PATTON BOGGS LLP

March 22, 2012

THE COMPUTER FRAUD AND ABUSE ACT SUBJECT TO DIFFERENT INTERPRETATIONS

Intellectual Property Client Alert

This Alert provides only general information and should not be relied upon as legal advice. This Alert may be considered attorney advertising under court and bar rules in certain jurisdictions.

For more information, contact your Patton Boggs LLP attorney or the authors listed below.

Richard Oparil
roparil@pattonboggs.com

Kevin Bell
kbell@pattonboggs.com

WWW.PATTONBOGGS.COM

Among its various provisions, the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, subjects a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer" to criminal penalties (§ 1030(a)(2)(C), (c)). Section 1030(a)(4) also prohibits "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…." A "protected computer" is one used in or affecting interstate commerce (§ 1030(e)(2)(B)). The phrase "without authorization" is not defined in the statute, but "exceeds authorized access" is defined to mean "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 so to obtain or alter" (§ 1030(e)(6)). While a criminal statute, civil suits may be brought under the CFAA in certain circumstances.

One open question is whether the CFAA imposes liability on employees who have permission to access computerized information but use the permitted access for an improper purpose? The federal courts are currently split on the issue.

The Ninth Circuit has held that employees who properly access information but use the information contrary to the employer's policies or against the employer's interests "exceeds authorized access." *United States v. Nosal*, 642 F.3d 781 (9th Cir.) ("We hold that an employee "exceeds authorized access" under § 1030 when he or she violates the employer's computer access restrictions—including use restrictions."), reh'g en banc granted, 661 F.3d 1180 (9th Cir. 2011). In another case, *Guest-Tek Interactive Entertainment Inc. v. Pullen*, 665 F. Supp. 2d 42 (D. Mass. 2009), the employer provided its employee, a sales vice president, with access to proprietary and trade secret information on its computer system. The employee copied thousands of computer files to a flash drive and launched a company that competes with the employer. The employer sued its former employee and his company for violation of the CFAA. The employee argued that the CFAA should be given a narrow reading and that the "without authorization" language means that the CFAA only reaches conduct by third-parties who do not have any authorization to access computer files. In considering the defendants' motion to dismiss the CFAA claim, the District Court noted that some "courts have opted for a more expansive view, finding that an employee accesses a computer 'without authorization' whenever the employee, with the employer's knowledge, acquires an interest that is adverse to that of his employer or is guilty of a serious breach of loyalty." The Court applied the expanded view of the CFAA and thus denied the defendants' motion to dismiss. See also *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577 (1st Cir. 2001) (former employee of a travel agent, in violation of his confidentiality agreement, used confidential information to create a program that enabled his new travel company to obtain information from his former employer's website and thus violated CFAA).

Other courts take a more narrow view of the CFAA and only find a violation when the employee exceeds the scope of her access to a protected computer. For example, in *Walter Bishop Assocs., Inc. v. O'Brien*, 2012 U.S. Dist. LEXIS 25219 (D. Minn. Feb. 28, 2012), three employees of an architectural firm had access to the "highest levels" of the firm's proprietary computerized information. They accessed and copied confidential information, including customer lists and drawings, and used the data to form their own company and compete with their employer, who then sued them for violating the CFAA. The District Court dismissed the case. The Court held that § 1030(a)(2) of the CFAA applies to access not use. The employer's computer-use policy limited employees' use of information, not the scope of access. The employer gave the defendant employees wide access to its computer system. Thus, because the employees could properly access the information, they did not violate the CFAA even though they used the information obtained for an improper purpose. See also *Xcedex, Inc. v. VMware, Inc*., 2011 U.S. Dist. LEXIS 70302 (D. Minn. June 8, 2011), adopted by 2011 U.S. Dist. LEXIS 70451 (D. Minn. June 30, 2011).

Companies should adopt policies which define employees' access to computerized information and limit its use to proper corporate purposes. For the moment, only in some jurisdictions can an employer invoke the CFAA against employees who accessed and then improperly used proprietary information stored on the company's computer. Ultimately, the proper interpretation of the scope of the CFAA may have to be decided by the U.S. Supreme Court.