

Computer Fraud & Abuse Act: Eleventh Circuit Finds Employer's Policy Defines Limits of Employee's Authorized Access

January 9, 2011

by Michael R. Greco

Time and time again, this blog has outlined the ongoing debate in the courts over whether the federal Computer Fraud & Abuse Act ("CFAA") applies in the context of departing employees. Namely, federal courts differ over whether the CFAA applies when an employee is accused of misappropriating his or her employer's confidential information or trade secrets by means of the employer's computer, to which the employee had authorized access as a result of his or her employment. A recent opinion by the United States Court of Appeals for the Eleventh Circuit may be seen by some as adding to debate.

In United States v. Roberto Rodriguez, the 11th Circuit took on the question of whether an employee "exceeds authorized access" under the CFAA by accessing information on a computer in a manner contrary to an employer's policies. Rodriguez is a former employee of the Social Security Administration ("SSA"). The SSA established a policy that prohibits employees from obtaining information from its databases without a business reason. The SSA notified employees of this policy through training sessions, notices published in the office, and banners that appear on computer screens daily. Employees were also required to sign forms annually acknowledging the policy.

In apparent disregard of this policy, Rodriguez was accused of repeatedly using SSA databases to obtain personal information concerning people he knew, including women in whom he had romantic interests. On one occasion, Rodriguez sent flowers on Valentine's Day to a woman he had met that had not given him her address. He later arrived at her doorstep uninvited. Some time later, he called to wish her a happy "half-birthday" even though she had not shared her birthday with him. He also accessed SSA databases to obtain information concerning several other women he met and to obtain information concerning their family members.

Rodriguez was charged and later convicted of criminally violating the CFAA by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] ... information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). Although this case involves a criminal indictment and prosecution, it is instructive in civil cases because the 11th Circuit's decision revolves around an element

commonly at issue in civil claims; namely, what it means to access a computer in excess of one's authority.

Rodriguez argued that he did not violate the CFAA because he accessed only databases that he was authorized to access as an employee of the SSA. The 11th Circuit found "his argument ignores both the law and the record." The Court explained:

"The Act defines the phrase 'exceeds authorized access' 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 to obtain or alter.' The policy of the [Social Security] Administration is that use of databases to obtain personal information is authorized only when done for business reasons. Rodriguez conceded at trial that his access of the victims' personal information was not in furtherance of his duties as a TeleServices representative and that 'he did access things that were unauthorized.' In light of this record, the plain language of the Act forecloses any argument that Rodriguez did not exceed his authorized access."

In its decision, the 11th Circuit stated that its opinion was not at odds with the Ninth Circuit's decision in LVRC Holdings v. Brekka because Brekka could be distinguished: "Brekka is distinguishable because the Administration told Rodriguez that he was not authorized to obtain personal information for nonbusiness reasons." Although this is an accurate observation, a California court recently cited Brekka in support of its decision rejecting an employer's CFAA claim even though the employer argued that the employee accessed information in a manner contrary to company policy. [See prior post Computer Fraud & Abuse Act: Court Rejects Argument That Employer's Corporate Policies Can Make Employee Access "Unauthorized" Under the CFAA.](#)

After the 11th Circuit's opinion in Rodriguez, one thing remains clear: employers and employees will continue to interpret and apply the CFAA differently. A copy of the 11th Circuit's decision in U.S. v. Rodriguez is available in pdf format below.

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

[US v. Rodriguez.pdf \(88.81 kb\)](#)