if this Court were to accept Nosal's invitation to "clarify" a charge that Nosal does not face, the Court would have to make premature and speculative judgments about the meaning of elements in § 1030(a)(2) that do not appear in § 1030(a)(4). For example, § 1030(a)(2) requires that a defendant "intentionally" exceed authorized access, a mens rea requirement that does not appear in § 1030(a)(4).[7] *Compare* 18 U.S.C. § 1030(a)(2) *with* 18 U.S.C. § 1030(a)(4). In

---

7 Nosal overlooks this intent requirement when he claims that § 1030(a)(2) "simply states that anyone who 'exceeds authorized access' and obtains information from a protected computer is guilty of a crime." Pet. 9-10 (footnote omitted). The dissent makes the same mistake. *See Nosal*, 642 F.3d at 789 (stating that § 1030(a)(2)(C) "*has no intent requirement*") (emphasis in original).

order to "clarify" how § 1030(a)(2) would apply to Nosal's hypothetical cases, the Court would first have to decide what it means to "intentionally" exceed authorized access under § 1030(a)(2). In addition to being speculative, this discussion would be wholly irrelevant to Nosal's own case, as § 1030(a)(4) does not require that a defendant "intentionally" exceed authorized access.

CONCLUSION

For the foregoing reasons, the petition for rehearing en banc should be denied.

Dated: July 20, 2011

/s/

JENNY C. ELLICKSON
Trial Attorney
U.S. Department of Justice
Criminal Division
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W. Suite 600
Washington, DC 20530
Phone: (202) 305-1674

CERTIFICATE OF COMPLIANCE

Pursuant to Ninth Circuit Rule 35-4 and 40-1, I certify that the attached response to a petition for panel rehearing and rehearing *en banc* is:

X Proportionately spaced, has a typeface of 14 points or more, and contains 4,187 words, which is fewer than 4,200 words; or,

__ Monospaced, has 10.5 or fewer characters per inch, and contains ____ words or ___ lines of text; or,

__ In compliance with Rule 32(c) of the Federal Rules of Appellate Procedure and not exceeding 15 pages.

DATED: July 20, 2011

/s/
JENNY C. ELLICKSON
Trial Attorney
U.S. Department of Justice
Criminal Division

CERTIFICATE OF SERVICE

I hereby certify that on July 20, 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.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days, to the following non-CM/ECF participants:

_____

Hanni M. Fakhoury
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

/s/
TYLE L. DOERR
Appellate Paralegal Specialist