En Banc Ninth Circuit's *Nosal* Decision Restricts Computer Fraud and Abuse Act's Reach

2012-04-11

Yesterday the *en banc* Ninth Circuit, by a vote of 9-2, limited the reach of the Computer Fraud and Abuse Act ("CFAA") by holding that gaining authorized access to information on a computer system and then using the information for a purpose prohibited by a computer-use agreement, even for a fraudulent purpose, does not constitute "exceed[ing] authorized access." 18 U.S.C. § 1030(a)(4). In his opinion for the court in *United States v. Nosal*, Chief Judge Kozinski reasoned that interpreting "exceeds authorized access" as "limited to violations of restrictions on access to information, and not restrictions on its *use*" was consistent with the Act's text, served the Act's principal purpose of targeting hackers, and would avoid "allow[ing] private parties to manipulate their computer-use and personnel policies so as to turn [employment and customer] relationships into ones policed by the criminal law." Slip Op. at 3872, 3868. The majority noted that its decision conflicts with decisions from three other courts of appeals. The Government will have 90 days (with possible extensions allowing a further 60) to file a petition for certiorari if it wants to take the issue to the Supreme Court.

Background

As described in our earlier alert, according to the indictment, Nosal quit his job at a company, signed a non-compete agreement, and then enlisted several former colleagues who still worked at the company to download information from a confidential company database so he could use the information to start a competing company. The former colleagues were authorized to access the database, but the company's computer-use policy prohibited disclosing confidential information. The Government indicted Nosal for aiding and abetting his former colleagues' alleged crime of "exceed[ing] authorized access" for a fraudulent purpose under the CFAA, as well as for wire fraud, trade secret theft, and other violations. The district court threw out the CFAA counts, holding that use of information for a forbidden purpose was insufficient, by itself, to bring the challenged conduct within the scope of "exceed[ing] authorized access." A Ninth Circuit panel reversed.

The *En Banc* Court's Reasoning

Chief Judge Kozinski began with the CFAA's text. The Act 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). He found nothing in the provision's terms indicating it was intended to reach mere illicit use. In support of that view, he emphasized the CFAA's focus on punishing hackers. The Act's prohibition on unauthorized access, he explained, may be read as "apply[ing] to *outside* hackers (individuals who have no authorized access to the computer at all)," while its prohibition on "exceed[ing] authorized access" sensibly applies "to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." Slip Op. at 3863.

But perhaps most important to the court's decision was the majority's concern that 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." *Id.* at 3864. "This," the court asserted, "would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime." Turning from workplace computer-use policies to websites' terms of service, the majority noted that "[o]ur access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of," "virtually no one reads or understands," and are often subject to change without notice. *Id.* at 3868-70. Interpreting the CFAA as prohibiting improper use of a computer could, in the *en banc* majority's view, "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.* at 3867.

Implications

1. The *en banc* court's opinion limits the options of prosecutors, who have been making more aggressive use of the CFAA in recent years, and of companies, who increasingly have been using the CFAA as a basis for claims against employees and former employees. The court's opinion covers the entire Ninth Circuit, including California. The impact of the opinion could be even broader if other courts adopt the Ninth Circuit's reading of the CFAA.
2. The Obama Administration now faces a dilemma about how to proceed. On the one hand, it has urged a broad reading of the CFAA in order to expand the arsenal of prosecutors targeting the growing problem computer-based crime. On the other hand, the majority opinion's concerns about privacy and over-criminalization may have appeal both to some within the Administration and to groups generally supportive of the Administration, as well as to some business groups. Seeking a ruling from the Supreme Court may bring vindication for the Government's broad view, but it might well lead to a more complete rejection of the Government's broad reading of the CFAA.
3. The Republican cybersecurity bill in the Senate, S. 2151, contains a provision that would amend the CFAA essentially in line with the *en banc* Ninth Circuit's ruling. Whatever happens in the courts, Congress may establish this narrower version of the CFAA through legislation.
4. This dispute over the scope of the CFAA is only one example of the broader phenomenon of courts and agencies struggling to apply laws written in the pre-Internet era to the novel data security and privacy issues that arise in cyberspace. The CFAA was enacted in the mid-

1980s, as was the Electronic Communications Privacy Act and the Stored Communications Act, when personal computers were just becoming fixtures in the workplace and before the Internet had been born (at least as a commercial phenomenon). The need to bring laws up to date is one of the main forces driving legislative efforts both in Congress and in many State legislatures.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Patrick J. Carome

RETIRED PARTNER

+1 202 663 6000

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195