Digital Media & Data Privacy Law

# Taking a Walk Back to a Kinder, Gentler Interpretation of the Computer Fraud and Abuse Act

We don't usually talk about four-year-old court decisions in the first instance here. But the Ninth Circuit has issued a pair of noteworthy opinions interpreting the Computer Fraud and Abuse Act in the last few weeks. And to understand those it will help to understand *United States v. Nosal, 676 F.3d 854 (9th Cir. 2012)* an *en banc* opinion authored by Judge Kozinski.

**Facts**

The facts are mercifully short. 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.

**Charges**

The government indicted Nosal on twenty counts, including trade secret theft, mail fraud, conspiracy and violations of the Computer Fraud and Abuse Act. The CFAA

**Legal Discussion**

Did Nosal violate the statute? Kozinski wrote that the operative language could be read in two ways: First, as Nosal suggested, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files – what the kids call "hacking" these days. Second, as the government proposed, 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.

The government focused on two key words from the statute. It first examined 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," the government argued that Korn/Ferry's computer use policy gave employees certain rights, and when the employees violated that policy, they "exceed[ed] authorized access." But the court said "entitled" in the statute referred 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. Then the government looked at the word "so" in the same phrase. *See* 18 U.S.C. § 1030(e)(6) ("accesser is not entitled *so* to obtain or alter"

PUBLISHED

July 26, 2016

FILED UNDER

Digital Media & Data Privacy Law

TOPICS

Data Breach

AUTHOR

David Smyth

ARTICLE URL

http://brookspierce.com/news-insights/taking-walk-back-kinder-gentler-interpretation-computer-fraud-and-abuse-act

(emphasis added)). The government read "so" to mean "in that manner," which it claimed must refer to use restrictions. In the government's view, reading the definition narrowly would render "so" superfluous.

The court didn't agree, and said the government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. But the court also said a narrow interpretation of "so" did not render it superfluous. One of Judge Kozinski's hypotheticals went like this: 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."

The government agreed that the CFAA was concerned with hacking, but only the "without authorization" part. In the government's version, the "exceeds authorized access" prohibition applied to people who are authorized to use the computer, but do so for an unauthorized purpose. But the court said it was 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).

When employees routinely g-chat with friends, check Facebook, shop for clothes, and watch sports highlights, computer-use policies that prohibit those activities could transform them into federal felonies with a broad interpretation of the CFAA. While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer (one of Judge Kozinski's favorite pastimes, I guess), you *could* be, the court said. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement. Also, employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. In the end, the court was too creeped out by the prospect of federal crimes being defined by employer computer use policies. We'll get into these issues more for the rest of the week.