

## **Analysis: Critics assail 1980s-era hacking law as out of step**

Grant McCool, Reuters

(Reuters) - A 1984 U.S. anti-hacking law passed when computer crime was in its infancy is under fire for potentially going too far in criminalizing the actions of employees who violate workplace policies.

Judges across the country are divided on how the 28-year-old law, the U.S. Computer Fraud and Abuse Act, can be applied. At the same time, the Justice Department has signaled it wants to ramp up prosecutions under the law, even as it has lost some cases.

Civil liberties advocates and some lawyers and judges are questioning whether the CFAA, intended to punish hackers and other trespassers who damage computer systems or steal customer information, can be used to prosecute people inside a company who download sensitive data without their employers' approval.

The debate is centered around a key phrase in the law: that it is illegal to "intentionally access a computer without authorization or exceed authorized access." Critics argue this language is too broad and vague and could turn ordinary people into criminals for things many do routinely, such as dabble in online shopping or scan an online matchmaking site at work.

"This statute has the potential to affect millions of Americans in the workplace who work at or use a computer to do their job," said Brent Cossrow, a partner at law firm Fisher & Phillips in Radnor, Pennsylvania, which specializes in computer breach cases. "Hopefully, it gets cleared up soon."

### **BOUND FOR SUPREME COURT?**

A split decision in April by the 9th U.S. Circuit Court of Appeals in San Francisco could be the case that forces the U.S. Supreme Court to examine the law's reach.

In a 9-2 ruling, the appeals court threw out criminal charges brought under the law against David Nosal, a former managing director at executive search firm Korn/Ferry International. Nosal was indicted in 2008 for allegedly persuading colleagues to download confidential source lists and contact information from the firm to use at his new business.

Three co-defendants pleaded guilty to CFAA violations. But Nosal fought the charges, arguing that he and his colleagues had been authorized to access the company's database. The appeals court supported Nosal's argument, and threw out the CFAA charges against him, though he still faces separate charges of trade secrets theft in U.S. District Court in San Francisco.

The 9th Circuit ruling was suspended to give the Justice Department time to consider petitioning the Supreme Court to review the case. If the Supreme Court were to hear the matter, it could potentially be on the docket for the upcoming term.

The Justice Department, which declined to comment on the case, has until August 8 to decide whether to seek Supreme Court review.

Nosal's lawyer, Steven Gruel, said his client wants to exonerate himself. "He's always said he did nothing wrong."

### NEW SCENARIOS

If the high court does not take the Nosal case, legal experts say, little is likely to get settled in the near future over how and when the law can be applied.

The CFAA was crafted before the Internet was omnipresent in the workplace. Employees today have vastly more sensitive company information accessible on their computers, leading to scenarios that the writers of the law may never have envisioned.

Some companies, such as Oracle Corp, which filed a brief supporting the Justice Department against Nosal, say such criminal prosecutions are justified.

Oracle said Congress rooted the statute in common-law trespass doctrines.

"Among them is the concept of restricted authorization: a person commits trespass not only when he or she enters property or a portion of it when told not to; a person commits trespass also when he or she has authorization to enter for some purposes but enters for different ones," the brief said.

Critics say the statute, which carries civil and criminal penalties, could be abused by employers.

The precedent that develops largely in the context of a private, workplace dispute "becomes something that people can go to jail for, and that's really dangerous," said Marcia Hoffman, senior staff attorney with the Electronic Frontier Foundation, a non-profit civil liberties organization.

Potential criminal penalties under the law range from one year to 10 years in prison, if the offense involves information relating to U.S. national security.

Prosecutors have brought about 550 federal criminal cases under the CFAA and related computer fraud laws in the past 5-1/2 years, according to court filings reviewed in Westlaw, a legal data division of Thomson Reuters. Over the same period, nearly 500 civil lawsuits were brought in private disputes citing the CFAA and related laws, the filings show.

## **Analysis: Critics assail 1980s-era hacking law as out of step**

Published on Electronic Component News (<http://www.ecnmag.com>)

---

The Justice Department wants to expand the penalties and prosecutions under the act, an Obama administration official told a hearing on Capitol Hill in November. Richard Downing, deputy section chief for computer crime and intellectual property, said it was important to retain the provisions of the law that apply to employee-use agreements.

Removing that section of the law "could make it difficult or impossible to deter and punish serious threats from malicious insiders," he told the Crime, Terrorism and Homeland Security Subcommittee of the House Judiciary Committee.

If the Justice Department were to go to the Supreme Court and lose over the CFAA, it would remove an arrow in its quiver for prosecuting those "insider" computer abuse cases.

Congress has partially addressed the issue while crafting new cyber security legislation. One possible amendment to a bill pending in the U.S. Senate would narrow criminal cases to exclude relatively innocuous violations of agreements governing the use of private computers, such as a social-network user signing up under a pseudonym.

### **MIXED RULINGS**

In February, the U.S. government lost another case involving an employee who had accessed company data, a case that also raised questions about use of the hacking statute.

That case involved a former Goldman Sachs Group Inc programmer, Sergey Aleynikov, who was accused of stealing code used in the bank's high-frequency trading system before leaving for a new company in Chicago.

Before Aleynikov went on trial, U.S. District Judge Denise Cote dismissed the charges brought under the CFAA, saying the government's interpretation "could convert an ordinary violation of the duty of loyalty or of a confidential agreement into a federal offense." But she let trade-secrets charges against him stand, and in December 2010 Aleynikov was found guilty.

That conviction was thrown out earlier this year by the 2nd U.S. Circuit Court of Appeals, and Aleynikov was freed after serving one year of an eight-year prison term.

The Nosal and Aleynikov cases conflict with an earlier appeals court ruling. That case was a civil dispute between a real estate developer, Jacob Citrin, and his former employer, International Airport Centers LLC. The 7th U.S. Circuit Court of Appeals in Chicago ruled in 2006 that Citrin violated the CFAA by installing a program that deleted files on a company laptop as he was departing for another job.

Citrin was not criminally charged and his case was settled on undisclosed terms, but a Justice Department guide for prosecutors on the CFAA points to the 7th Circuit

## **Analysis: Critics assail 1980s-era hacking law as out of step**

Published on Electronic Component News (<http://www.ecnmag.com>)

---

ruling as "the leading authority" for the position that when an employee is doing something disloyal to an employer, authorized access to the computer ends under the law.

Citrin's lawyers, Ronald Marmer and John Koch, of Jenner & Block in Chicago, had no comment. Citrin is now CEO of Cargo Ventures in Doral, Florida, according to his company's web site.

Unless the Supreme Court ultimately weighs in, the inconsistent decisions will continue, said lawyer John Dozier, of Dozier Internet Law, a Glen Allen, Virginia law firm.

Without clarity, he said, "what is going to be illegal in one part of the country is not illegal in the other."

The cases are USA v David Nosal in the 9th U.S. Circuit Court of Appeals 10-10038 and International Airport Centers LLC v Jacob Citrin in the 7th U.S. Circuit Court of Appeals No. 05-1522 and USA v Aleynikov, U.S. District Court for the Southern District of New York 10-00096.

(Editing by Martha Graybow, Edward Tobin and Leslie Gevirtz)

**Source URL (retrieved on 08/23/2014 - 4:42am):**

<http://www.ecnmag.com/news/2012/07/analysis-critics-assail-1980s-era-hacking-law-out-step>