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

APPELLEE'S BRIEF

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 Contents continued

TABLE OF AUTHORITIES

CASES

Table of Authorities continued

STATUTES

MISCELLANEOUS

INTRODUCTION

This is a misappropriation case. As the government correctly frames the issue, the question is whether the Computer Fraud and Abuse Act (CFAA) makes it a federal crime for employees to "obtain[] information from a work computer for the purpose of aiding [a] competing business." (Govt. Brief at 2.) In other words, the government does not allege that Mr. Nosal or his alleged co-conspirators accessed any computers that they were not entitled to access. Nor does it allege that they accessed any information that they were not entitled to access. Rather, the government alleges that Mr. Nosal's co-conspirators accessed and obtained proprietary information, and then used that information for an impermissible purpose — namely, to assist Mr. Nosal in starting a competing business venture.

Whether the CFAA covers misappropriation is a question that has divided courts over the last decade. The language of the CFAA itself does not offer a clear answer. The first courts to face the misappropriation question generally interpreted the statute broadly and held that the CFAA implicitly covers such conduct. In recent years, however, more courts have chosen a more cautious path. The docket of civil CFAA cases has ballooned, and in the last few years, federal prosecutors have attempted to use the CFAA to attack a wide variety of misconduct, including everything from ticket scalping to cyber-bullying to employee misappropriation.

The enormous potential scope of the CFAA has troubled courts and commentators alike.[1] Indeed, the very fact that a federal criminal statute could conceivably cover such a wide array of conduct is troubling.

Against that backdrop, this Court recently ruled for the first time on the CFAA's scope in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). In *Brekka*, this Court explicitly rejected cases allowing a misappropriation theory, and it instead adopted a sensibly narrow construction of the statute. As the district court below recognized, that narrow construction does not allow for prosecutions based on theories of employee misappropriation. *Brekka* squarely rejected the government's theory of this case.

In this appeal, the government contends that the relevant portions of *Brekka* were dicta, and thus that this is an issue of first impression. (Govt. Brief at 10.) That is flatly false. The government also complains that because *Brekka* was a civil case, the government did not have any opportunity to be heard. (Govt. Brief at 23 n.9.) It may be, therefore, that the government's ultimate goal in this appeal

---

[1]As Orin Kerr, the nation's leading computer crime scholar, put it: "The CFAA is a remarkably broad statute, and the recent prosecutions in [the Lori Drew case] and Nosal show that federal prosecutors eventually will try to exploit the breadth and ambiguity of the statute to bring prosecutions based on aggressive readings of the statute." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1587 (2010).

is to overrule *Brekka* using en banc proceedings. But especially in light of Due Process and fair warning concerns, *Brekka* was correctly decided. In any event, for the purposes of this three-judge panel's disposition, *Brekka* makes this an easy case.

STATEMENT OF JURISDICTION

As the basis for this Court's jurisdiction, the government relies solely on 28 U.S.C. § 1291, the general statute codifying the final judgment rule. It is not the case, however, that the dismissal of some but not all counts automatically creates an immediately appealable final judgment. *See Am. States Ins. Co. v. Dastar Corp.*, 318 F.3d 881, 888-89 (9th Cir. 2003).

A more natural basis of jurisdiction might be the Criminal Appeals Act, 18 U.S.C. § 3731. This Court's jurisprudence regarding the Criminal Appeals Act, however, remains unsettled or even contradictory. *Compare United States v. Dior*, 671 F.2d 351, 355 (9th Cir. 1982) (holding that an interlocutory appeal by the government must satisfy both § 1291 and § 3731), *with United States v. Russell*, 804 F.2d 571, 573 (9th Cir. 1986) (holding that if an interlocutory appeal by the government satisfies § 3731, it need not satisfy § 1291.).[2] It is perhaps for that

[2] *See also United States v. Fernandez*, 231 F.3d 1240, 1244 (9th Cir. 2000) (following *Dior*); *United States v. Cote*, 51 F.3d 178, 180 (9th Cir. 1995) (following *Dior*); *United States v. Woodruff*, 50 F.3d 673, 675 (9th Cir. 1995)

very reason that the government avoided relying on § 3731. In any event, the precise basis for this Court's jurisdiction is unclear.

SUMMARY OF ARGUMENT

The indictment in this case alleges that Mr. Nosal and his co-conspirators violated the Computer Fraud and Abuse Act when they obtained and then misappropriated information stored on their employer's computer. But this Court has already held that the CFAA does not cover acts of misappropriation. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). Under *Brekka*, the government's allegations failed to state an offense.

Moreover, even if the question were not already settled in this Circuit, ordinary principles of statutory interpretation would require dismissal of the relevant counts. Both the text and the legislative history of the CFAA suggest that the statute was not intended to cover acts of employee misappropriation. In addition, given the lack of clarity in the statute and the widespread disagreement among courts regarding its scope, the fair warning requirement compels a narrow reading.

(following *Russell*).

ARGUMENT

I. AS THIS COURT HAS ALREADY HELD, THE COMPUTER FRAUD AND ABUSE ACT DOES NOT COVER ACTS OF MISAPPROPRIATION

A. Applying *Brekka*

This Court's resolution of this appeal should start and end with *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). Like this case, *Brekka* was a misappropriation case. This Court was required to resolve whether a misappropriation theory was actionable under the CFAA. This Court thus examined the language of the CFAA and the competing case law interpreting that language. Noting that the CFAA is primarily a criminal statute, this Court made clear that its interpretation must be guided by the rule of lenity. Taking all of those considerations into account, this Court rejected the misappropriation theory of the CFAA. It settled on the following narrower interpretation of the statute:

> This leads to a sensible interpretation of §§ 1030(a)(2) and (4), which gives effect to both the phrase "without authorization" and the phrase "exceeds authorized access": a person who "intentionally accesses a computer without authorization," §§ 1030(a)(2) and (4), accesses a computer without any permission at all, while a person who "exceeds authorized access," *id*., has permission to access the computer, but accesses information on the computer that the person is not entitled to access.

Id. at 1133.

That single paragraph disposes of this appeal. As the government concedes, Mr. Nosal's co-conspirators did not access a computer without any permission at all, so they cannot be prosecuted under the "without authorization" prong. They also did not access information on the computer that they were not entitled to access, so they cannot be prosecuted under the "exceeding authorized access" prong. Since their alleged conduct does not fit under either prong of the CFAA, as interpreted by *Brekka*, the criminal charges cannot proceed.

In short, *Brekka* rejected the misappropriation theory of the CFAA and thus vitiated the government's theory of this case. Presumably, the government believes that *Brekka* was wrongly decided and hopes for its demise. In prosecutions around the country, the government has argued for much broader interpretations of the CFAA — and thus for much broader federal prosecutorial authority. In this appeal, the government offers the following oblique attack on *Brekka*'s legitimacy:

> [T]he Court should note that *Brekka* decided a civil matter based on its construction of a predominantly criminal statute. The government was not a party to that matter, and did not have an opportunity to be heard.

(Govt. Brief at 23 n.9.)

Of course, at least at this stage of its appeal, the government cannot directly challenge *Brekka's* holding, so it must instead attempt to evade it. Its brief on

appeal attempts two evasive maneuvers. First, it argues that the relevant portions of *Brekka* were mere dicta. Second, it argues that certain passages of that purported dicta, pried from their context, actually *support* the misappropriation theory of the CFAA. Neither argument is persuasive.

1. Holding and "Dicta"

The relevant portion of the CFAA has two prongs: the "without authorization" prong and the "exceeding authorization" prong. The government now concedes that it cannot prosecute Mr. Nosal under the former, so its case is based entirely on the latter. Although *Brekka* explicitly discussed both prongs of the CFAA, the government now contends that *Brekka's* analysis of the "exceeding authorization" prong was dicta. That is false for several reasons.

First, the government implicitly relies on a broad notion of "dicta" that this Court has rejected. This Court has warned that a party (or a subsequent panel) may not evade precedent simply by attaching a label of "dicta" to unhelpful portions of an earlier opinion. Rather, "a prior decision has binding effect to the extent that 'it is clear that a majority of the panel has focused on the legal issue presented by the case before it and made a deliberate decision to resolve the issue.'" *United States v. Cassel*, 408 F.3d 622, 633 n.9 (9th Cir. 2005) (quoting *United States v. Johnson*, 256 F.3d 895, 916 (9th Cir. 2001) (en banc) (plurality op. of Kozinski, J.)). There

is no question but that the *Brekka* panel made a deliberate decision to resolve the meaning of the "exceeding authorization" prong. Second, *Brekka's* analysis of the "exceeding authorization" prong constitutes holding, not dicta, under any sensible definition of that distinction. The panel's core analysis focused on the plain meaning of the term "authorization." 581 F.3d at 1132-33. Because that term appears in both prongs of the statute, the panel's definition of that term yielded a conclusive and binding interpretation of both prongs of the statute. As the panel recognized, no court could sensibly issue a holding on the meaning of one prong of the statute while ignoring the other. Thus, the panel adopted a "sensible interpretation" of the term authorization—an interpretation "which gives effect to both the phrase 'without authorization' and the phrase 'exceeds authorized access.'" *Id*. at 1133.

In short, in order to decide the case before it, the *Brekka* panel was required to adopt a coherent interpretation covering both prongs of the statute. And in any event, although the employer in *Brekka* relied primarily on the "without authorization" prong, the panel suggested that the employer had at least implicitly raised an argument under the "exceeding authorization" prong as well. *See id*. at 1135 n.7. Based on its coherent interpretation of both prongs, the panel rejected that argument as well.

Brekka's analysis of both CFAA prongs constitutes binding precedent, not dicta. If the government wishes to challenge that analysis, it may seek en banc proceedings or Supreme Court review. It may not simply dismiss it with a pejorative label.

2. Brekka's Definition of the "Exceeding Authorization" Prong

The government next contends that *Brekka's* purported dicta regarding of the "exceeding authorization" prong actually *validates* rather than undermines its theory of this prosecution. This argument would be baffling if it were not so easily disassembled. In order to make its argument work, the government simply plucks one sentence the *Brekka* opinion, and quotes it out of context, while ignoring the opinion's core holding.

Brekka says: "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. That sentence, standing alone, would seem to suggest that employers may place limitations *of any sort* on employees' computer use, and when an employee violates any such limitation, she has committed a federal crime.

But that sentence does not stand alone. In the very next paragraph, the *Brekka* court offered its definitive conclusion regarding the meaning of the statute,

including the meaning of the second prong: "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*." *Id*. (emphasis added). In other words, after stating in general terms that exceeding authorization means exceeding limitations, the court clarified that *only certain kinds* of limitations can give rise to criminal liability.

An employer may say to an employee: "You have permission to access the Cronos database but not the Poseidon database, because the Poseidon database is highly confidential." Under *Brekka*, if an employee violates those limitations, he has committed a crime under the CFAA. That result is sensible, since in this hypothetical, the employee has committed an act similar to hacking. To put it in common law terms, the employee has committed an act of trespass, not merely an act of misappropriation.

An employer may also say to an employee: "You have permission to access any database on the company server, but you may only do so for the good of the company, not for your own enrichment." Under *Brekka*, if any employee violates those limitations, he has not committed a crime under the CFAA. The employee may be liable for breach of contract or for some violation of state law, but his act of misappropriation cannot be prosecuted under the CFAA. In this hypothetical,

the employee has not "accesse[d] information on the computer that the person is not entitled to access," and so cannot be prosecuted. As one court aptly put it: "'Exceeds authorized access' should not be confused with exceeds authorized use." *Bell Aero. Servs. v. U.S. Aero Servs.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010).

In the relevant counts, the government never alleged that Mr. Nosal or his alleged co-conspirators ever accessed information that they were not entitled to access. Rather, the government alleged that they accessed information that they were entitled to access, but then used that information for impermissible purposes. Under *Brekka*, the government's allegations do not constitute a crime.

B. Reasoning in the Absence of *Brekka*

The government is desperate to characterize this appeal as presenting a question of first impression. For the reasons given above, that is false: This case is controlled by *Brekka*. But even if this were a question of first impression—even if *Brekka* had never been decided — the result would be the same. Ordinary principles of statutory interpretation, including the fair warning requirement, would require dismissal of the counts.

1. Statutory Text and Structure

A straightforward reading of the statutory text suggests that Congress did

not intend to cover acts of misappropriation. In the text itself, Congress offered the following definition of the phrase "exceeds authorized access": "[T]he 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." 18 U.S.C. § 1030(e)(6). The most natural reading of that language requires dismissal of the relevant counts. Again, the gist of the government's allegation in this case is not that the defendants obtained information that they were not entitled to obtain — rather, its allegation is that the defendants *misused* that information.

As many courts have recognized, "the plain language of § 1030(a)(2), (4), and (5)(A)(iii) target the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (internal quotation marks omitted); *see also Orbit One Communs. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The plain language of the CFAA supports a narrow reading. The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation.").

The government, however, argues that the statutory term "entitled" implicitly contains a misappropriation theory of liability. According to the

government, when an employee obtains information for improper purposes, he loses his "entitlement" to obtain that information. Even aside from the semantic gymnastics involved in such an interpretation, the problem with the government's argument is that it conflates the two prongs of the CFAA. The words "authorize" and "entitle" are synonymous. If improper purpose somehow automatically revoked authorization, then acting "without authorization" and "exceeding authorization" would be coextensive. *See Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342-43 (D. Ga. 2007) (explaining how the "entitlement" theory of misappropriation liability "conflates the meaning of those two distinct phrases and overlooks their application in § 1030(e)(6)."). The government's reading of the statute would disrupt the two-pronged structure chosen by Congress.

In sum, the statutory text and structure of the CFAA support a narrower reading than the one proposed by the government. The text and structure support the result this Court already reached in *Brekka*.

2. Legislative History

The government also argues that the legislative history of the statute supports a broad reading. Specifically, the government relies on the Senate Report from the Judiciary Committee explaining the 1986 amendment to the statute. *See* S. Rep. No. 99-432 (1986). A more careful reading of that Report, however,

supports the opposite position.

The first version of the CFAA covered not only access without authorization but also access *with* authorization"for purposes to which such authorization does not extend." In other words, the original statute appeared to cover (among other things) acts of misappropriation. In 1986, Congress replaced that language with the current "exceeds authorized access" language, as well as definition provided in § 1030(e)(6). Relying on the 1986 Senate Report, the government argues that the current version is the same as the earlier version and that the amendment had no substantive effect. (Govt. Brief at 18 & n.6.)

A closer examination of the Senate Report, however, suggests that Congress replaced the earlier language precisely because it was too broad. Senators Mathias and Leahy appended their own statement to the Report and explained in more detail the reason for the 1986 amendments. They explained how the original version of the CFAA had been passed in haste, as part of a legislative rider. *See* S. Rep. No. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494). As a result, in 1984, the House had never voted on a series of narrowing amendments, which had been unanimously approved by the Senate. The purpose of the 1986 amendments was to fix the shortcomings of the original version. *See id.*

Specifically, Congress replaced the earlier improper "purposes" language

precisely to "remove[] from the sweep of the statute one of the murkier grounds of liability." *Id*. In short, as Senators Mathias and Leahy explained, one of the principle purposes of the 1986 amendment was to exclude a misappropriation theory of liability and replace it with something both more narrow and less vague. *See Gast*, 535 F.Supp. 2d at 966 ("The legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."); *Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (discussing the 1986 Senate Report and concluding that the amendment was intended to narrow the scope of the statute).

Thus, even if *Brekka* were not controlling, and even if the text itself were not clear, the legislative history demonstrates that the current version of the CFAA was not intended to cover acts of employee misappropriation.

3. The CFAA and the Fair Warning Requirement

Perhaps most importantly, and most fundamentally, the application of the fair warning requirement would compel a narrow reading even if Brekka had not already settled the question.

a. The Requirement of Fair Warning

Criminal laws must be clear so that citizens may know what conduct is forbidden and what conduct is allowed. This principle, which is derived from the

Ex Post Facto Clause and the Due Process Clause, is known as the fair warning requirement. As the Supreme Court has explained, it has several specific doctrinal components.

> There are three related manifestations of the fair warning requirement. First, the vagueness doctrine bars enforcement of a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application. Second, as a sort of junior version of the vagueness doctrine, the canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered. Third, although clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute, due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope. In each of these guises, the touchstone is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal.

United States v. Lanier, 520 U.S. 259, 266-67 (1997) (citations and internal quotation marks omitted).

The Supreme Court's recent decision in *United States v. Skilling*, 561 U.S. __, 130 S. Ct. 2896 (2010), illustrates the proper application of the fair warning requirement. In *Skilling*, the Court faced a challenge to the honest services fraud statute, 18 U.S.C. § 1346. The defendant argued that § 1346 was void for

vagueness, while the government argued that the statute covered a wide range of conduct. Consistent with the fair warning requirement, the Court chose a middle path and adopted a narrow construction of the statute.

The Court noted that lower courts had reached inconsistent results regarding the scope of § 1346. *See* 130 S. Ct. at 2927 n.36. As a result, it was difficult or impossible to know exactly conduct what was covered by the statute. The Court concluded that if the statute were given the sort of broad construction urged by the government, it would be void as unconstitutionally vague, in part because it would potentially cover a wide variety of conduct that was not "seriously culpable." *Id*. at 2932-33. The Supreme Court thus pared the statute to its core and ruled that "honest services fraud" covers only kickbacks and bribery.[3] The ruling was an example of the operation of the rule of lenity. And according to the court, its narrowing construction was the only result consistent with the fair warning requirement.

b. Varying Interpretations by Courts

The Computer Fraud and Abuse Act is afflicted by the same maladies that plagued the honest services fraud statute. It is susceptible to a variety of different

[3] Justices Scalia, Thomas, and Kenney concurred in the result, but argued that the void-for-vagueness doctrine required the statute to be invalidated altogether. *Id*. at 2935-2963.

interpretations. Courts around the country have issued widely varying rulings regarding the statute's scope. If the government's proposed construction were accepted, the statute would cover a remarkably broad range of conduct, including conduct that is not seriously culpable. Such a broad construction would render the statute unconstitutionally vague. Thus, the only way save the statute is to interpret it narrowly — in precisely the way this Court already construed the statute in *Brekka*.

The government argues that the "exceeding authorization" prong of the CFAA is not in any way vague or ambiguous. That argument is obtuse. The wide divisions in the existing case law demonstrate beyond doubt that the statute can reasonably be interpreted in different ways.

In the body of case law interpreting the CFAA, there are two sharply divided camps. *See Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D.N.Y. 2010) (discussing the "two different ways" that courts have interpreted the statute). Some courts have ruled that the statute covers

misappropriation,[4] while others have ruled that it does not.[5] And even within those two camps, there are further divisions.

For example, even if it were true that the CFAA covers misappropriation, there are different possible views about what counts as misappropriation, or what acts of misappropriation were covered. Among other possibilities, it could mean: (1) that an employee is guilty if she violates a general common law duty of loyalty, (2) that an employee is guilty if she violates a specific state law duty of loyalty, (3) that an employee is guilty if she violates a corporate usage policy, or (4) that an employee is guilty if she violates a specific term of an employment contract. Within the misappropriation camp, different courts have chosen different formulations.

For example, in *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th

---

[4] *See, e.g., United States v. John*, 597 F.3d 263, 271-13 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000).

[5] *See, e.g., Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D.N.Y. 2010); *Bell Aero. Servs. v. U.S. Aero Servs.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 610-13 (M.D. Tenn. 2010); *Black & Decker v. Smith*, 568 F. Supp. 2d 929, 933-36 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 963-68 (D. Ariz. 2008); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342-43 (D. Ga. 2007).

Cir. 2006), the Seventh Circuit reasoned that an employee violates the CFAA any time she violates a duty of loyalty, as defined by the general common law of agency. The Fifth Circuit has also accepted a misappropriation theory, but has given an even broader definition of what conduct is covered. In the Fifth Circuit, an employee violates the CFAA any time that she violated "expected norms of intended use or the nature of the relationship established between the computer owner and the user." *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) (internal quotation marks omitted).[6]

c. Varying Interpretations by the Government

Even in the course of this litigation, the government has taken varying positions on what conduct constitutes a crime. In its initial filing below, the government argued that the alleged conduct was criminal because Mr. Nosal and his co-defendants acted contrary to their employer's interest, and thus that any "authorization" was automatically withdrawn under principles of agency law.[7] In its post-*Brekka* filing below, the government argued that the alleged conduct was

[6] The "expected norms of intended use" construction adopted by the Fifth Circuit is so extraordinarily vague that it is hard to see how any employee could possibly know what is illegal and what is not.

[7] United States' Opposition to Defendant Nosal's Second Motion to Dismiss Indictment at 13-14 (Feb. 2, 2009) (Dkt 87).

criminal primarily because Mr. Nosal and his co-defendants violated the terms of their employment agreements.[8] Now on appeal, the government makes another subtle shift. Instead of relying on employment agreements, the government argues that the alleged conduct was criminal because Mr. Nosal and his co-defendants violated corporate policies and violated the terms of pop-up banners that appeared during database use.

Careful consideration of the government's shifting positions raises a host of questions that could affect not only this case but many future cases. Is a violation of a formal employment contract required, or is violation of corporate policy sufficient? If a violation of corporate policy is sufficient, how specific must that policy be, and how clearly must it be communicated to employees? Is an occasional pop-up banner sufficient? Could an employee avoid liability by showing that he was unaware of the policy, or misunderstood it?

The government does not even attempt to answer any of these questions. It does not even attempt to draw a reasonably clear line between legal and illegal conduct.

---

[8] United States' Opposition to Defendant Nosal's Motion to Reconsider at 12-14 (Nov. 2, 2009) (Dkt 124).

d. *Difficulties in Applying a Misappropriation Theory*

At this point in the litigation, the government's position appears to be that the alleged conduct constituted a federal crime because it violated Korn-Ferry corporate policies, and it violated the terms of a pop-up banner. The relevant pop-up banner apparently said that the database "is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." The government's legal theory thus appears to be that any employer can create federal criminal liability for misappropriation simply by installing a pop-up banner saying that computers may be used for the employer's business only.

If that somewhat Orwellian legal theory were accepted, it would raise innumerable problems of application. Professor Kerr explained why:

> Interpreting the CFAA to prohibit employee access of an employer's computer for reasons outside the employment context runs afoul of [the fair warning requirement]. First, the theory gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited. The key consideration seems to be motive, but the employee has no way to determine what motives are illicit - and in the case of mixed motives, what proportion are illicit. Is use of an employer's computer for personal reasons always prohibited? Sometimes prohibited? If sometimes, when? And if some amount of personal use is permitted, where is the line? If use of an employer's computer directly contrary to the employer's interest is required, how contrary is directly contrary? Is mere waste of the

> employee's time enough? The cases generally deal with the dramatic facts of an employee who accessed a sensitive and valuable database to gather data that could be used to establish a competing company. But how sensitive does the database need to be? How valuable does the data need to be?

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1586 (2010).

Once again, the government does not even attempt to answer these questions. What is clear, however, is that the government's proposed interpretation of the CFAA would criminalize an astonishingly wide variety of routine employee behavior. It is inconceivable that Congress intended such a result. As *Skilling* demonstrates, the fair warning requirement does not allow courts to reach such a result in the absence of much clearer direction from Congress.

//

//

//

//

//

CONCLUSION

For the reasons stated, the district court's ruling dismissing Counts 2, 4,5,6, and 7 should be affirmed.

Dated: September 7, 2010

Respectfully submitted,

RIORDAN & HORGAN

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

By /s/ Dennis P Riordan

Attorneys for Defendant
DAVID NOSAL

STATEMENT OF RELATED CASES

Appellee is aware of no related cases pending in this Court.

CERTIFICATION REGARDING BRIEF FORM

I, Dennis P. Riordan, hereby certify that the foregoing Appellee's Brief is proportionately spaced, has a typeface of 14 points, and contains 5,095 words.

Dated: September 7, 2010

/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 September 7, 2010, 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