Digital Media & Data Privacy Law

Ninth Circuit Interprets "Without Authorization" under the Computer Fraud and Abuse Act

When we last left David Nosal, he had escaped liability under the Computer Fraud and Abuse Act after convincing some of his former colleagues at executive search firm Korn/Ferry to use their log-in credentials to download source lists, names and contact information from a confidential database and transfer that information to Nosal. The U.S. Court of Appeals for the Ninth Circuit held that violating Korn/Ferry's policy against disclosing confidential information did not amount to violations of the CFAA, and overturned his convictions under that law.

But the government wasn't finished with Mr. Nosal, and filed a second superseding indictment against him in February 2013. His ultimate conviction under the CFAA was upheld by the Ninth Circuit on July 5th.

Facts

All of these facts come from the court's slip opinion. Nosal was a high-level regional director at Korn/Ferry. He announced his intention to leave the firm in 2004, but agreed to stay on for an additional year as a contractor to finish a handful of open searches, subject to a blanket non-competition agreement. During this interim period, Nosal secretly launched his own search firm along with other Korn/Ferry employees, including Becky Christian, Mark Jacobson, and Nosal's former executive assistant, Jacqueline Froehlich-L'Heureaux. As of Dec. 8, 2004, Korn/Ferry revoked

One thing the new firm didn't have was Korn/Ferry's core asset: "Searcher," an internal database of contact and biographical information on over one million executives. Its name lacked inspiration, but Searcher was apparently quite comprehensive. Anyway, password sharing for all of Korn/Ferry's computer systems was prohibited by a confidentiality agreement that each new employee was required to sign.

After Nosal became a contractor and Christian and Jacobson left Korn/Ferry, the company revoked each of their credentials to access its computer system. On three occasions Christian and Jacobson borrowed access credentials from Froehlich-L'Heureaux, who stayed on at Nosal's request. In March 2005, Korn/Ferry received an email from an unidentified person advising that Nosal was conducting his own business in violation of his non-compete agreement. The company launched an investigation and, in July 2005, contacted government authorities. In April 2005, Nosal told Christian to obtain some source lists from Searcher to expedite their work for a new client. Instead of explaining the request to Froehlich-L'Heureaux, Christian asked to borrow her access credentials, which she then used to log into Searcher, sending the results to Nosal. In July 2005, Christian and Jacobson logged in as Froehlich-L'Heureaux to download information on over 2,400 executives.

Discussion

PUBLISHED

July 27, 2016

FILED UNDER

Digital Media & Data Privacy Law

TOPICS

Data Security

AUTHOR

David Smyth

ARTICLE URL

http://brookspierce.com/news-insights/ninth-circuit-interprets-"without-authorization"-under-computer-fraud-and-abuse-act

The CFAA was originally enacted in 1984 and amended in 1986 to "deter[] and punish[] certain 'high-tech' crimes," and "to penalize thefts of property via computer that occur as part of a scheme to defraud." Slip Op. at 13. The statutory subsection in this version of Nosal is 18 U.S.C. § 1030(a)(4), which provides: "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 . . . shall be punished . . . ." The statute doesn't explicitly define "without authorization," but the court found it to be an unambiguous term that should be given its ordinary meaning. Slip. Op. at 14.

In Nosal's first trip through the Ninth Circuit, authorization was not in doubt. What that first case did not address was whether Nosal's access to Korn/Ferry computers *after* both Nosal and his coconspirators had terminated their employment and Korn/Ferry revoked their permission to access the computers was "without authorization."

As *Nosal I* made clear, the CFAA was not intended to cover unauthorized use of information. Such use was not at issue in this case, *Nosal II*. Rather, under § 1030(a)(4), Nosal was charged with unauthorized access – getting into the computer after categorically being barred from entry.

After the login credentials of Nosal, Christian, and Jacobson were revoked on Dec. 8, 2004, they became "outsiders" and were no longer authorized to access Korn/Ferry computers, including Searcher. The court could find no authority to suggest that a former employee whose computer access had been revoked could access his former employer's computer system and be deemed to act with authorization.

Apart from the instruction, Nosal challenged the sufficiency of the evidence, claiming evidence of intent was insufficient because he didn't have advance knowledge that Christian and Jacobson would use Froehlich-L'Heureaux's password. The court held that that attack failed because, "after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." Slip Op. at 28 (citing *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)). The court said a juror also could have easily concluded that Nosal, having worked with Froehlich-L'Heureaux for years on a daily basis, would have known that she had herself never run custom reports, developed source lists or pulled old source lists. When Nosal specifically directed Christian to access Korn/Ferry's computer system to "[g]et what I need," Nosal knew that the only way Christian and Jacobson could access the source lists was "without authorization" because Korn-Ferry had revoked their access credentials.

What to Know

This decision gives companies a big stick to use against employees or former employees who might use another's log-in information to access and misappropriate corporate data. It also creates the very real possibility that one could become criminally liable for using somebody else's password to access a protected computer. Is that what the statute is meant to prohibit? Judge Reinhardt dissented to note "the majority's (somewhat circular) dictionary definition of 'authorization' – permission conferred by an authority." Under Judge Reinhardt's construction, "authorization" might have been effectively granted by Froehlich-L'Heureaux. We'll see if the full court reviews the panel's decision here.