Michael M. Ratoza
Portland, Shareholder

Direct Dial: 503.499.4695
Fax: 503.295.0915
Email Attorney

Ninth Circuit Expands Criminal Liability Under Computer Fraud and Abuse Act

By Michael M. Ratoza

The Ninth Circuit's recently expanded application of the Computer Fraud and Abuse Act provides enhanced criminal remedies for the unauthorized use of protected computer data.

The *Computer Fraud and Abuse Act* (CFAA)[1] creates civil and criminal liability in certain instances for conduct relating to the unauthorized access to a computer, or exceeding the authorized access to a computer. The CFAA restricts several forms of computer access and use, including the following conduct:

> 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, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period[.]

18 U.S.C. §1030(a)(4).

Previous cases have extended the civil reach of this statute beyond traditional hacking conduct to include civil claims against employees and third party competitors who obtain unauthorized access to proprietary computer data.

The Ninth Circuit has recently expanded the use of CFAA into the criminal arena to fight against the violation of restricted use of a business computer. Last week, the Ninth Circuit's opinion in *USA v. Nosal*[2] confirms the court's views on criminal application of the CFAA in a business context. The court made clear the following basic tenets under CFAA §1030(a)(4):

1. If the business owner of the computer does not restrict a user's access to and use of computer data, then a user's access to computer data and the use of the data for purposes contrary to the interest of the computer owner does not constitute a crime under CFAA. The lack of specifically defined access restrictions prevents the criminal expansion of the CFAA.
2. If the business owner of the computer restricts access to computer data to certain authorized users, and restricts the use of computer data, then there is criminal liability under CFAA §1030(a)(4) if:
    - The person who accesses the computer does so in violation of the computer owner's specific restrictions on computer access;
    - The person accesses the computer data with the intent to defraud the owner of the computer data; and
    - By accessing the computer data in violation of the restrictions, the person "furthers the intended fraud and obtains anything of value."
3. If a person without access to the computer induces another person who has access to obtain and pass along restricted data, then under criminal conspiracy theories both the person without access who receives the restricted data and the person with access who passes along the restricted data may be criminally liable.

The *Nosal* case deals with a former employee of a business who engaged with several existing employees of the business to obtain proprietary information from the business' computer system. The former employee intended to use this information to establish a competing business. The existing employees had access to the computer data, but their access and use were restricted by the employer's specific written business rules. Indeed, the employer's use restrictions were "clear and conspicuous." The employer required its employees to sign employment agreements that specifically prohibited "use and disclosure of all such information, except for legitimate * * * business * * *." Further, the employer's computer system displayed a cautionary message whenever a user logged on, stating:

> This computer system and information it stores and processes are the property of * * *. You need specific authority to access any * * * system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution * * *.

The criminal case was brought when the existing employees used their restricted access to obtain proprietary data and pass the data to the former employee for purposes of developing a competing business. This conduct occurred in direct violation of the employer's specifically defined use restrictions. While this type of conduct for some time has exposed an employee to civil liability for violating specific computer use restrictions, the *Nosal* case represents the first criminal use of the CFAA in this manner by the Ninth Circuit.

The Ninth Circuit's *Nosal* opinion goes to some length to explain that the foregoing criminalization of computer access is not designed to impose liability on an employee who uses an employer's computer system for unauthorized use that is merely personal and non-fraudulent. The court explains that the CFAA does not criminalize an employee's personal use of a work computer, "for example, to access their personal email accounts or to check the latest college basketball scores."

While the *Nosal* opinion involves the restricted use of a computer system by an ex-employee and current employees, the teaching of *Nosal* is not limited to the employment context. There are other examples in which a person can intentionally access and use computer data in violation of specific restrictions and for a fraudulent purpose. Examples of potential liability outside of the employment context include:

- accessing a computer database with a "borrowed" access code when the owner of the database specifically requires that each user obtain his or her own access code, or
- accessing and using a computer database to redistribute downloaded data in violation of a personal use agreement, or
- using a computer database for commercial purposes when the use agreement restricts usage to personal or household purposes.

As indicated, the CFAA is not limited to the traditional concept of hacking. But to assure that the criminal aspects of the CFAA apply, the owner of the computer must clearly and conspicuously establish access and use restrictions.

Michael M. Ratoza advises and assists clients in the use of the Internet and the protection of proprietary data. More information about this eAlert, or about IP in general, can be obtained from the author, michael.ratoza@bullivant.com, or from the IP Group of Bullivant Houser Bailey PC, www.bulllivant.com.

---

[1] 18 U.S.C. §1030.
[2] USA v. Nosal, ___ F.3d ____ (9th Cir. April 28, 2011), http://www.ca9.uscourts.gov/opinions/.