676 F.3d 854
United States Court of Appeals,
Ninth Circuit.

UNITED STATES of America, Plaintiff–Appellant,
v.
David NOSAL, Defendant–Appellee.

No. 10–10038. | Argued and Submitted Dec. 15, 2011. | Filed April 10, 2012.

Synopsis

Background: Defendant charged with violating the Computer Fraud and Abuse Act (CFAA) and other crimes moved to dismiss the indictment. The United States District Court for the Northern District of California, Marilyn H. Patel, Senior District Judge, 2009 WL 981336, denied the motion. On reconsideration, however, the District Court, 2010 WL 934257, dismissed most of the CFAA charges. Government appealed. The Court of Appeals, 642 F.3d 781, initially reversed and remanded, but subsequently granted rehearing en banc, 661 F.3d 1180.

[Holding:] The Court of Appeals, Kozinski, Chief Judge, held that the phrase "exceeds authorized access," within the meaning of CFAA, is limited to access restrictions, not use restrictions.

Affirmed.

Silverman, Circuit Judge, filed a dissenting opinion in which Tallman, Circuit Judge concurred.

Opinion

Opinion by Chief Judge KOZINSKI; Dissent by Judge SILVERMAN.

***856 OPINION**

KOZINSKI, Chief Judge:

Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes 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 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 ***857** 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.

[. . .]

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

***860** 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]

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 ***861** 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 service 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 ***862** 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*, 559 U.S. 460, 130 S.Ct. 1577, 1591, 176 L.Ed.2d 435 (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, 108 S.Ct. 2751, 101 L.Ed.2d 788 (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, 108 S.Ct. at 2763. 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.

[. . .]

CONCLUSION

[4] 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, 5 L.Ed. 37 (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, 120 S.Ct. at 1912 (internal quotation marks and citation omitted).

[5] 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, 92 S.Ct. 515, 30 L.Ed.2d 488 (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)).

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 ***864** "exceeds authorized access" in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.

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:

[. . .]

I respectfully dissent.

Parallel Citations

36 IER Cases 865, 12 Cal. Daily Op. Serv. 3874, 2012 Daily Journal D.A.R. 4500

Footnotes

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."

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).

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.

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 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, 1986 U.S.C.C.A.N. 2479 at 2494. Were there any need to rely on legislative history, it would seem to support Nosal's position rather than the government's.

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).

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?Category ID=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/TermsOf Use), 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.