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
December 15, 2011—San Francisco, California

Filed April 10, 2012

Before: Alex Kozinski, Chief Judge, Harry Pregerson, Barry G. Silverman, M. Margaret McKeown, Kim McLane Wardlaw, Ronald M. Gould, Richard A. Paez, Richard C. Tallman, Richard R. Clifton, Jay S. Bybee and Mary H. Murguia, Circuit Judges.

Opinion by Chief Judge Kozinski;
Dissent by Judge Silverman

COUNSEL

Jenny C. Ellickson (argued), Lanny A. Breuer, Jaikumar Ramaswamy, Scott N. Schools, Kyle Francis Waldinger, United States Department of Justice, San Francisco, California, for the plaintiff-appellant.

Ted Sampsell Jones (argued), Dennis P. Riordan, Donald M. Horgan, Riordan & Horgan, San Francisco, California, for the defendant-appellee.

Kathryn M. Davis, Law Office of Kathryn M. Davis, Pasadena, California, filed a brief on behalf of amicus curiae En Pointe Technologies, Inc., in support of the plaintiff-appellant.

Geoffrey M. Howard, David B. Salmons, Bryan M. Killian, Bingham McCutchen, LLP, San Francisco, California, filed a brief on behalf of amicus curiae Oracle America Inc., in support of the plaintiff-appellant.

Kenneth M. Stern, Law Offices of Kenneth M. Stern, Woodland Hills, California, filed a brief in support of the plaintiff-appellant.

Marcia Hofmann, Electronic Frontier Foundation, San Francisco, California, filed a brief on behalf of amicus curiae Electronic Frontier Foundation in support of the defendant-appellee.

OPINION

KOZINSKI, Chief Judge:

Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Some-

times we use them for play at work. Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website? This depends on how broadly we read the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

FACTS

David Nosal used to work for Korn/Ferry, an executive search firm. Shortly after he left the company, he convinced some of his former colleagues who were still working for Korn/Ferry to help him start a competing business. The employees used their log-in credentials to download source lists, names and contact information from a confidential database on the company's computer, and then transferred that information to Nosal. The employees were authorized to access the database, but Korn/Ferry had a policy that forbade disclosing confidential information.[1] The government indicted Nosal on twenty counts, including trade secret theft, mail fraud, conspiracy and violations of the CFAA. The CFAA counts charged Nosal with violations of 18 U.S.C. § 1030(a)(4), for aiding and abetting the Korn/Ferry employees in "exceed[ing their] authorized access" with intent to defraud.

Nosal filed a motion to dismiss the CFAA counts, arguing that the statute targets only hackers, not individuals who access a computer with authorization but then misuse information they obtain by means of such access. The district court initially rejected Nosal's argument, holding that when a person accesses a computer "knowingly and with the intent to defraud . . . [it] renders the access unauthorized or in excess

[1]The opening screen of the database also included the warning: "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only."

of authorization." Shortly afterwards, however, we decided *LVRC Holdings LLC* v. *Brekka*, 581 F.3d 1127 (9th Cir. 2009), which construed narrowly the phrases "without authorization" and "exceeds authorized access" in the CFAA. Nosal filed a motion for reconsideration and a second motion to dismiss.

The district court reversed field and followed *Brekka*'s guidance that "[t]here is simply no way to read [the definition of 'exceeds authorized access'] to incorporate corporate policies governing use of information unless the word alter is interpreted to mean misappropriate," as "[s]uch an interpretation would defy the plain meaning of the word alter, as well as common sense." Accordingly, the district court dismissed counts 2 and 4-7 for failure to state an offense. The government appeals. We have jurisdiction over this interlocutory appeal. 18 U.S.C. § 3731; *United States* v. *Russell*, 804 F.2d 571, 573 (9th Cir. 1986). We review de novo. *United States* v. *Boren*, 278 F.3d 911, 913 (9th Cir. 2002).

DISCUSSION

[1] The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This language can be read either of two ways: First, as Nosal suggests and the district court held, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data: He would "exceed[ ] authorized access" if he looks at the customer lists. Second, as the government proposes, the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. For example, an employee may be authorized to

access customer lists in order to do his job but not to send them to a competitor.

[2] The government argues that the statutory text can support only the latter interpretation of "exceeds authorized access." In its opening brief, it focuses on the word "entitled" in the phrase an "accesser is not *entitled* so to obtain or alter." *Id.* § 1030(e)(6) (emphasis added). Pointing to one dictionary definition of "entitle" as "to furnish with a right," *Webster's New Riverside University Dictionary* 435, the government argues that Korn/Ferry's computer use policy gives employees certain rights, and when the employees violated that policy, they "exceed[ed] authorized access." But "entitled" in the statutory text refers to how an accesser "obtain[s] or alter[s]" the information, whereas the computer use policy uses "entitled" to limit how the information is used after it is obtained. This is a poor fit with the statutory language. An equally or more sensible reading of "entitled" is as a synonym for "authorized."[2] So read, "exceeds authorized access" would refer to data or files on a computer that one is not authorized to access.

In its reply brief and at oral argument, the government focuses on the word "so" in the same phrase. *See* 18 U.S.C. § 1030(e)(6) ("accesser is not entitled *so* to obtain or alter" (emphasis added)). The government reads "so" to mean "in that manner," which it claims must refer to use restrictions. In the government's view, reading the definition narrowly would render "so" superfluous.

The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. This places a great deal of weight on a

[2] *Fowler's* offers these as usage examples: "Everyone is entitled to an opinion" and "We are entitled to make personal choices." "Fowler's Modern English Usage: Entitled," Answers.com, http://www.answers.com/topic/entitle (last visited Mar. 5, 2012).

two-letter word that is essentially a conjunction. If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.[3] Under the presumption that Congress acts interstitially, we construe a statute as displacing a substantial portion of the common law only where Congress has clearly indicated its intent to do so. *See Jones* v. *United States*, 529 U.S. 848, 858 (2000) ("[U]nless Congress conveys its purpose clearly, it will not be deemed to have significantly changed the federal-state balance in the prosecution of crimes." (internal quotation marks omitted)).

In any event, the government's "so" argument doesn't work because the word has meaning even if it doesn't refer to use restrictions. Suppose an employer keeps certain information in a separate database that can be viewed on a computer screen, but not copied or downloaded. If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not "entitled *so* to obtain." Or, let's say an employee is given full access to the information, provided he logs in with his username and password. In an effort to cover his tracks, he uses another employee's login to copy information from the database. Once again, this would be an employee who is authorized to access the information but does so in a manner he was not authorized "so to obtain." Of course, this all assumes that "so" must have a substantive

[3]Congress did just that in the federal trade secrets statute—18 U.S.C. § 1832—where it used the common law terms for misappropriation, including "with intent to convert," "steals," "appropriates" and "takes." *See* 18 U.S.C. § 1832(a). The government also charged Nosal with violating 18 U.S.C. § 1832, and those charges remain pending.

meaning to make sense of the statute. But Congress could just as well have included "so" as a connector or for emphasis.[4]

While the CFAA is susceptible to the government's broad interpretation, we find Nosal's narrower one more plausible. Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, "[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system." S. Rep. No. 99-432, at 9 (1986) (Conf. Rep.). The government agrees that the CFAA was concerned with hacking, which is why it also prohibits accessing a computer "without authorization." According to the government, *that* prohibition applies to hackers, so the "exceeds authorized access" prohibition must apply to people who are authorized to use the computer, but do so for an unauthorized purpose. But it is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.[5]

[4]The government fails to acknowledge that its own construction of "exceeds authorized access" suffers from the same flaw of superfluity by rendering an entire element of subsection 1030(a)(4) meaningless. Subsection 1030(a)(4) requires a person to (1) knowingly and (2) with intent to defraud (3) access a protected computer (4) without authorization or exceeding authorized access (5) in order to further the intended fraud. *See* 18 U.S.C. § 1030(a)(4). Using a computer to defraud the company necessarily contravenes company policy. Therefore, if someone accesses a computer with intent to defraud—satisfying elements (2) and (3)—he would invariably satisfy (4) under the government's definition.

[5]Although the legislative history of the CFAA discusses this anti-hacking purpose, and says nothing about exceeding authorized use of

The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer.

[3] The government argues that defendants here did have notice that their conduct was wrongful by the fraud and materiality requirements in subsection 1030(a)(4), which punishes whoever:

> 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.

---

information, the government claims that the legislative history supports its interpretation. It points to an earlier version of the statute, which defined "exceeds authorized access" as "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." Pub. L. No. 99-474, § 2(c), 100 Stat. 1213 (1986). But *that* language was removed and replaced by the current phrase and definition. And Senators Mathias and Leahy—members of the Senate Judiciary Committee—explained that the purpose of replacing the original broader language was to "remove[ ] from the sweep of the statute one of the murkier grounds of liability, under which a[n] . . . employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances." S. Rep. No. 99-432, at 21. Were there any need to rely on legislative history, it would seem to support Nosal's position rather than the government's.

18 U.S.C. § 1030(a)(4). But "exceeds authorized access" is used elsewhere in the CFAA as a basis for criminal culpability without intent to defraud. Subsection 1030(a)(2)(C) requires only that the person who "exceeds authorized access" have "obtain[ed] . . . information from any protected computer." Because "protected computer" is defined as a computer affected by or involved in interstate commerce—effectively all computers with Internet access—the government's interpretation of "exceeds authorized access" makes every violation of a private computer use policy a federal crime. *See id.* § 1030(e)(2)(B).

[4] The government argues that our ruling today would construe "exceeds authorized access" only in subsection 1030(a)(4), and we could give the phrase a narrower meaning when we construe other subsections. This is just not so: Once we define the phrase for the purpose of subsection 1030(a)(4), that definition must apply equally to the rest of the statute pursuant to the "standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning." *Powerex Corp.* v. *Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007). The phrase appears five times in the first seven subsections of the statute, including subsection 1030(a)(2)(C). *See* 18 U.S.C. § 1030(a)(1), (2), (4) and (7). Giving a different interpretation to each is impossible because Congress provided a *single* definition of "exceeds authorized access" for all iterations of the statutory phrase. *See id.* § 1030(e)(6). Congress obviously meant "exceeds authorized access" to have the same meaning throughout section 1030. We must therefore consider how the interpretation we adopt will operate wherever in that section the phrase appears.

In the case of the CFAA, the broadest provision is subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent. Were we to adopt the government's pro-

posed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct.

Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes. While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you *could* be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit.[6] Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement.[7]

[6]Enforcement of the CFAA against minor workplace dalliances is not chimerical. Employers have invoked the CFAA against employees in civil cases. In a recent Florida case, after an employee sued her employer for wrongful termination, the company counterclaimed that plaintiff violated section 1030(a)(2)(C) by making personal use of the Internet at work—checking Facebook and sending personal email—in violation of company policy. *See Lee* v. *PMSI, Inc.*, No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011). The district court dismissed the counterclaim, but it could not have done so if "exceeds authorized access" included violations of private computer use policies.

[7]This concern persists even if intent to defraud is required. Suppose an employee spends six hours tending his FarmVille stable on his work computer. The employee has full access to his computer and the Internet, but the company has a policy that work computers may be used only for business purposes. The employer should be able to fire the employee, but that's quite different from having him arrested as a federal criminal. Yet, under the government's construction of the statute, the employee "exceeds authorized access" by using the computer for non-work activities. Given that the employee deprives his company of six hours of work a day, an aggressive prosecutor might claim that he's defrauding the company, and thereby violating section 1030(a)(4).

Employer-employee and company-consumer relationships are traditionally governed by tort and contract law; the government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law. Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read. Consider the typical corporate policy that computers can be used only for business purposes. What exactly is a "nonbusiness purpose"? If you use the computer to check the weather report for a business trip? For the company softball game? For your vacation to Hawaii? And if minor personal uses are tolerated, how can an employee be on notice of what constitutes a violation sufficient to trigger criminal liability?

Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.

The effect this broad construction of the CFAA has on workplace conduct pales by comparison with its effect on everyone else who uses a computer, smart-phone, iPad, Kindle, Nook, X-box, Blu-Ray player or any other Internet-enabled device. The Internet is a means for communicating via computers: Whenever we access a web page, commence a download, post a message on somebody's Facebook wall, shop on Amazon, bid on eBay, publish a blog, rate a movie on IMDb, read www.NYT.com, watch YouTube and do the thousands of other things we routinely do online, we are using

one computer to send commands to other computers at remote locations. Our access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands.[8]

For example, it's not widely known that, up until very recently, Google forbade minors from using its services. *See* Google Terms of Service, effective April 16, 2007—March 1, 2012, § 2.3, http://www.google.com/intl/en/ policies/terms/ archive/20070416 ("You may not use the Services and may not accept the Terms if . . . you are not of legal age to form a binding contract with Google . . . .") (last visited Mar. 4, 2012).[9] Adopting the government's interpretation would turn vast numbers of teens and pre-teens into juvenile delinquents—and their parents and teachers into delinquency contributors. Similarly, Facebook makes it a violation of the terms of ser-

[8]*See, e.g.*, Craigslist Terms of Use (http://www.craigslist.org/about/terms.of.use), eBay User Agreement (http://pages.ebay.com/help/policies/user-agreement.html?rt=nc), eHarmony Terms of Service (http://www.eharmony.com/about/terms), Facebook Statement of Rights and Responsibilities (http://www.facebook.com/#!/legal/terms), Google Terms of Service (http://www.google.com/intl/en/policies/terms/), Hulu Terms of Use (http://www.hulu.com/terms), IMDb Conditions of Use (http://www.imdb.com/help/show_article?conditions), JDate Terms and Conditions of Service (http://www.jdate.com/Applications/Article/ArticleView.aspx?CategoryID=1948&ArticleID=6498&HideNav=True#service), LinkedIn User Agreement (http://www.linkedin.com/static?key=user_agreement), Match.com Terms of Use Agreement (http://www.match.com/registration/ membagr.aspx?lid=4), MySpace.com Terms of Use Agreement (http://www.myspace.com/Help/Terms?pm_cmp=ed_footer), Netflix Terms of Use (https://signup.netflix.com/TermsOfUse), Pandora Terms of Use (http://www.pandora.com/legal), Spotify Terms and Conditions of Use (http://www.spotify.com/us/legal/end-user-agreement/), Twitter Terms of Service (http://twitter.com/tos), Wikimedia Terms of Use (http://wikimediafoundation.org/wiki/Terms_of_use) and YouTube Terms of Service (http://www.youtube.com/t/terms).

[9]A number of other well-known websites, including Netflix, eBay, Twitter and Amazon, have this age restriction.

vice to let anyone log into your account. *See* Facebook Statement of Rights and Responsibilities § 4.8 http://www.facebook.com/legal/terms ("You will not share your password, . . . let anyone else access your account, or do anything else that might jeopardize the security of your account.") (last visited Mar. 4, 2012). Yet it's very common for people to let close friends and relatives check their email or access their online accounts. Some may be aware that, if discovered, they may suffer a rebuke from the ISP or a loss of access, but few imagine they might be marched off to federal prison for doing so.

Or consider the numerous dating websites whose terms of use prohibit inaccurate or misleading information. *See, e.g.*, eHarmony Terms of Service § 2(I), http://www.eharmony.com/about/terms ("You will not provide inaccurate, misleading or false information to eHarmony or to any other user.") (last visited Mar. 4, 2012). Or eBay and Craigslist, where it's a violation of the terms of use to post items in an inappropriate category. *See, e.g.*, eBay User Agreement, http://pages.ebay.com/help/policies/user-agreement.html ("While using eBay sites, services and tools, you will not: post content or items in an inappropriate category or areas on our sites and services . . . ."") (last visited Mar. 4, 2012). Under the government's proposed interpretation of the CFAA, posting for sale an item prohibited by Craigslist's policy, or describing yourself as "tall, dark and handsome," when you're actually short and homely, will earn you a handsome orange jumpsuit.

Not only are the terms of service vague and generally unknown—unless you look real hard at the small print at the bottom of a webpage—but website owners retain the right to change the terms at any time and without notice. *See, e.g.*, YouTube Terms of Service § 1.B, http://www.youtube.com/t/terms ("YouTube may, in its sole discretion, modify or revise these Terms of Service and policies at any time, and you agree to be bound by such modifications or revisions.") (last

visited Mar. 4, 2012). Accordingly, behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.

The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor. *Cf. United States* v. *Stevens*, 130 S. Ct. 1577, 1591 (2010) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly."). And it's not clear we *can* trust the government when a tempting target comes along. Take the case of the mom who posed as a 17-year-old boy and cyber-bullied her daughter's classmate. The Justice Department prosecuted her under 18 U.S.C. § 1030(a)(2)(C) for violating MySpace's terms of service, which prohibited lying about identifying information, including age. *See United States* v. *Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). Lying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight. The difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after.

In *United States* v. *Kozminski*, 487 U.S. 931 (1988), the Supreme Court refused to adopt the government's broad interpretation of a statute because it would "criminalize a broad range of day-to-day activity." *Id.* at 949. Applying the rule of lenity, the Court warned that the broader statutory interpretation would "delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes" and would "subject individuals to the risk of arbitrary or discriminatory prosecution and conviction." *Id.* By giving that much power to prosecutors, we're inviting discriminatory and arbitrary enforcement.

We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of

corporate computer use restrictions or violations of a duty of loyalty. *See United States* v. *Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States* v. *John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC* v. *Citrin*, 440 F.3d 418 (7th Cir. 2006). These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access." They therefore failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid "making criminal law in Congress's stead." *United States* v. *Santos*, 553 U.S. 507, 514 (2008).

We therefore respectfully decline to follow our sister circuits and urge them to reconsider instead. For our part, we continue to follow in the path blazed by *Brekka*, 581 F.3d 1127, and the growing number of courts that have reached the same conclusion. These courts recognize that the plain language of the CFAA "target[s] 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 Commc'ns, Inc.* 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."); *Diamond Power Int'l, Inc.* v. *Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) ("[A] violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted."); *Int'l Ass'n of Machinists & Aerospace Workers* v. *Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005) ("[T]he CFAA, however, do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access.").

CONCLUSION

[5] We need not decide today whether Congress *could* base criminal liability on violations of a company or website's

computer use restrictions. Instead, we hold that the phrase "exceeds authorized access" in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly. The rule of lenity requires "penal laws . . . to be construed strictly." *United States* v. *Wiltberger*, 18 U.S. (5 Wheat.) 76, 95 (1820). "[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Jones*, 529 U.S. at 858 (internal quotation marks and citation omitted).

The rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals. "[B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity." *United States* v. *Bass*, 404 U.S. 336, 348 (1971). "If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [Nosal] engaged, then 'we must choose the interpretation least likely to impose penalties unintended by Congress.' " *United States* v. *Cabaccang*, 332 F.3d 622, 635 n.22 (9th Cir. 2003) (quoting *United States* v. *Arzate-Nunez*, 18 F.3d 730, 736 (9th Cir. 1994)).

[6] This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere. *See supra* note 3. Therefore, we hold that "exceeds authorized access" in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.

[7] Because Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail to meet the element of "without authorization, or exceeds authorized access" under 18 U.S.C. § 1030(a)(4). Accordingly, we affirm the judgment of the district court dismissing counts 2 and 4-7 for failure to state an offense. The government may, of course, prosecute Nosal on the remaining counts of the indictment.

AFFIRMED.

SILVERMAN, Circuit Judge, with whom TALLMAN, Circuit Judge concurs, dissenting:

This case has nothing to do with playing sudoku, checking email, fibbing on dating sites, or any of the other activities that the majority rightly values. It has everything to do with stealing an employer's valuable information to set up a competing business with the purloined data, siphoned away from the victim, knowing such access and use were prohibited in the defendants' employment contracts. The indictment here charged that Nosal and his co-conspirators knowingly exceeded the access to a protected company computer they were given by an executive search firm that employed them; that they did so with the intent to defraud; and further, that they stole the victim's valuable proprietary information by means of that fraudulent conduct in order to profit from using it. In ridiculing scenarios not remotely presented by *this* case, the majority does a good job of knocking down straw men — far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy.

The majority also takes a plainly written statute and parses it in a hyper-complicated way that distorts the obvious intent

of Congress. No other circuit that has considered this statute finds the problems that the majority does.

18 U.S.C. § 1030(a)(4) is quite clear. It states, in relevant part:

> (a) Whoever—
>
> > (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 . . .
>
> shall be punished . . . .

Thus, it is perfectly clear that a person with *both* the requisite mens rea *and* the specific intent to defraud — but *only* such persons — can violate this subsection in one of two ways: first, by accessing a computer without authorization, or second, by exceeding authorized access. 18 U.S.C. § 1030(e)(6) defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

"As this definition 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.' " *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).

"[T]he definition of the term 'exceeds authorized access' from § 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer. The plain language of the statute therefore indicates that

'authorization' depends on actions taken by the employer." *Id.* at 1135. In *Brekka*, we explained that a person "exceeds authorized access" when that person has permission to access a computer but accesses information on the computer that the person is not entitled to access. *Id.* at 1133. In that case, an employee allegedly emailed an employer's proprietary documents to his personal computer to use in a competing business. *Id.* at 1134. We held that one does not exceed authorized access simply by "breach[ing] a state law duty of loyalty to an employer" and that, because the employee did not breach a contract with his employer, he could not be liable under the Computer Fraud and Abuse Act. *Id.* at 1135, 1135 n.7.

This is not an esoteric concept. A bank teller is entitled to access a bank's money for legitimate banking purposes, but not to take the bank's money for himself. A new car buyer may be entitled to take a vehicle around the block on a test drive. But the buyer would not be entitled — he would "exceed his authority" — to take the vehicle to Mexico on a drug run. A person of ordinary intelligence understands that he may be totally prohibited from doing something *altogether*, or authorized to do something but prohibited from going *beyond* what is authorized. This is no doubt why the statute covers not only "unauthorized access," but also "exceed[ing] authorized access." The statute contemplates both means of committing the theft.

The majority holds that a person "exceeds authorized access" only when that person has permission to access a computer generally, but is *completely* prohibited from accessing a different portion of the computer (or different information on the computer). The majority's interpretation conflicts with the plain language of the statute. Furthermore, none of the circuits that have analyzed the meaning of "exceeds authorized access" as used in the Computer Fraud and Abuse Act read the statute the way the majority does. Both the Fifth and Eleventh Circuits have explicitly held that employees

who knowingly violate clear company computer restrictions agreements "exceed authorized access" under the CFAA.

In *United States v. John*, 597 F.3d 263, 271-73 (5th Cir. 2010), the Fifth Circuit held that an employee of Citigroup exceeded her authorized access in violation of § 1030(a)(2) when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud. As the Fifth Circuit noted in *John*, "an employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business. An employee would 'exceed[ ] authorized access' if he or she used that access to obtain or steal information as part of a criminal scheme." *Id.* at 271 (alteration in original). At the very least, when an employee "knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of [a criminally fraudulent] scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access.' " *Id.* at 273.

Similarly, the Eleventh Circuit held in *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010), that an employee of the Social Security Administration exceeded his authorized access under § 1030(a)(2) when he obtained personal information about former girlfriends and potential paramours and used that information to send the women flowers or to show up at their homes. The court rejected Rodriguez's argument that unlike the defendant in *John*, his use was "not criminal." The court held: "The problem with Rodriguez's argument is that his use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access." *Id.*; *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).

The Third Circuit has also implicitly adopted the Fifth and Eleventh circuit's reasoning. In *United States v. Teague*, 646 F.3d 1119, 1121-22 (8th Cir. 2011), the court upheld a conviction under § 1030(a)(2) and (c)(2)(A) where an employee of a government contractor used his privileged access to a government database to obtain President Obama's private student loan records.

The indictment here alleges that Nosal and his co-conspirators knowingly exceeded the authority that they had to access their employer's computer, and that they did so with the intent to defraud and to steal trade secrets and proprietary information from the company's database for Nosal's competing business. It is alleged that at the time the employee co-conspirators accessed the database they *knew* they only were allowed to use the database for a legitimate business purpose because the co-conspirators allegedly signed an agreement which restricted the use and disclosure of information on the database except for legitimate Korn/Ferry business. Moreover, it is alleged that before using a unique username and password to log on to the Korn/Ferry computer and database, the employees were notified that the information stored on those computers were the property of Korn/Ferry and that to access the information without relevant authority could lead to disciplinary action and criminal prosecution. Therefore, it is alleged, that when Nosal's co-conspirators accessed the database to obtain Korn/Ferry's secret source lists, names, and contact information with the intent to defraud Korn/Ferry by setting up a competing company to take business away using the stolen data, they "exceed[ed their] authorized access" to a computer with an intent to defraud Korn/Ferry and therefore violated 18 U.S.C. § 1030(a)(4). If true, these allegations adequately state a crime under a commonsense reading of this particular subsection.

Furthermore, it does not advance the ball to consider, as the majority does, the parade of horribles that might occur under *different* subsections of the CFAA, such as subsection

(a)(2)(C), which does not have the scienter or specific intent to defraud requirements that subsection (a)(4) has. *Maldonado v. Morales*, 556 F.3d 1037, 1044 (9th Cir. 2009) ("The role of the courts is neither to issue advisory opinions nor to declare rights in hypothetical cases, but to adjudicate live cases or controversies.") (citation and internal quotation marks omitted). Other sections of the CFAA may or may not be unconstitutionally vague or pose other problems. We need to wait for an actual case or controversy to frame these issues, rather than posit a laundry list of wacky hypotheticals. I express no opinion on the validity or application of other subsections of 18 U.S.C § 1030, other than § 1030(a)(4), and with all due respect, neither should the majority.

The majority's opinion is driven out of a well meaning but ultimately misguided concern that if employment agreements or internet terms of service violations could subject someone to criminal liability, all internet users will suddenly become criminals overnight. I fail to see how anyone can seriously conclude that reading ESPN.com in contravention of office policy could come within the ambit of 18 U.S.C. § 1030(a)(4), a statute explicitly requiring an intent to defraud, the obtaining of something of value by means of that fraud, while doing so "knowingly." And even if an imaginative judge can conjure up far-fetched hypotheticals producing federal prison terms for accessing word puzzles, jokes, and sports scores while at work, well, . . . that is what an as-applied challenge is for. Meantime, back to this case, 18 U.S.C. § 1030(a)(4) clearly is aimed at, and limited to, knowing and intentional fraud. Because the indictment adequately states the elements of a valid crime, the district court erred in dismissing the charges.

I respectfully dissent.