The big chill: the Computer Fraud and Abuse act and whistleblower disclosures

David J. Marshall and Andrew Schroeder

The National Law Journal

November 1, 2011

In a case argued recently before the U.S. Court of Appeals for the 9th Circuit, the appellee made an unusual argument: It asked the court to review another case en banc. The argued case was *En Pointe Technologies Inc. v. Sarcom Inc.*, No. 10-55452 (9th Cir. filed March 26, 2010), a civil action under the Computer Fraud and Abuse Act, 18 U.S.C. 1030, whose outcome may turn on the 9th Circuit's controversial interpretation of the *CFAA in U.S. v. Nosal*, No. 10-10038 (9th Cir. April 28, 2011). On Oct. 27, the 9th Circuit voted to rehear Nosal en banc and ordered that the three-judge panel's decision from April not be cited as precedent by or to any court in the circuit. For millions of employees who work in the states that make up the very large 9th Circuit, and especially for those who might be thinking of blowing the whistle on employer wrongdoing, the court's decision to take another look at the Nosal case is a very welcome development.

The Nosal case centers on an executive at Korn/Ferry International, an executive-search firm, who left the company to start a competing business. He then recruited three Korn/Ferry employees to join him in the venture, and conspired to have them access and remove proprietary information using their access to Korn/Ferry's extensive database of executive candidates. Korn/Ferry had taken "considerable measures" to maintain the confidentiality of the information and, in agreements with employees, had explicitly restricted the use of the information to Korn/Ferry's business purposes.

To the employment lawyer, this sounds like a fairly common scenario leading to civil claims, either threatened or filed, for theft of trade secrets, breach of contract and breach of fiduciary duty. In this case, however, the U.S. government indicted David Nosal and one of the current employees under Section (a)(4) of the CFAA, which imposes criminal penalties on anyone who, "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." Since the employees were authorized users of the confidential database (for limited purposes), the key issue in the case was whether the employees "exceed[ed]" their "authorized access" for purposes of the statute by using their computers in a way that violated their employer's use policies. Put more broadly, the question is whether an employer's computer-use restrictions can serve to demarcate innocent versus criminal

behavior under the CFAA. The answer from a three-judge panel of the 9th Circuit was simple: Yes, they can.

There are obvious reasons to question why the CFAA, a statute designed to criminalize "hacking," should apply to the situation in Nosal, and to be concerned that the slippery slope attending this holding can easily extend to such common workplace transgressions as an employee's personal use of the Internet when a policy forbids it. (Although there is an "intent to defraud" limitation in one section of the CFAA, a parallel provision has no such limitation.) But the three-judge panel's holding in Nosal also created an ominous situation for a particular segment of employees in the 9th Circuit--those who may be considering reporting their employer's financial, securities, environmental, nuclear, aviation or other violations of law to government regulators.

Anyone involved in government regulation knows the value of a whistleblower — someone on the inside of a company who has closely observed wrongdoing — to successful enforcement actions under federal laws, and anyone who represents whistleblowers knows the value of documents in bringing their allegations to light. Documents often provide key evidence of wrongdoing and make it more likely that resource-starved regulators will take an interest in the whistleblower's allegations in the first place. Documents reduce the investigative burden on enforcement actions that do go forward. Documents shed light on the nature of the wrongdoing and the identities of the wrongdoers, thus focusing investigations earlier and reducing the need for government "fishing expeditions." Documents can also be critical in demonstrating the credibility of the whistleblower, an individual who will be under a tremendous amount of stress and whose allegations may be discounted because of it.

The current state of the law on whether employees may disclosure confidential company information to the government as part of their whistleblowing is a fact-specific legal minefield, but it is probably accurate to say that an employee who is not an attorney, and who comes across incriminating documents during the course of his employment, may disclose those documents to the government without facing criminal prosecution (or, if the employee signed a confidentiality agreement, a successful lawsuit for breach of contract). In fact, the U.S. Department of Labor's Administrative Review Board just last month observed that an employee's taking of confidential employer information and providing it to the Internal Revenue Service or U.S. Securities and Exchange Commission through those agencies' whistleblower-reward programs, if done "lawfully," might constitute protected activity under the anti-retaliation provisions of the Sarbanes-Oxley Act. See *Vannoy v. Celanese Corp.*, 2008-SOX-064 (ARB Sept. 28, 2011), slip. op. at 15-17. The Administrative Review Board noted that Congress had designed these whistleblower-reward programs specifically to "encourage whistleblowers to disclose confidential company information in furtherance of enforcement of tax and securities laws." Id. at 16.

The view of the three-judge panel that decided Nosal in April threatens to undermine the effect of these and other whistleblower laws. In the panel's view, an employer's computer-use restrictions define when an employee "exceeds" his or her authorization under the CFAA. It is difficult to believe there is a computer-use policy in existence that authorizes an employee to disclose evidence of the company's wrongdoing to third parties, nor could such an exception necessarily be inferred from language

restricting use of company computers to "legitimate business purposes." Although courts can refuse to enforce a confidentiality contract made by private parties in the name of "public policy," it is difficult to see how they could do so in a federal criminal statute that does not otherwise carve out such conduct.

In sum, the Nosal decision that the 9th Circuit will now reconsider suggests that an employee who discloses information obtained from his computer to the government would violate the CFAA and commit a federal crime. Keep in mind that this could apply not just to an employee who sought out incriminating information using surreptitious methods, but also to one who came across the documents while doing his own job. While one might hope that federal prosecutors would exercise discretion not to bring cases involving such disclosures, a low likelihood of eventual prosecution will not lessen the "chilling effect" of an en banc ruling that adopts the reasoning of the panel decision in Nosal.

If the full court agrees with the panel, this case might ensure that whistleblowers — or at least those without a duty to report — will rarely disclose information to regulators or will do so without documentary support, reducing the chances that their allegations will lead to enforcement actions. And even if these concerns could be put aside, the whistleblower will face yet another problem: A whistleblower who provides documents to a regulator could be sued by his or her employer for civil damages under the CFAA. Whether or not an employer could come up with a viable theory of compensable damages, there are few individuals who can pay the costs of defense while the employer tries to substantiate one. Again, a whistleblower is unlikely to run that gauntlet in the first place.

The 9th Circuit's en banc decision in *Nosal* is almost certain to have sweeping implications for whistleblowers and other employees. Anyone who favors enforcement of regulatory laws, as well as the protections that those laws afford whistleblowers, should hope that the 9th Circuit uses this opportunity to correct a decision that could deter would-be whistleblowers from coming forward with evidence of corporate wrongdoing.

David J. Marshall is a partner at Katz, Marshall & Banks, a whistleblower and employment-law firm based in Washington. He specializes in the representation of whistleblowers in retaliation cases and qui tam lawsuits, and in the Securities and Exchange Commission and Internal Revenue Service whistleblower-reward programs. He also serves on the advisory board of the Government Accountability Project and the board of directors of the Public Justice Foundation. Andrew Schroeder is a law clerk at the firm and a writer.