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

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.)

4

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

12

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

15

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