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.

REPLY BRIEF FOR THE UNITED STATES

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

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

SCOTT N. SCHOOLS
Associate Deputy Attorney General
United States Department of Justice
Attorney for the United States, Acting
Under Authority Conferred by 28
U.S.C. § 515

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

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: October 22, 2010

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES, RULES, AND GUIDELINES

LEGISLATIVE MATERIALS

PUBLICATIONS

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.

REPLY BRIEF FOR THE UNITED STATES

ADDITIONAL STATEMENT OF JURISDICTION

This is a government appeal from an order of the district court dismissing Counts 2 & 4-7 the superseding Indictment (the "Indictment"). In its opening brief, the government cited 28 U.S.C. § 1291 as the jurisdictional basis for the appeal. As Nosal points out, jurisdiction in fact rests on 18 U.S.C. § 3731. That statute specifically authorizes a government appeal from an order dismissing "one or more counts" of an indictment. Specifically, section 3731 provides that "[i]n a criminal case an appeal by the United States shall lie to a court of appeals from a decision, judgment, or order of a district court dismissing an indictment . . . as to any one or more counts, or any part thereof. . . ." Id.; see also United States v. Sanabria, 437 U.S. 54, 69 n.23 (1978) ("We agree with the Court of Appeals

…that there is no statutory barrier to an appeal from an order dismissing only a portion of a count. One express purpose of 18 U.S.C. § 3731 (1976 ed.) is to permit appeals from orders dismissing indictments 'as to any one or more counts.' A 'count' is the usual organizational subunit of an indictment, and it would therefore appear that Congress intended to authorize appeals from any order dismissing an indictment in whole or in part."); United States v. Russell, 804 F.2d 571, 573 (9th Cir. 1986) (finding jurisdiction to hear government's interlocutory appeal of district court's pre-trial dismissal of 12 counts from 28-count indictment); United States v. Warren, 601 F.2d 471, 473 (9th Cir. 1979) (per curiam) (citing both 28 U.S.C. § 1291 and 18 U.S.C. § 3731 in government appeal of district court's order dismissing indictment); United States v. Marubeni Am. Corp., 611 F.2d 763, 764-65 (9th Cir. 1980) (Section 3731 authorizes appeal of partial dismissal of a count).

ARGUMENT

The government disagrees with Nosal's characterization of this appeal as "a misappropriation case." The government is not arguing that Nosal's co-conspirators "exceeded authorized access" under 18 U.S.C. § 1030 (hereinafter, the "CFAA") because they misused computer data that they were authorized to obtain. Nor is the government claiming that their "improper purpose somehow automatically revoked authorization," rendering their access "without

authorization." Def. Brief at 13. Rather, the government alleges that Korn Ferry granted Nosal's co-conspirators a restricted right to access Korn Ferry computers by explicitly instructing Nosal's co-conspirators to access information in the Searcher database only for legitimate Korn Ferry business purposes.[1] When Nosal's co-conspirators accessed the Searcher database for other purposes, they violated this express access restriction and thereby obtained proprietary Korn Ferry information that they were "not entitled so to obtain." 18 U.S.C. § 1030(e)(6).

In other words, Nosal's co-conspirators "exceeded authorized access" when they engaged in the conduct charged in Counts 2 & 4-7 of the Indictment. As discussed below, this conclusion is consistent with this Court's analysis in LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009). Moreover, Nosal's competing interpretation of "exceeds authorized access" cannot be reconciled with the text and legislative history of 18 U.S.C. § 1030 (hereinafter, the "CFAA"). Because the meaning of "exceeds authorized access" is unambiguous in this case,

[1] Among other things, the government alleges that Korn Ferry: (1) prohibited employees from accessing Korn Ferry's computer system without "specific authority," (2) used a computer banner to inform employees that certain functions of the Searcher database were "intended to be used by Korn/Ferry employees for work on Korn/Ferry business only," and (3) prohibited the use and disclosure of information on Korn Ferry's computer system except for legitimate Korn Ferry business. ER 25, 100-04.

there is no basis for concluding that the statute is unconstitutionally vague as applied to Nosal and his co-conspirators.

I. Brekka Supports the Government's Interpretation of "Exceeds Authorized Access."

Because the government alleges that Nosal's co-conspirators accessed Korn Ferry computers in a way that violated Korn Ferry's explicit, pre-existing restrictions on access, this case presents a different issue than the one this Court decided in LVRC Holdings LLC v. Brekka. See Govt. Brief at 21-23. In Brekka, the plaintiff-employer did not claim that it had imposed express limitations on the defendant-employee's authority to access the documents at issue, nor that the defendant-employee had violated any such access restrictions. See Brekka, 581 F.3d at 1129, 1133, 1135. Rather, the question in Brekka was whether the defendant lost his 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 1134.

Even though Brekka does not squarely address the issue in this appeal, it discusses the meaning of "exceeds authorized access" and reaches a conclusion that supports the government's theory in this case. Specifically, the Court in Brekka states that it is "clear" that an individual exceeds authorized access within the meaning of 18 U.S.C. § 1030(e)(6) when he "is authorized to use a computer *for certain purposes* but goes beyond those limitations." Id. at 1133 (emphasis

added). This language directly supports the government's position that someone "exceeds authorized access" when he accesses a computer in violation of a purpose-based restriction on access, as Nosal's co-conspirators allegedly did in this case.

Nosal urges the Court to disregard this language in Brekka and focus instead on a subsequent sentence in the opinion, which explains that ". . . a person who 'exceeds authorized access' has permission to access the computer, but accesses information on the computer that the person is not entitled to access." Brekka, 581 F.3d at 1133 (internal citation omitted). However, this sentence is also consistent with the government's position in this appeal. As discussed above, the government alleges that Nosal's co-conspirators were not entitled to access information on Korn Ferry computers, and specifically information in the Searcher database, unless they had a legitimate Korn Ferry business purpose for doing so. ER 25, 100-04. Because the co-conspirators lacked this required purpose when they accessed the Searcher database to further their competing business, they obtained "information on the computer that [they were] not entitled to access." Brekka, 581 F.3d at 1133. The hypothetical possibility that Nosal's co-conspirators might have been entitled to access the same information in other circumstances – *i.e.*, when they had a legitimate Korn Ferry business purpose for

doing so – did not entitle them to obtain this information when they accessed the Searcher database for non-Korn Ferry purposes.

Brekka also does not support Nosal's claim that someone can exceed authorized access only by violating "certain kinds" of access limitations – specifically, access limitations that completely prohibit the person from accessing certain data at all, under any circumstances. Def. Brief at 10. Nothing in Brekka suggests that the Court even contemplated such a distinction, nor did the facts of that case provide a reason for the Court to do so. Instead, Brekka simply acknowledges that the relevant issue for "exceeding authorized access" is whether the accesser accessed information "that the accesser is not entitled so to obtain." 581 F.3d at 1135 n.7 (quoting 18 U.S.C. § 1030(e)(6)). Furthermore, as discussed above and in the government's opening brief, the Court in Brekka states that it was "clear" that an individual exceeds authorized access within the meaning of 18 U.S.C. § 1030(e)(6) when he "is authorized to use a computer *for certain purposes* but goes beyond those limitations." Id. at 1133 (emphasis added).

In short, the government agrees with Brekka's brief discussion of the term "exceeds authorized access" and, despite Nosal's claims, does not "evade" Brekka in any way.

II. Nosal's Interpretation of "Exceeds Authorized Access" Is Inconsistent with the Text and Legislative History of the CFAA.

Because Brekka does not resolve the specific issue raised in this appeal, this Court must now decide whether Nosal's co-conspirators could have "exceeded authorized access" when they engaged in the conduct described in Counts 2 & 4-7. Nosal argues that his co-conspirators did not "exceed authorized access" because, in Nosal's view, the term "exceeds authorized access" applies only to someone who accesses data that the accesser is completely prohibited from obtaining at all, in any manner. However, this interpretation of "exceeds authorized access" is at odds with the text and legislative history of the CFAA. Indeed, both the statutory text and the legislative history confirm the government's interpretation of the CFAA: an individual exceeds authorized access when he accesses a computer and obtains information in a manner that the authorizing party has specifically prohibited (*e.g.*, by accessing the computer for a specifically prohibited purpose).

A. Statutory Text

Under the CFAA, "'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). Nosal argues that this definition encompasses only situations where the accesser has obtained information that the accesser is *never* entitled to obtain, under any circumstances. Def. Brief at 10-13. However, Nosal's interpretation is

inconsistent with the final words of the definition, "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). "So" means "[i]n the state or manner indicated or expressed." Webster's II New Riverside University Dictionary 1102 (1988). Because of the presence of the word "so," the meaning of the concluding phrase in 18 U.S.C. § 1030(e)(6) is unambiguous: someone exceeds authorized access when he obtains or alters information that he is not entitled to obtain or alter *in those circumstances*. The word "so" clarifies that the accesser might have been entitled to obtain the information *in some other circumstances*, but not in the way he did – *i.e.*, he was "not entitled *so* to obtain" the information. 18 U.S.C. § 1030(e)(6) (emphasis added).

For example, an employer could grant an employee access to all information on its computer system, but it could restrict that access authority in various ways. It may tell the employee, "You have permission to access any medical records on the computer system, but only between the hours of 9:00 a.m. and 5:00 p.m., only with the written approval of a supervisor, and only when a doctor has specifically requested the records." When these circumstances are not present, the employee is no more entitled to obtain the medical records than is another employee who is prohibited from accessing the medical records at all. And if the first employee accesses a medical record in a way that violates any of these specific restrictions,

that employee would not be entitled "so to obtain" that medical record and would have exceeded authorized access under the CFAA.

In short, the definition of "exceeds authorized access" shows that someone exceeds authorized access by obtaining information in a prohibited manner, even if the accesser might be entitled to obtain the same information under other circumstances. Moreover, nothing in the text of the CFAA suggests that purpose-based access restrictions – *e.g.*, restrictions that authorize the accesser to obtain the information only for a specified purpose – are an exception to this general rule. For that reason, the hypothetical employee above exceeds authorized access even if the employee violates only the employer's purpose-based access restriction by obtaining a medical record for a reason other than a doctor request. See United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."); Cont'l Group, Inc. v. KW Prop. Mgmt., LLC, 622 F. Supp. 2d 1357, 1372 (S.D. Fla. 2009) ("substantial likelihood" that defendant exceeded authorization when she downloaded files for her own purposes, where her employer's computer access policies stated that its computers "are provided for business use" and any equipment is provided "to be used solely for [the employer's] purposes").

B. Legislative History

The plain meaning of "exceeds authorized access" is confirmed by the relevant legislative history, which supports the government's interpretation of the statute. The current definition of "exceeds authorized access" was enacted in 1986, as part of a bill that revised and added to the original version of the CFAA that passed in 1984.[2] See Govt. Brief at 16-17. The Senate Report for the 1986 bill provided the following explanation for Congress's introduction of the term "exceeds authorized access" in sections 1030(a)(1) and (2) of the existing statute:

> Section 2(c) [of the 1986 bill] substitutes the phrase 'exceeds authorized access' for the more cumbersome phrase in present 18 U.S.C. § 1030(a)(1) and (2), 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend'. The Committee intends this change to simplify the language in 18 U.S.C. § 1030(a)(1) and (2), and the phrase 'exceeds authorized access' is defined separately in Section (2)(g) of the bill.

S. Rep. No. 99-432, pt. 3 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2486.

In other words, the term "exceeds authorized access" replaced a "more cumbersome phrase" that specifically discussed accesses in violation of purpose-

---

[2] The Senate Report for the 1986 bill explained that the Judiciary Committee's concern about computer fraud and abuse had become "more pronounced" because of the proliferation of computers and mounting evidence that "existing criminal laws are insufficient to address the problem of computer crime." S. Rep. No. 99-432, pt. 1, reprinted in 1986 U.S.C.C.A.N. 2479, 2479. The resulting bill was "a consensus bill aimed at deterring and punishing certain 'high-tech' crimes in a manner consistent with the States' own criminal laws in this area." Id., reprinted in 1986 U.S.C.C.A.N. 2479, 2482.

based restrictions and therefore encompassed the charged conduct in this case.[3] As the government explained in its opening brief, Congress did not intend to restrict the scope of the original phrase, but merely wanted to replace it with a shorter, simpler term. See Govt. Brief at 17-18. If anything, Congress actually expanded the scope of the original phrase because the definition of "exceeds authorized access" encompasses accesses that violate any type of access restriction, not just those that violate purpose-based restrictions. See Govt. Brief at 18.

Nosal asks the Court to scrutinize the last section of the Senate Report, entitled "Additional Views of Messrs. Mathias and Leahy," but that section does not support Nosal's claim that "Congress replaced the earlier language precisely because it was too broad." Def. Brief at 14. In fact, the focus of Senators Mathias and Leahy's discussion was the scope of 18 U.S.C. § 1030(a)(3) – a provision that has not been charged in this case – rather than the meaning of "exceeds authorized access." See S. Rep. No. 99-432, pt. 8, reprinted in 1986 U.S.C.C.A.N. 2479, 2493-96. When the senators expressed concern about potential "murkiness" in the CFAA, they were discussing the potential problems with imposing liability for

[3] Even Nosal tacitly acknowledges that the 1984 language would encompass the conduct at issue here, notwithstanding his imprecise description of that conduct as "misappropriation." See Def. Brief at 14 ("[T]he original statute appeared to cover (among other things) acts of misappropriation.").

exceeding authorized access under section 1030(a)(3). See id., reprinted in 1986 U.S.C.C.A.N. 2479, 2494. Unlike section 1030(a)(4), with which Nosal has been charged, section 1030(a)(3) imposes criminal liability on individuals based only upon unauthorized access to a non-public U.S. government computer, and without requiring the additional elements that the individual acted with the intent to defraud or obtained anything as a result of the access.

Senators Mathias and Leahy's concerns about "murkiness" were fully addressed by the 1986 bill, which restricted the scope of section 1030(a)(3) only to accesses that occurred "without authorization." Specifically, Senators Mathias and Leahy explained that the revised version of section 1030(a)(3) "includes three salutary features that minimize the possibility that this computer crime legislation could be misused to weaken the Freedom of Information Act, or to impose unnecessary obstacles to the public's right to know about government activities." Id. The second such feature was that the bill limited liability under section 1030(a)(3) to accesses that occurred "without authorization," which the bill accomplished by deleting the original, bulkier version of "exceeds authorized access" from section 1030(a)(3). See id.; compare Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ti. 2, sec. 2102(a), 98 Stat. 1837 (1984), with Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, sec. 2(b), 100 Stat. 1213 (1986). This change to section 1030(a)(3) was

intended to "remove[] from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization." S. Rep. No. 99-432, pt. 8, reprinted in 1986 U.S.C.C.A.N. 2479, 2494-95.

Although Senators Mathias and Leahy were concerned about imposing criminal liability under section 1030(a)(3) for exceeding authorized access, they plainly did not think that the concept of exceeding authorized access was, itself, murky, as they approved of a bill that preserved that basis for liability in sections 1030(a)(1) and (2) and included it in a new provision, section 1030(a)(4). Moreover, the senators' discussion of "exceeds authorized access" in the context of section 1030(a)(3) reveals that their understanding of this term is the same as the government's. Specifically, the senators recognized that an employee's "access to computerized data might be legitimate in some circumstances," but that in other circumstances, the employee "might be held to exceed his authorization" by accessing the same data. S. Rep. No. 99-432, pt. 8, reprinted in 1986 U.S.C.C.A.N. 2479, 2494-95. The senators were concerned about imposing liability on such an individual under section 1030(a)(3), but they had no similar concerns about subjecting the same person to liability under sections 1030(a)(1), (2), and (4). In other words, the senators believed that it was appropriate for the

CFAA to criminalize some accesses to computer data that occurred in an unauthorized manner, even when the person accessing the data might have been permitted to access the same data in other circumstances.

For all of these reasons, the legislative history of the CFAA confirms that the definition of "exceeds authorized access" has the scope that Congress intended and encompasses those who access computer data in violation of an express purpose-based restriction on access.

III. The CFAA Provides Fair Warning of Its Scope and Is Not Unconstitutionally Vague.

The CFAA, as applied to Nosal and his co-conspirators, also provides fair warning of its scope and is not unconstitutionally vague. To satisfy due process, and thereby overcome a vagueness challenge, a penal statute must define the criminal offense (1) "with sufficient definiteness that ordinary people can understand what conduct is prohibited," and (2) "in a manner that does not encourage arbitrary and discriminatory enforcement." Skilling v. United States, 130 S. Ct. 2896, 2927-28 (2010) (quoting Kolender v. Lawson, 461 U.S. 352, 357 (1983)). Courts should "consider whether a statute is vague as applied to the particular facts at issue, for '[a] plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others.'" Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2718-19 (2010) (quoting Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.,

455 U.S. 489, 495 (1982)). Accordingly, when reviewing a statute for vagueness, a court should not consider how the statute applies in hypothetical circumstances. See id. at 2719.

Here, the terms of the CFAA are clear in their application to the conduct of Nosal and his co-conspirators, which means that Nosal's vagueness challenge must fail. See Humanitarian Law Project, 130 S. Ct. at 2720. Nosal's vagueness argument is based on the alleged ambiguity of the term "exceeds authorized access," and he does not argue that any other statutory terms are ambiguous or vague. As discussed in the government's opening brief and in the previous sections, the term "exceeds authorized access" plainly encompasses the conduct charged in Counts 2 & 4-7 – *i.e.*, accessing computers in a manner that violates express access restrictions. Under the circumstances, and particularly in light of the plain text and legislative history of the CFAA, an ordinary person would have understood that Nosal's co-conspirators exceeded authorized access when they accessed Korn Ferry computers in a way that violated Korn Ferry's access restrictions.[4] Because the CFAA therefore defines the criminal offenses charged in Counts 2 & 4-7 "with sufficient definiteness that ordinary people can

[4] Korn Ferry even informed its computer users that accessing any Korn Ferry system or information without "specific authority" could lead to criminal prosecution. ER 25.

understand what conduct is prohibited," Skilling, 130 S. Ct. at 2927-28, the statute satisfies the first requirement of due process.

The CFAA also satisfies the second requirement of due process because it defines the criminal offenses charged in Counts 2 & 4-7 "in a manner that does not encourage arbitrary and discriminatory enforcement." Id. Counts 2 & 4-7 allege violations of 18 U.S.C. § 1030(a)(4), which imposes criminal liability only on those who exceed authorized access "knowingly and with intent to defraud." 18 U.S.C. § 1030(a)(4); see ER 31-32. This scienter requirement "limits the discretion of law enforcement and mitigates any perceived vagueness. . . ." United States v. Wyatt, 408 F.3d 1257, 1261 (9th Cir. 2005).

Furthermore, simply exceeding authorized access with the requisite intent, without more, is not enough to subject someone to liability under section 1030(a)(4) – the statute also requires that the person both act with the intent to defraud and use the computer access to "further[] the intended fraud and obtain anything of value. . . ." 18 U.S.C. § 1030(a)(4). Like the other elements of section 1030(a)(4), these requirements are objective and do not depend on the subjective judgment or discretion of a law enforcement officer. See Kolender v. Lawson, 461 U.S. 352, 358 (1983) (criminal statute encouraged arbitrary and discriminatory enforcement because it vested "virtually complete discretion in the hands of the police to determine whether the suspect has satisfied the statute"). Accordingly,

section 1030(a)(4) satisfies the second due-process requirement because it establishes sufficient guidelines to govern law enforcement and does not permit a "standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections." Kolender, 461 U.S. at 358 (quoting Smith v. Goguen, 415 U.S. 566, 575 (1974)).

Nosal argues that the government's interpretation of CFAA is unconstitutionally vague because it would enable the CFAA to "cover a remarkably broad range of conduct, including conduct that is not seriously culpable." Def. Brief at 18; see also id. at 23-24. Although Nosal refers generally to "the CFAA," the only charging provision at issue in this case – and therefore the only charging provision that Nosal may challenge for vagueness – is section 1030(a)(4), which is the basis for Counts 2 & 4-7.[5] It is difficult to see how this provision, which requires both intent to defraud and obtaining something of value through the intended fraud, could cover "conduct that is not seriously culpable" or "criminalize an astonishingly wide variety of routine employee behavior." Def. Brief at 18, 23. Furthermore, a criminal statute is not improper simply because it might apply to a broad range of conduct. See United States v. Banks, 514 F.3d

[5] Because this Court should only consider whether the CFAA is vague as applied to the facts of Nosal's case, Nosal cannot argue that other CFAA provisions with which he has not been charged, such as 18 U.S.C. § 1030(a)(2), might be rendered vague by the government's interpretation of "exceeds authorized access." See Humanitarian Law Project, 130 S. Ct. at 2718-19.

959, 967 (9th Cir. 2008) ("Although . . . criminal statutes should generally be construed narrowly, this principle does not operate as a flat prohibition on statutes that are drafted to apply to a broad range of conduct."). In any event, though, the potential applicability of the CFAA in other cases is not relevant to Nosal's vagueness challenge, which must be decided based on the particular facts of Nosal's own case. See Humanitarian Law Project, 130 S. Ct. at 2721 (noting that plaintiffs had pointed to "hypothetical situations" designed to test the limits of the statute at issue, but concluding that "[w]hatever force these arguments might have in the abstract, they are beside the point here").

Nosal also argues that the CFAA is vague because courts have disagreed about the scope of the term "exceeds authorized access" in other cases. See Def. Brief at 18. However, the existence of disagreement does not automatically render the statute vague or ambiguous as applied to Nosal and his co-conspirators. Furthermore, the "two sharply divided camps" that Nosal identifies, see Def. Brief at 19 n.4 & 5, have predominantly split over a question that is not at issue in this appeal – specifically, whether a person exceeds authorized access when she lawfully accesses information but then misuses or misappropriates that information.[6] The government is alleging something different in Counts 2 & 4-7:

[6] See, e.g., Orbit One Communications, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010) (executives were granted "unfettered access" to computer system); Bell Aero. Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp.

that Nosal's co-conspirators exceeded authorized access by violating Korn Ferry's explicit access restrictions, not by misusing information that Korn Ferry authorized them to obtain. This type of allegation has received much less attention from courts, and Nosal has not identified a meaningful split of authority on this question.

Of the cases listed in footnote 5 of Nosal's brief, it appears that only Diamond Power International, Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D. Ga. 2007), involved an allegation that someone violated a restriction on access, rather than simply a restriction on subsequent use of information. See id. at 1327-28 ("Diamond Power further restricted access to the Oracle network by permitting those with authorization only to access files containing information necessary to their work tasks."). Although the district court concluded that this allegation did not establish that the defendant had exceeded authorized access, its reasoning confused a violation of a purpose-based access restriction with an authorized

---

2d 1267, 1273 (M.D. Ala. 2010) (employees were permitted to access computer network "and any information on that network," and "there is no evidence that they exceeded that authorization"); ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 613 (M.D. Tenn. 2010) ("RMP complains, not that Camacho went beyond his authorization to access information he was not entitled to see, but that he subsequently misused that information by sharing it with AllParts."); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 936 (W.D. Tenn. 2008) ("[T]he Plaintiff objects not to Smith's accessing of the information, but to his later misuse thereof."); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 968 (D. Ariz. 2008) ("Shamrock conceded that Gast was permitted to view the specific files he allegedly emailed to himself.").

access that results in misuse or misappropriation. See id. at 1342 ("[A] violation does not depend upon the defendant's unauthorized use of *information*, but rather on the defendant's unauthorized use of *access*."). The government believes that Diamond Power's analysis is flawed, but in any event, the existence of such a district court opinion does not establish that the CFAA is unconstitutionally vague or ambiguous.

Nosal also argues that the government's interpretation of "exceeds authorized access" leads to confusion because the statute does not specify how an access restriction may be imposed on the accessing party (*e.g.*, by employment contract, corporate policy, or pop-up banner). See Def. Brief at 21. There is no constitutional requirement that the statute be so specific, particularly when there is no rational basis for making criminal liability dependent on the type of document used to describe the access restriction.

Furthermore, whether and how someone was authorized to use a computer system is a "true-or-false determination, not a subjective judgment such as whether conduct is 'annoying' or 'indecent'" that might be indicative of vagueness. United States v. Williams 553 U.S. 285, 306 (2008). Even though it may sometimes be difficult to determine whether someone has exceeded authorized access, "[t]he problem that poses is addressed, not by the doctrine of vagueness, but by the requirement of proof beyond a reasonable doubt." Id. "What renders a statute

vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what that fact is." Id. Accordingly, to the extent that Nosal questions whether certain documents were sufficient to restrict his co-conspirators' right to access the Korn Ferry computer systems, those questions can and should be resolved by a jury, and not by a dismissal order.

CONCLUSION

For the foregoing reasons, and for the reasons set forth in the government's opening brief, a defendant "exceeds authorized access" for purposes of 18 U.S.C. § 1030 when: (1) his right to access a computer is restricted, rather than unlimited, and (2) he accesses the computer in a manner that exceeds or violates those restrictions. Because the government has properly alleged that Nosal's co-conspirators exceeded authorized access, the district court's dismissal of Counts 2 & 4-7 should be reversed, and these counts should be reinstated for trial.

Dated: October 22, 2010

Respectfully submitted,

SCOTT N. SCHOOLS
Associate Deputy Attorney General
United States Department of Justice
Attorney for the United States, Acting Under Authority Conferred by 28 U.S.C. § 515

KYLE F. WALDINGER
Assistant United States Attorney
Northern District of California

LANNY A. BREUER
Assistant Attorney General
United States Department of Justice
Criminal Division

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

CERTIFICATE OF RELATED CASES

Counsel for the United States is aware of the following related cases pending before this court:

None.

Dated: October 22, 2010

/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

I, Jenny C. Ellickson, hereby certify that the foregoing Brief for the United States complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B), inasmuch as the brief is proportionately spaced, has a typeface of 14 points or more and contains 4,913 words. This certification is based on the word count of the word-processing system used in preparing the government's brief: WordPerfect for Windows, version X4.

Dated: October 22, 2010

/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 SERVICE

I hereby certify that on October 22, 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.

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:

_____

Marcia Hoffman
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

/s/
TYLE L. DOERR
Appellate Paralegal Specialist

ADDENDUM

TABLE OF CONTENTS

18 U.S.C.A. § 1030 (2004)

United States Code Annotated Currentness

Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes
Chapter 47. Fraud and False Statements (Refs & Annos)
§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—
(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; [FN1]
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $5,000; and
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) [FN2] (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(2) the term “protected computer” means a computer—
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
(3) the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term “financial institution” means—
(A) an institution, [FN3] with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;
(5) the term “financial record” means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term “exceeds authorized access ” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
(7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).