UNITED STATES OF AMERICA v. DAVID NOSAL

No. 10-10038

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

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 data- base 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 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 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). [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."

The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. 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. 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)).

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.

… 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. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement.

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). 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 State- ment 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 any- thing 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.

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 some- one an AUSA has reason to go after.

CONCLUSION

[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…

…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.