haynesboone
Setting precedent.

Haynes and Boone's Newsroom

California Computer Hacking Case Highlights Important Circuit Split on the Computer Fraud and Abuse Act

04/17/2013

Ronald W. Breaux, Emily Westridge Black, Timothy Newman

The computer hacking trial of David Nosal is under way in federal district court in California. The trial is being followed with interest in the business community because it is the latest development in a case that highlights an important split in the interpretation of the Computer Fraud and Abuse Act ("CFAA") that has far-reaching ramifications with respect to liability–and protection for companies' proprietary information. A 2008 indictment charged Nosal with violating the CFAA through his role in an alleged conspiracy to obtain proprietary and sensitive information from his former employer through unauthorized access to the employer's computer network. The trial follows a Ninth Circuit opinion dismissing some, but not all, of the government's CFAA claims based on that court's reading of the phrase "exceeds authorized access," which is much narrower than the interpretation adopted by several other circuits.

The phrase "exceeds authorized access" is 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." 18 U.S.C. § 1030(e)(6). As the Ninth Circuit Court of Appeals spelled out in *United States v. Nosal*, this definition may be interpreted in two ways: (1) "[I]t 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,'" or (2) "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."

Prior to the *Nosal* decision, the Fifth, Seventh, and Eleventh circuits had adopted the latter, much broader interpretation of "exceeds authorized access." In *United States v. John*, for example, the Fifth Circuit held that a bank employee exceeded her authorized access and violated the CFAA when she printed customer account information and provided it to her brother so that he could make fraudulent charges on customers' accounts. According to the court, "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."

In *Nosal*, on the other hand, the Ninth Circuit adopted the narrower interpretation of the term and held that it "is limited to violations of restrictions on *access* to information, and not restrictions on its *use*." The Ninth Circuit criticized the reasoning of the Fifth, Seventh, and Eleventh circuits, writing that the narrower interpretation is "a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking–the circumvention of technological access barriers–not misappropriation of trade secrets–a subject Congress has dealt with elsewhere." Last year, the Fourth Circuit Court of Appeals followed *Nosal* and adopted a similarly narrow interpretation of "exceeds authorized access."

This circuit split regarding the meaning of "exceeds authorized access" effectively creates vastly divergent liability schemes under the CFAA, depending on where the alleged offense was committed. The Supreme

Court may soon be called upon to resolve this critical split.

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
214.651.5688
ron.breaux@haynesboone.com

Bill Morrison
214.651.5018
bill.morrison@haynesboone.com

Emily Westridge Black
214.651.5221
emily.westridgeblack@haynesboone.com

Timothy Newman
214.651.5029
timothy.newman@haynesboone.com