

The Patchwork Application Of The CFAA

August 17, 2012 | [Social Media And Technology](#), [Labor And Employment](#)



**Jeanine M.
Gozdecki**
Partner

Go ahead, all you employees on the west coast and the mid-southeast. Please. Use your employer's computers to download confidential documents, surreptitiously transfer the company's contacts, and "borrow" all the forms you need to start your own competing company. As it turns out, the federal law known as the Computer Fraud and Abuse Act (CFAA) doesn't apply to you. (*Side note* We aren't suggesting that you actually do this.)

But, beware if you live in other parts of the country—for example, in Chicago, Dallas or Atlanta. Employees based in those cities, in other parts of the South and Midwest, and who commit the same offense will likely face criminal and civil penalties under the CFAA.

Have I overstated the contrast? Glossed over the nuances? Perhaps. Those downloading confidential documents in the Ninth Circuit still face liability, but not under the federal CFAA. The trouble is that some courts think the CFAA applies to disloyal employees; other courts don't. Worse, the U.S. Department of Justice (DOJ) has decided to allow the rift to remain.

As a quick review, the CFAA prohibits individuals from "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access and . . . obtain[ing] anything of value." 18 U.S.C. §1030(a)(4). Employers have successfully used the CFAA to augment claims against former employees who have stolen company secrets and information from the company's computer system. The government has pursued criminal claims under the CFAA against those employees as well.

But, in April of this year, the Ninth Circuit limited the scope of the CFAA in the appeal of a trade secrets/mail fraud case against a former Korn/Ferry employee when he left and started a competing company. The Ninth Circuit narrowly interpreted the CFAA, essentially finding that it was a law designed to punish "hackers," not misappropriation of trade secrets. The Ninth Circuit's decision was joined by the **Fourth Circuit** (VA, WV, NC, SC)), but contradicts decisions issued by the **Seventh Circuit** (IN, IL, WI), the **Fifth Circuit** (TX, LA, MS), and the **Eleventh Circuit** (FL, GA, AL).

Regardless of your own opinion on how far the law should extend, the DOJ missed an opportunity to bring clarity to businesses (and assistant U.S. attorneys) on this issue. The CFAA divide is ripe for resolution by the Supreme Court, but for some reason, the DOJ declined. (The subject, perhaps, of another blog post?) In the meantime, the recent Ninth Circuit decision reminds companies to evaluate their internal confidentiality and computer use policies, to confirm they have appropriately protected confidential and other valuable information. If they haven't, then let's take

RELATED PRACTICE AREAS

Internet and Technology
Labor and Employment
Workplace Culture 2.0

RELATED TOPICS

Computer Fraud and Abuse Act

steps to bolster those security measures. As lawyers, we are compelled to pay attention to the shifting winds, and where our employees—whether in L.A. or Chicago—happen to be standing at the time.