FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellant,* v. DAVID NOSAL, *Defendant-Appellee.*	No. 10-10038 D.C. No. 3:08-cr-00237-MHP-1 OPINION

Appeal from the United States District Court
for the Northern District of California
Marilyn H. Patel, Senior District Judge, Presiding

Argued and Submitted
February 14, 2011—San Francisco, California

Filed April 28, 2011

Before: Diarmuid F. O'Scannlain and Stephen S. Trott,
Circuit Judges, and Tena Campbell, District Judge.*

Opinion by Judge Trott;
Dissent by Judge Campbell

*The Honorable Tena Campbell, Senior United States District Judge for the District of Utah, sitting by designation.

COUNSEL

Jenny C. Ellison and Jaikumar Ramaswamy, United States Department of Justice, Washington, D.C., for the plaintiff-appellant.

Dennis P. Riordan, Riordan & Horgan, San Francisco, California, for the defendant-appellee.

OPINION

TROTT, Circuit Judge:

The United States appeals from the district court's dismissal of several counts of an indictment charging David Nosal with, *inter alia*, numerous violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.[1] Subsection (a)(4), the subsection under which Nosal was charged, subjects to punishment anyone who "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." *Id.* § 1030(a)(4). The indictment alleges that Nosal's co-conspirators exceeded their authorized access to their employer's computer system in violation of § 1030(a)(4) by obtaining information from the computer system for the

[1]Unless otherwise noted, all statutory references refer to Title 18 of the United States Code.

purpose of defrauding their employer and helping Nosal set up a competing business.

The district court relied on our decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), in determining that an employee does not exceed authorized access to a computer by accessing information unless the employee has no authority to access the information under *any* circumstances — in other words, an employer's restrictions on the use of the computer or of the information stored on that computer are irrelevant to determining whether an employee has exceeded his or her authorization. The government contends, on the other hand, that *Brekka* counsels in favor of its interpretation of the statute — that an employee exceeds authorized access when he or she obtains information from the computer and uses it for a purpose that violates the employer's restrictions on the use of the information.

We have jurisdiction under 18 U.S.C. § 3731, and we agree with the government. Although we are mindful of the concerns raised by defense counsel regarding the criminalization of violations of an employer's computer use policy, we are persuaded that the specific intent and causation requirements of § 1030(a)(4) sufficiently protect against criminal prosecution those employees whose only violation of employer policy is the use of a company computer for personal — but innocuous — reasons. We therefore reverse and remand to the district court with instructions to reinstate Counts 2, 4, 5, 6, and 7.

I

BACKGROUND

For purposes of our review, the indictment's allegations must be taken as true. *United States v. Fiander*, 547 F.3d 1036, 1041 n.3 (9th Cir. 2008).

A

THE ALLEGATIONS AGAINST NOSAL

From approximately April 1996 to October 2004, Nosal worked as an executive for Korn/Ferry International ("Korn/Ferry"), an executive search firm. When Nosal left Korn/Ferry in October 2004, he signed a Separation and General Release Agreement and an Independent Contractor Agreement. Pursuant to these contracts, Nosal agreed to serve as an independent contractor for Korn/Ferry and not to compete with Korn/Ferry for one year. In return, Korn/Ferry agreed to pay Nosal two lump-sum payments in addition to twelve monthly payments of $25,000.

Shortly after leaving his employment, Nosal engaged three Korn/Ferry employees to help him start a competing business. The indictment alleges that these employees obtained trade secrets and other proprietary information by using their user accounts to access the Korn/Ferry computer system. Specifically, the employees transferred to Nosal source lists, names, and contact information from the "Searcher" database — a "highly confidential and proprietary database of executives and companies" — which was considered by Korn/Ferry "to be one of the most comprehensive databases of executive candidates in the world."

Paragraphs 9-11 of the indictment describe Korn/Ferry's efforts to keep its database secure:

> 9. Korn/Ferry undertook considerable measures to maintain the confidentiality of the information contained in the Searcher database. These measures included controlling electronic access to the Searcher database and controlling physical access to the computer servers that contained the database. Korn/Ferry employees received unique usernames and created passwords for use on the company's computer sys-

> tems, including for use in accessing the Searcher database. These usernames and passwords were intended to be used by the Korn/Ferry employee only.
>
> 10. Korn/Ferry required all of its employees . . . to enter into agreements that both explained the proprietary nature of the information disclosed or made available to Korn/Ferry employees (including the information contained in the Searcher database) and *restricted the use and disclosure of all such information, except for legitimate Korn/Ferry business*. . . .
>
> 11. Among other additional measures, Korn/Ferry also declared the confidentiality of the information in the Searcher database by placing the phrase "Korn/Ferry Proprietary and Confidential" on every Custom Report generated from the Searcher database. Further, when an individual logged into the Korn/Ferry computer system, that computer system displayed the following notification, in sum and substance:
>
> > This computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and *to do so without the relevant authority can lead to disciplinary action or criminal prosecution*. . . .

(emphasis added) (third alteration in original).

B

DISTRICT COURT PROCEEDINGS

On June 26, 2008, the government filed a twenty-count superseding indictment against Nosal and one of his accom-

plices. Counts 2 through 9 of the indictment allege that the Korn/Ferry employees who conspired with Nosal — and Nosal himself as an aider and abettor — violated § 1030(a)(4).

Nosal filed a motion to dismiss the indictment. He argued "that the CFAA was aimed primarily at computer hackers and that the statute does not cover employees who misappropriate information or who violate contractual confidentiality agreements by using employer-owned information in a manner inconsistent with those agreements." In other words, the Korn/Ferry employees could not have acted "without authorization," nor could they have "exceed[ed] authorized access," because they had permission to access the computer and its information under certain circumstances.

Recognizing that the question was one of first impression in the Ninth Circuit, the district court described the "two lines of diverging case law on this issue":

> Some courts, including two courts of appeal, have broadly construed the CFAA to hold an employee acting to access an employer's computer to obtain business information with intent to defraud, i.e., for their own personal benefit or the benefit of a competitor, act "without authorization" or "exceed authorization" in violation of the statute. These courts have generally held that *authorized access to a company computer terminated once an employee acted with adverse or nefarious interests* and against the duty of loyalty imposed on an employee in an agency relationship with his or her employer or former employer.
>
> Other courts have refused to hold employees with access and nefarious interests within the statute, concluding that a violation for accessing a protected computer "without authorization" or in "excess of

> authorized access" occurs *only when initial access or the access of certain information is not permitted in the first instance*. Those courts have generally reasoned that the CFAA is intended to punish computer hackers, electronic trespassers and other "outsiders" but not employees who abuse computer access privileges to misuse information derived from their employment.

(citations omitted) (emphasis added).

At first, the district court rejected Nosal's argument, holding that a person's accessing a computer "knowingly and with intent to defraud . . . renders the access unauthorized or in excess of authorization." Thus, the court refused to dismiss Counts 2 through 9 of the superseding indictment.[2]

After the district court denied Nosal's motion to dismiss, however, we decided *LVRC Holdings LLC v. Brekka*, which considered the construction of the phrase "without authorization." Nosal then filed a motion to reconsider, arguing that *Brekka* required dismissal of the CFAA counts. The district court agreed with Nosal as to most of the counts and dismissed Counts 2 and 4-7. In doing so, the court held that the *Brekka* decision compelled the dismissal and that the phrase "exceeds authorized access" as used in § 1030 means having permission to access a *portion* of a computer (or certain information on a computer), but accessing a different portion of the computer (or different information on the computer) that the employee is not entitled to access under any circumstances.

[2]The district court also denied Nosal's motion with respect to Counts 1, 10, and 11, alleging violations of the Economic Espionage Act, 18 U.S.C. § 1832. It granted Nosal's motion to dismiss with respect to Counts 12 through 20, alleging mail fraud in violation of 18 U.S.C. §§ 1341 and 1349. These rulings are not before us.

The district court stated that intent is irrelevant in determining whether a person exceeds authorized access, even if an employee's access to the computer is expressly limited by the employer's use restrictions. The district court gave as an example the following hypothetical:

> [I]f a person is authorized to access the "F" drive on a computer or network but is not authorized to access the "G" drive of that same computer or network, the individual would "exceed authorized access" if he obtained or altered anything on the "G" drive.

On the other hand, if the employee accessed the "F" drive in a manner that violates the employer's access restrictions, the employee would not have violated subsection (a)(4) — even if he did so with the intent to defraud, furthered the intended fraud, and obtained something of value.

Because the conspirators had authority to obtain information from the Searcher database for legitimate Korn/Ferry *business purposes*, the district court held that they did not exceed their authorized access by doing so, even if they acted with a fraudulent intent.[3] The government appealed.

II

STANDARD OF REVIEW

We review de novo a district court's dismissal of an indictment, or of certain counts of that indictment, based on the district court's interpretation of a federal statute. *United States v. Boren*, 278 F.3d 911, 913 (9th Cir. 2002).

[3]The district court refused to dismiss Counts 3, 8, and 9 because it was possible under those allegations that one or more of Nosal's co-conspirators accessed the system *after* their employment had ended — which would constitute access "without authorization."

III

DISCUSSION

We are not faced in this appeal with an argument that Nosal's accomplices accessed the Searcher database "without authorization." The question we must answer here is whether those accomplices could have *exceeded* their authorized access by accessing information that they were entitled to access only under limited circumstances. We hold that an employee "exceeds authorized access" under § 1030 when he or she violates the employer's computer access restrictions — including use restrictions.

A

THE STATUTORY LANGUAGE

[1] "The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data." *Brekka*, 581 F.3d at 1131. We begin our task of deciphering the meaning of this federal statute, as always, with its plain language. *See United States v. Maciel-Alcala*, 612 F.3d 1092, 1098 (9th Cir. 2010). Subsection (a)(4) subjects to punishment anyone who

> 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.

18 U.S.C. § 1030(a)(4).

[2] Although the statute does not define the phrase "without authorization," it does state that "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." *Id.* § 1030(e)(6) (emphasis added).

[3] The government contends that Nosal's interpretation of "exceeds authorized access" would render superfluous the word "so" in the statutory definition. We agree. "So" in this context means "in a manner or way that is indicated or suggested." *Webster's Third New Int'l Dictionary* 2159 (Philip Babcock Gove, ed. 2002). Thus, an employee exceeds authorized access under § 1030(e)(6) when the employee uses that authorized access "to obtain or alter information in the computer that the accesser is not entitled [in that manner] to obtain or alter." We decline to render meaningless a word duly enacted by Congress. *See Corley v. United States*, 129 S. Ct. 1558, 1566 (2009) ("[O]ne of the most basic interpretive canons [is] that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." (internal quotation marks and alteration omitted)). Because the statute refers to an accesser who is not entitled to access information in a certain manner, whether someone has exceeded authorized access must be defined by those access limitations. The plain language of the statute supports the government's interpretation.

B

LVRC HOLDINGS LLC v. BREKKA

We must now address Nosal's argument that *Brekka* requires us to decide this appeal in his favor notwithstanding the plain meaning of the phrase "exceeds authorized access."

[4] We held in *Brekka* that it is the *employer's* actions that determine whether an employee acts without authorization to access a computer in violation of § 1030. Brekka was an employee at an addiction treatment center who was negotiating with his employer, LVRC Holdings, for the purchase of an ownership interest in the business. During the course of those negotiations, Brekka emailed several business documents to his and his wife's personal email accounts. The negotiations broke down, and Brekka left his employment with LVRC. *Brekka*, 581 F.3d at 1129-30. LVRC later discovered the emails Brekka had sent to himself and sued him under § 1030(g), which provides for a private right of action under the CFAA.

Relying primarily on *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), LVRC argued that Brekka acted "without authorization" because by accessing and emailing the documents he acted contrary to his employer's interest. *In Citrin*, the Seventh Circuit held that an employee loses authorization to use a computer when the employee violates a state law duty of loyalty because, based on common law agency principles, the employee's actions terminated the employer-employee relationship "and with it his authority to access the [computer]." *Id.* at 420-21. In the Seventh Circuit, therefore, an employee accesses a computer "without authorization" the moment the employee uses a computer or information on a computer in a manner adverse to the employer's interest.

We rejected the *Citrin* approach as inconsistent with our conclusion that, for purposes of § 1030, it is the action of the *employer* that determines whether an employee is authorized to access the computer:

> If the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary

> duty to an employer would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner.

Brekka, 581 F.3d 1135. How is an employee supposed to know when authorization has been revoked if the employer does not inform the employee of the revocation? It was this concern that motivated us to apply the rule of lenity, " 'which is rooted in considerations of notice [and] requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government.' " *Id.* at 1135 (quoting *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006)). Because LVRC had not notified Brekka of any restrictions on his access to the computer, Brekka had no way to know whether — or when — his access would have become unauthorized. Therefore, as long as an employee has *some* permission to use the computer for *some* purpose, that employee accesses the computer *with* authorization even if the employee acts with a fraudulent intent.

In determining that the phrase "without authorization" encompassed only those situations where a defendant had no authorization to access a computer at all, we also relied heavily on the statutory definition of the phrase "exceeds authorized access." *Id.* at 1133. We rejected the argument that accessing a computer "without authorization" could mean accessing the computer for unauthorized purposes because to accept such an argument would effectively remove the "exceeds authorized access" language from the statute entirely. Rather, the "sensible interpretation" we adopted in *Brekka* gives effect to both prongs:

> As this definition [in § 1030(e)(6)] makes clear, 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." On the other hand, a person who uses a computer "without authorization"

> has no rights, limited or otherwise, to access the computer in question.

Id. (emphasis added) (second alteration in original).

[5] Our decision today that an employer's use restrictions define whether an employee "exceeds authorized access" is simply an application of *Brekka*'s reasoning. As we held in that case, "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.' " *Id.* at 1133. Based on the " 'ordinary, contemporary, [and] common meaning' " of the word "authorization," *id.* at 1132 (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979)), we held that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it," *id.* at 1133. Therefore, the *only* logical interpretation of "exceeds authorized *access" is that the employer has placed* limitations on the employee's "permission to use" the computer and the employee has violated — or "exceeded" — those limitations.

We do face a substantial factual distinction in this case: the existence of access restrictions instituted by the employer. The employee in *Brekka* had unfettered access to the company computer — "LVRC and Brekka did not have a written employment agreement, nor did LVRC promulgate employee guidelines that would prohibit employees from emailing LVRC documents to personal computers." *Id.* at 1129. Therefore, Brekka did not exceed his authorized access any more than he acted without authorization: he was entitled to obtain the information because he had not acted in a way that violated any access restrictions.

[6] By contrast, Korn/Ferry employees were subject to a computer use policy that placed clear and conspicuous restrictions on the employees' access both to the system in general and to the Searcher database in particular. By using their

authorized access to defraud Korn/Ferry in violation of Korn/Ferry's access restrictions, Nosal's accomplices certainly had fair warning that they were subjecting themselves to criminal liability. For this reason, we conclude that the rule of lenity, which applied with particular force in interpreting the phrase "without authorization," does not support ignoring the statutory language and the core rationale of *Brekka*. Nosal's argument that the government's "Orwellian" interpretation would improperly criminalize certain actions depending only on the vagaries and whims of the employer is foreclosed by *Brekka*, which held unequivocally that under § 1030 the *employer* determines whether an employee is authorized. *Id.* at 1133, 1135. 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.

C

OTHER CIRCUIT AUTHORITY

The other circuits that have addressed the meaning of "exceeds authorized access" in the context of employers' access restrictions have also determined that the phrase encompasses such restrictions. In *United States v. John*, 597 F.3d 263 (5th Cir. 2010), the Fifth Circuit held that an employee of Citigroup exceeded her authorized access when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud. The Fifth Circuit stated that "at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime," the user is subject to prosecution under § 1030. *Id.* at 271.

The Eleventh Circuit recently held that an employee of the Social Security Administration exceeded his authorized access under § 1030(a)(2) when he obtained personal infor-

mation about former girlfriends and potential paramours and used that information to send flowers or to show up at women's homes. *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010). In so doing, the court distinguished *Brekka* along the same lines that we do here:

> [In *Brekka*, the] treatment center had no policy prohibiting employees from emailing company documents to personal email accounts, and there was no dispute that Brekka had been authorized to obtain the documents or to send the emails while he was employed. *Brekka* is distinguishable because *the Administration told [Defendant] Rodriguez that he was not authorized to obtain personal information for nonbusiness reasons*.

Id. (citations omitted) (emphasis added). *See also EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001) (holding that an employee likely exceeded his authorized access when he used that access to disclose information in violation of a confidentiality agreement into which the employee voluntarily entered).

For all of the foregoing reasons, we now join our sister circuits.

D

INTENT AND CAUSATION

[7] 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. Rather, an employee violates this subsection if the employee (1) violates an employer's restriction on com-

puter access, (2) with an *intent to defraud*, and (3) by that action "*furthers the intended fraud* and *obtains anything of value*." 18 U.S.C. § 1030(a)(4) (emphasis added). 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).

IV

CONCLUSION

Brekka held that a person accesses a computer without authorization "when the person has not received permission to use the computer for any purpose." 581 F.3d at 1135. Today, we clarify that under the CFAA, an employee accesses a computer in excess of his or her authorization when that access violates the employer's access restrictions, which may include restrictions on the employee's use of the computer or of the information contained in that computer. We reaffirm our previous conclusion that "an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access.' " *Id.* at 1133 (alteration in original). Therefore, we REVERSE the district court's decision and REMAND with instructions to reinstate Counts 2 and 4-7 of the superseding indictment.

CAMPBELL, District Judge, dissenting:

Because I believe that construing "exceeds authorized access" to include "violating an employer's computer access restrictions — including use restrictions" does not further Congress's stated purpose in enacting the CFAA, and in fact

renders one of the statute's provisions unconstitutionally vague, I must respectfully dissent.

The majority focuses on the intent requirement of 18 U.S.C. § 1030(a)(4) to explain why its interpretation of "exceeds authorized access" does not "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." The majority notes:

> [S]ubsection (a)(4) does not criminalize the mere violation of an employer's use restrictions. Rather, an employee violates this subsection if the employee (1) violates an employer's restriction on computer access, (2) with an *intent to defraud*, and (3) by that action "*furthers the intended fraud* and *obtains anything of value*." 18 U.S.C. § 1030(a)(4) (emphasis added). 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).

But it is a firm rule of statutory construction that "identical words used in different parts of the same statute are generally presumed to have the same meaning." *IBP, Inc. v. Alvarez*, 546 U.S. 21, 34 (2005). "Exceeds authorized access" appears in other provisions of the statute, including the much broader § 1030(a)(2)(C), *which has no intent requirement*.

Under § 1030(a)(2)(C), a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer," is guilty of a crime, where a "protected computer" includes any computer connected to the internet,

see 18 U.S.C. § 1030(e)(2)(B) ("[T]he term 'protected computer' means a computer . . . which is used in or affecting interstate or foreign commerce or communication . . . .").

Accordingly, under the majority's interpretation, any person who obtains information from any computer connected to the internet, in violation of her employer's computer use restrictions, is guilty of a federal crime under § 1030(a)(2)(C). For example, Mr. Nosal's employer, Korn/Ferry, prohibited use of its proprietary database except for legitimate Korn/Ferry business. Under the majority's interpretation, had Mr. Nosal ever viewed any information in that database out of curiosity instead of for legitimate Korn/Ferry business, he would be guilty of a federal crime.[1]

DEFINITENESS

"[T]he void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). A statute imposing criminal liability according to the terms of employers' computer access restrictions would not give fair notice of what conduct is prohibited, because employers' computer access restrictions are not necessarily drafted with the definiteness or precision that would be required for a criminal statute.[2,3]

[1]Further, *Brekka's* holding is rendered meaningless by the majority's holding, because, to invoke the federal criminal law, employers merely need to include in their computer access restrictions that an employee's authorization to access a computer ends when he breaches his duty of loyalty.

[2]By essentially incorporating privately drafted computer access restrictions into a criminal statute, the majority's construction binds Congress to the language of those restrictions.

[3]In addition, computer use policies can be altered without notice. Under the majority's interpretation of "exceeds authorization," an employee

ARBITRARY ENFORCEMENT

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.

In *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), the question before the district court was "whether an intentional breach of an Internet website's terms of service, without more, is sufficient to constitute a misdemeanor violation of the CFAA; and, if so, would the statute, as so interpreted, survive constitutional challenges on the grounds of vagueness and related doctrines." *Drew*, 259 F.R.D. at 451.

In holding that the government's interpretation of the CFAA would render § 1030(a)(2)(C) unconstitutionally vague, the court explained that:

> if every [breach of an Internet website's terms of service] does qualify [as a violation of the CFAA], then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution. All manner of situations will be covered . . . . All can be prosecuted. Given the 'standardless sweep that results, federal law enforcement entities would be improperly free to 'pursue their personal predilections.'

---

would have an affirmative obligation to stay current on her employer's computer use policy to know what conduct could be criminally punished. Implicitly addressing this issue, the majority builds in a necessary safeguard: Although it is the *employer* who determines whether an employee is "authorized" or "exceeds authorization," the employee must "ha[ve] knowledge" of the employer's limitations in order to exceed authorized access. This knowledge requirement is not found in the statute, and only becomes necessary upon adopting the majority's interpretation of "exceeds authorization."

Drew, 259 F.R.D. at 467 (quoting *Kolender v. Lawson*, 461 U.S. 352, 358 (1983)).

The majority's reading of § 1030(a)(4) similarly renders § 1030(a)(2)(C) unconstitutionally vague.

STATUTORY CONSTRUCTION

It is a cardinal principle of statutory construction that an Act of Congress should be construed, where "fairly possible," in a manner that does not result in its invalidity. *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001). Here, where "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), "exceeds authorized access" could be interpreted as the majority has interpreted it, rendering § 1030(a)(2)(C) of the statute unconstitutionally vague.

Or, the "so" on which the majority's interpretation hinges could have been added for emphasis alone, as was undoubtedly the case in another provision of the same statute. *See* 18 U.S.C. § 1030(a)(1) (proscribing theft of government secrets by someone "with reason to believe that *such information so obtained* could be used to the injury of the United States" (emphasis added)). This latter interpretation is consistent with this court's interpretation of the same phrase in *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." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2010).

Because Congress enacted the CFAA to curb computer hacking, *see* S. Rep. No. 99-432 at 2-3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480-2481, the latter interpretation is not only "fairly possible," but in fact conforms more closely to what Congress intended. When the CFAA was enacted, "computer crime" was considered a new type of

crime that existing criminal laws were insufficient to address. *See* S. Rep. No. 99-432 at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2479. For example, exceeding one's authorized access to a computer by hacking into a drive that one is never authorized to access would be a "computer crime," which Congress intended to proscribe. On the other hand, under the majority's interpretation of "exceeds authorized access," the CFAA would proscribe fraud (a standalone crime) that happens to be effectuated through the use of a computer and in violation of a computer use policy. This was not Congress's intent.

For the reasons stated above, I respectfully dissent.