LOS ANGELES
Daily Journal
www.dailyjournal.com
FRIDAY, MAY 25, 2012

Access versus use: Nosal decision creates circuit split

By Thomas P. O'Brien, Daniel Prince and Katy Wanner

The U.S. Supreme Court soon may be asked to resolve an apparent circuit split concerning the breadth and scope of the Computer Fraud and Abuse Act (CFAA),, 18 U.S.C. Section 1030, specifically the provision criminalizing "exceeding authorized access." In April, an e*n banc* panel of the 9th U.S. Circuit Court of Appeals, in *United States v. Nosal*, explicitly rejected the 5th, 7th and 11th Circuits' reasoning regarding this statutory language. Indeed, Chief Judge Alex Kozinski, writing for the panel, urged that the CFAA should be construed narrowly — to prohibit hacking or the unauthorized access to data or files — so as to avoid turning harmless computer uses such as "g-chatting with friends, playing games, shopping or watching sports highlights" into federal crimes. Specifically, the 9th Circuit found that so long as an employee is authorized to access the information he or she obtains, such access is not prohibited by the CFAA, even if the employee stole the data or transferred it to a third party (although, as Chief Judge Kozinski recognized, the unauthorized use or misappropriation of such data may constitute a violation of 18 U.S.C. Section 1832, the federal trade secrets statute, or other laws). Ultimately, the *Nosal* decision may reduce employers' protection of their proprietary information, in that it removes a possible claim against the misuse of their proprietary information.

On the other hand, the 5th, 7th and 11th Circuits all have held that the CFAA broadly covers violations of corporate computer use restrictions or violations of duties of loyalty. See *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); and *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Indeed, the issue of data protection addressed in these opinions may impact the majority of businesses, as a recent survey has found that a whopping 59 percent of employees who leave their jobs take company data with them. See "Data Loss Risks During Downsizing," Ponemon Institute, Feb. 23, 2009. As evidenced, this is a significant issue for employers and employees alike.

The CFAA was enacted in 1986, as an amendment to the Counterfeit Access Device and Abuse Act. While both home and office computers were on the market at the time, neither businesses nor end-users had such a strong reliance on computer and Internet use thereby necessitating a legal regime to protect data from hackers or other potential wrongdoers. In that environment, Congress introduced H.R. 4718 (which later became the CFAA) to provide both civil and criminal penalties for fraud and related activities in connection with "access devices" and computers.

Nosal decision may reduce employers' protection of their proprietary information, in that it removes a possible claim against the misuse of their proprietary information.

The CFAA's sponsor, Rep. William J. Hughes, of New Jersey, acknowledged that he intended the CFAA to target computer "hackers." Indeed, Representative Hughes feared that, "computer technology — with all its gains — has left us with a new breed of criminal: [t]he technologically sophisticated criminal who breaks into computerized data files ... [t]he hacker of today can become the white-collar crime superstar of tomorrow."

Despite the CFAA's initially limited purpose, prosecutors and courts have routinely sought to expand it into many contexts beyond Hughes' supposed white-collar hacker. As recently as February of 2010, the 5th Circuit, in *United States v. John*, 597 F.3d 263 (5th Cir. 2010), found that the CFAA extends to the unauthorized "use" of information rather than mere unauthorized "access." In *John*, the defendant was an employee, not a hacker, authorized to view and print all of the sensitive financial information that she obtained from Citigroup. Holding that the defendant's employment agreement prohibited her "use" of the computer system to perpetrate fraud, the 5th Circuit ruled that the defendant's use of the data in a "criminally fraudulent scheme" exceeds "authorized access" within the meaning of the CFAA.

Nosal's procedural soap opera has been unfolding for years. After leaving his former employer, Korn/Ferry, defendant David Nosal convinced some of his former colleagues to use their log-in credentials to download and provide to him source lists and names and contact information from a confidential database on the Korn/Ferry computer system. While these employees were authorized to access this information, Korn/Ferry had a data policy forbidding disclosure of confidential information. Like many other companies, whenever Korn/Ferry employees accessed the database, the opening screen reminded them that the product was intended to be used only by Korn/Ferry employees for Korn/Ferry matters. Despite these well-known restrictions, Nosal intended to use this sensitive information to start a competing business.

Upon discovering Nosal's scheme, the government indicted him on 20 counts, including charges of trade secret theft, mail fraud, conspiracy and CFAA violations alleging aiding and abetting of unauthorized "use" of the data. Subsequently, Nosal filed a motion to dismiss the CFAA counts, which the district court initially rejected. Shortly afterwards, the 9th Circuit decided *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), finding that the CFAA narrowly applied to computer "access" but not "use" of computerized data. In light of *Brekka*'s narrow holding, the *Nosal* district court reversed itself and dismissed the CFAA counts.

Upon appellate review, a 3-judge 9th Circuit panel then reversed the district court's dismissal of the CFAA counts, limiting the *Brekka* holding, and (mostly) aligning the 9th Circuit with the other circuits.

Only a year later, sitting *en banc*, the 9th Circuit replaced the panel decision and held that the CFAA expressly prohibits improper "access" to computerized information but not misuse or misappropriation, creating a clear circuit split. Indeed, the *en banc* court found that interpreting the CFAA to criminalize Nosal's misappropriation of his former employer's data, would "transform

the CFAA from an anti-hacking statute into an expansive misappropriation statute." In fact, the 9th Circuit suggests that such innocuous activities as online shopping or "visiting www.dailysudoku.com" could be the next step on the slippery slope of criminalizing "use" rather than "access."

The 9th Circuit's limitation of the CFAA should remind employers to pay attention to security protocols for their sensitive proprietary information. Under the *Nosal* holding, an employer with branches in multiple states now faces different standards for whether its computer-use policy protects its proprietary data. In many states, including but not limited to Louisiana, Mississippi, Texas, Illinois, Indiana and Wisconsin, a carefully crafted computer-use policy will ensure that employees who inappropriately "use" information they obtain from their employers, will be liable under the CFAA.

In contrast, employers in the 9th Circuit cannot rely on this protection. Thus, these business owners should evaluate their physical internal data protection strategies to ensure that information is as protected as possible from misappropriation.

However, all is not lost for 9th Circuit employers concerned with data protection. In the *Nosal* opinion, the 9th Circuit emphasizes that while it splits from the decisions in the 5th, 7th and 11th Circuits, it does not annihilate trade secret protections. Instead, the CFAA addresses hacking, or the "circumvention of technological access barriers," while other statutes address economic espionage or the theft of trade secrets. Indeed, in recent years, the federal government has increased its focus on intellectual property and trade secret protection under statutes such as the Economic Espionage Act. Similarly, civil juries have drastically increased the size of intellectual-property jury awards.

Finally, if a petition is filed, the Supreme Court may choose to accept certiorari on the interpretation of access versus use in the CFAA. Thus, employers should keep track of the Supreme Court docket to assess whether the Nosal opinion will actually impact their employment decisions.

Thomas P. O'Brien *is a litigation partner with Paul Hastings in Los Angeles, where he leads the firm's White Collar practice on the West Coast.*

Daniel Prince *is an associate in the Litigation and Intellectual Property practices of Paul Hastings and is based in the firm's Los Angeles office.*

Katy Wanner *is an associate in the Litigation practice of Paul Hastings' Los Angeles office.*