4th Circuit Issues Employee Friendly CFAA Opinion

Insights
8.02.12

As readers of this blog know, we have been following the diverse and seemingly irreconciliable decisions from federal courts regarding the scope of the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Last week, in WEC Carolina Energy Solutions LLC ("WEC") v. Miller, the U.S. Court of Appeals for the 4th Circuit weighed in on what continues to be one of the hottest debates within the federal judiciary in recent memory: whether the CFAA applies to disloyal employees who access their employer's workplace computers to misappropriate, copy or otherwise transfer corporate data.

The facts in WEC v. Miller were similar to those in other recent CFAA cases. According to the 4th Circuit's opinion, a copy of which is available below, WEC provided specialized welding and related services to the power generation sector. As the 4th Circuit explained, Arc Energy Services, Inc. ("Arc") was one of WEC's competitors in South Carolina. WEC provided "Miller with a laptop computer and cell phone, and authorized his access to the company's intranet and computer servers." According to WEC's complaint, "Miller had access to numerous confidential and trade secret documents stored on ... computer servers, including pricing terms, pending projects[,] and the technical capabilities of WEC." WEC implemented employment policies that prohibited the use of such information without authorization or downloading it to a personal computer. But as the appellate court noted, "[t]hese policies did not restrict Miller's authorization to access the information."

In its Complaint, WEC alleged that before Miller resigned, he and his assistant at WEC downloaded and emailed WEC's confidential information to personal email accounts and a personal computer. WEC claimed that this information was used by Miller in a successful pitch to Arc after Miller's resignation. Miller moved to dismiss WEC's CFAA claims, and in opposition WEC argued that Miller violated the CFAA and WEC's employment policies by downloading WEC's confidential information to a personal computer. WEC also argued that Miller breached his fiduciary duty to WEC when he downloaded this information to his personal computer, thereby losing the authority to access it. WEC Carolina Energy Solutions, LLC v. Miller, No. 0:10-cv-2775-CMC, 2011 WL 379458, at *5 (D.S.C., Feb. 3, 2011). These arguments were rejected by the district court, which held that "WEC's company policies regulated use of information not access to that information. Thus, even if Miller and Kelley's purpose in accessing the information was contrary to company policies regulating use, it would not establish a violation of company policies relevant to access and, consequently, would not support liability under the CFAA."

This decision was affirmed by the appellate court. Diving headfirst into the debate regarding the scope of the CFAA, the 4th Circuit observed that in interpreting the CFAA, "two schools of thought exist." The first comes out of Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006), in which the court held that "when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it." The second school of thought, "articulated by the 9th Circuit and followed by the district court here, interprets 'without authorization' and 'exceeds authorized access' literally and narrowly, limiting the terms' application to situations where an individual accesses a computer or information on a computer without permission."

The appellate court rejected WEC's arguments in favor of following the Citrin line of cases, and adopted what is perceived as the employee-centric view articulated in Brekka and Nosal. As the appellate court held, "we adopt a narrow reading of the terms 'without authorization' and 'exceeds authorized access' and hold that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access." In a nod to the potential impact of its opinion, the appellate court noted its "conclusion here likely will disappoint employers hoping for a means to rein in rogue employees." "But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy."

Brent Cossrow is a partner in Fisher Phillips' Employee Defection & Trade Secrets Practice Group. Mr. Cossrow's practice focuses on e-discovery and other electronically stored information issues. As always, please feel free to share your thoughts and questions in the comment space below.

WEC v Miller.pdf (65.78 kb)

Related People

Brent A. Cossrow
Regional Managing Partner
610.230.2135
Email