haynesboone
Setting precedent.

Haynes and Boone's Newsroom

California Man Convicted of Hacking into Former Employer's Computer Network

04/25/2013

Ronald W. Breaux, Emily Westridge Black, Timothy Newman

A jury in the Northern District of California has convicted David Nosal of violating the Computer Fraud and Abuse Act ("CFAA") by accessing his former employer's computer network without authorization to obtain confidential information for use in a competing business. The business community has followed this case closely because it has far-reaching implications for the future application of the CFAA and, more importantly, for companies' ability to protect their sensitive proprietary data.

As described in our last alert on this case, available here, Nosal's prosecution followed a decision by the United States Court of Appeals for the Ninth Circuit regarding the meaning of the phrase "exceeds authorized access," a term defined in the CFAA 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." Rejecting the broad interpretation of the Fifth, Seventh, and Eleventh circuits, which criminalizes unauthorized use of information that an employee is authorized to access, the Ninth Circuit adopted a narrow view of the phrase, holding that the purpose of the CFAA is "to punish hacking - the circumvention of technological access barriers - not misappropriation of trade secrets - a subject Congress has dealt with elsewhere." Applying this analysis, the court dismissed some, but not all, of the government's CFAA claims against Nosal.

Nonetheless, a jury has convicted Nosal on the remaining CFAA charges and on "theft of trade secrets" charges. According to reports, the jury did not hear evidence that Nosal "hacked" into his former employer's network in the traditional sense of the word. Instead, the prosecution argued that Nosal convinced employees at his former employer to give him information they were permitted to access. Defense attorneys requested - and the court has scheduled - a hearing to determine whether the CFAA conviction can stand based on these facts, laying the groundwork for another Ninth Circuit opinion, and perhaps a decision by the United States Supreme Court, regarding the scope of the CFAA.

Haynes and Boone counsels clients on all aspects of data security and privacy, including how they can better protect against, identify, and remediate computer hacking activity. We also help clients that have been impacted by illegal hacking navigate the civil, criminal, and regulatory inquiries that arise. We welcome the opportunity to consult with and advise any companies that have concerns regarding any aspect of cybersecurity.

For more information regarding the firm's data security practice, contact one of the attorneys listed below.

Ronald W. Breaux	Bill Morrison	David Siegal
214.651.5688	214.651.5018	212.659.4995
ron.breaux@haynesboone.com	bill.morrison@haynesboone.com	david.siegal@haynesboone.com
Mark Erickson	Emily Westridge Black	Timothy Newman
949.202.3052	214.651.5221	214.651.5029
mark.erickson@haynesboone.com	emily.westridgeblack@haynesboone.com	timothy.newman@haynesboone.com