CFAA Does Not Apply to Employee Data Theft According to 9th Circuit

Insights
4.11.12

Dispute Seems Destined for United States Supreme Court

"Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes we use them for play at work. Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website? This depends on how broadly we read the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030."

And so begins the reasoning of the United States Court of Appeals for the 9th Circuit on way to its conclusion that the CFAA does not apply to data theft by an employee who steals information he was permitted to access in the first place.

The CFAA makes it unlawful to access a computer without authorization, or to exceed the scope of one's authorization, for the purpose of obtaining or altering information in the computer that one is not entitled to obtain or alter.

In US v. Nosal, the U.S. Court of Appeals for the 9th Circuit acknowledged that the CFAA can be read either of two ways: First, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files. This is colloquially known as 'hacking.'

The Court offers an example. "[A]ssume an employee is permitted to access only product information on the company's computer but accesses customer data: He would 'exceed authorized access' if he looks at the customer lists."

But the Court noted that the statute also could be interpreted differently. Namely, the language might refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. "For example, an employee may be authorized to access customer lists in order to do his job but not to send them to a competitor."

And so goes the dispute. According to the government, employees violate the CFAA when they access information on their employer's computer for an improper purpose.

A majority of the 9th Circuit rejected the government's view of the CFAA with a litany of colorful language and hypotheticals:

"The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes....For example, it's not widely known that, up until very recently, Google forbade minors from using its services. Adopting the government's interpretation would turn vast numbers of teens and pre-teens into juvenile delinquents and their parents and teachers into delinquency contributors."

From the 9th Circuit's perspective, the danger is palpable. "Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes."

"Under the government's proposed interpretation of the CFAA, posting for sale an item prohibited by Craigslist's policy, or describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit."

In reaching its conclusion, the 9th Circuit acknowledged that its decision was at odds with numerous "decisions of our sister circuits" reaching different conclusions; e.g., the 5th, 7th and 11th Circuits. But it simply asked that its "sister circuits" reconsider based on the content of the 9th Circuit opinion.

But the split of opinion in federal court is not simply a split among the circuits. Notably, there was a dissenting opinion filed concurrently with the 9th Circuit's decision in Nosal.

The Dissent

The dissent blasted the theoretical illustrations contained in the majority opinion. "This case has nothing to do with playing sudoku, checking email, fibbing on dating sites, or any of the other activities that the majority rightly values. It has everything to do with stealing an employer's valuable information to set up a competing business with the purloined data, siphoned away from the victim, knowing such access and use were prohibited in the defendants' employment contracts."

The dissent continued: "In ridiculing scenarios not remotely presented by this case, the majority does a good job of knocking down straw men, and far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy."

Offering its own analogy, the dissent observed that a bank teller is entitled to access a bank's money for legitimate banking purposes, but he may not take the money for himself.

In short, the dissent concluded that "it does not advance the ball to consider, as the majority does, the parade of horribles that might occur under different subsections of the CFAA." That is why courts have the authority to consider constitutional challenges to the manner in which statues are applied.

"The role of the courts is neither to issue advisory opinions nor to declare rights in hypothetical cases, but to adjudicate live cases or controversies....We need to wait for an actual case or controversy to frame these issues, rather than posit a laundry list of wacky hypotheticals."

And so goes the internally conflicted thinking of the United States Court of Appeals for the 9th Circuit. One has to wonder, if the justices of the 9th Circuit cannot agree among themselves whether to agree or disagree with other federal circuits, how long will it be before the U.S. Supreme Court has to weigh in on the matter?

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either follow Michael R. Greco on Twitter or on LinkedIn or subscribe to this blog's RSS feed.

US_v_Nosal.pdf (103.39 kb)

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email