Patterson Belknap Webb & Tyler LLP

Alert December 2015

The "Cannibal Cop" and Protection of Computerized Data

In an unusual criminal case, the Second Circuit Court of Appeals recently weighed in on an important question at the intersection of employment law and data security.[1] The decision will likely have implications wherever questions arise about unauthorized access and use of computerized data—from a disloyal employee who extracts trade secrets from an employer's system in violation of an employment agreement, to a business that scrapes valuable information from a competitor's website for competitive use in violation of the site's use provisions.

The issue concerned the interpretation of the Computer Fraud and Abuse Act ("CFAA"), a statute that imposes both criminal and civil liability on any person who "exceeds authorized access" to a computer and obtains information from it. 18 U.S.C. § 1030. The federal courts have been divided on whether someone who is authorized to access particular information from a computer but does so for an impermissible purpose has violated the statute. The Second Circuit said no: if a person is authorized to access particular information from the computer, the fact that he or she did so in violation of the terms under which he or she was permitted access does not make the conduct unlawful under the CFAA.

The case involved Gilberto Valle, who has been dubbed by the press as the "Cannibal Cop." Valle was a New York City police officer who participated in an Internet sex fetish community called Dark Fetish Network ("DFN"). According to the case opinion, Valle communicated with other DFN members about committing horrific acts of sexual violence, including kidnapping, raping, torturing, and cannibalizing various women. Using an NYPD computer program, he searched for information about a particular woman whom he had discussed kidnapping with another DFN member. Although he was permitted to use the computer program as part of his job, this particular search violated NYPD policy, which barred use of the program for purposes other than an officer's official duties.

Based on this conduct, Valle was charged with violating the CFAA and with conspiracy to kidnap. A jury found Valle guilty on both charges. The trial judge granted Valle's motion for a judgment of acquittal on the conspiracy charge but let stand the jury's verdict of guilt on the CFAA charge.

On appeal, the prosecution argued that Valle had "exceed[ed] authorized access" of the police computer program—and therefore violated the CFAA—by using the program for a non-police purpose, in violation of his employer's rules. On this view, the terms of use are a condition of access to the information, such that use for an unauthorized purpose is no better than accessing prohibited information. Valle argued that his purpose in accessing the computer program did not matter: as a police officer he was authorized to access the program and that the "exceeds authorized access" language of the statute applies solely when a person who is allowed to access only certain information on a computer instead accesses information that was prohibited to him.

Reviewing the statutory language, the legislative history, and the motivating policies behind the Act, the court found some support for both interpretations. However, because the CFAA is a statute that carries criminal penalties, the court applied the rule of lenity and resolved the uncertainty in the manner that favors the defendant. The court thus found that if a defendant was authorized to access information from a computer for any purpose, then the act of accessing it does not violate the CFAA, even if the defendant used the information for an improper purpose.

---

1 *United States v. Valle*, No. 14-2710-cr, 2015 U.S. App. LEXIS 21028 (2d Cir. Dec. 3, 2015).

The court expressed concern that the prosecution's reading of the statute would make the application of a criminal statute depend on "the vagaries of private policies that are lengthy, opaque, subject to change and seldom read."[2] The prosecution's argument, the court noted, would make a criminal out of "any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy."[3] Therefore, the court reversed the judgment of conviction as to the CFAA charge.[4]

The Importance of the Decision

The *Valle* decision takes out of the hands of businesses in the Second Circuit what might have been a potent weapon to protect their valuable data. Because the CFAA provides civil as well as criminal remedies, and (as interpreted) covers all computers connected to the Internet, businesses have attempted to invoke it against, for example, employees who take their employer's data to set up competitive businesses[5] and website users who "scrape" content from the business's site in violation of the site's terms of use.[6] Although businesses can attempt to use contracts to bar such unapproved uses of their data, this requires mutual manifestation of assent, which may, in some instances, be more difficult to obtain and demonstrate than it is to show that a user was not authorized to access data for a particular purpose.

The use of the CFAA to punish persons like Valle, who accessed a federal database to obtain information about an alleged intended kidnapping victim, or even disloyal employees who attempt to extract an employer's trade secrets, may strike many as very different from the prospect of bringing this statute to bear on persons who merely use information available on publicly accessible websites in violation of the posted terms of service. The hypothetical prosecution of "millions" of Americans for the latter "offense" weighed on both the majority in *Valle* and in prior decisions of other courts that have adopted the narrower view of the reach of the CFAA.[7] Thus, in order to avoid possible application of the CFAA to unintended and seemingly draconian circumstances, the court construed it as inapplicable to *any* instances where the defendant had actual access to the computerized information but used it for an unauthorized purpose, no matter how clear the prohibition or the user's assent to such conditions on access.

The court's decision in *Valle* further deepens an existing split among the federal courts of appeals.[8] It was also accompanied by a vigorous dissent from one member of the three-judge panel. It is therefore a potential candidate

2 *Id.* at *48 (quoting *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (*en banc*)).
3 *Id.* at *49 (quoting *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012)).
4 In the more widely discussed aspect of the opinion, the court affirmed the trial court's judgment of acquittal on the conspiracy charge, finding that the evidence presented at trial was insufficient for a reasonable jury to conclude beyond a reasonable doubt that Valle had the specific intent to kidnap anyone, rather than simply fantasizing about doing so.
5 *See, e.g.*, *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012).
6 *See, e.g.*, *Craigslist, Inc. v. 3Taps, Inc.,* 964 F. Supp. 2d 1178, 1183-84 (N.D. Cal. Aug. 16, 2013) (denying motion to dismiss CFAA claim against business that persisted in "scraping" data from Craigslist even after Craigslist withdrew the business's authorization to use the Craigslist website).
7 *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (*en banc*).
8 *Compare WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (affirming dismissal of CFAA claim against defendant who, while employed by plaintiff, allegedly took from the plaintiff information that he had access to and shared it with a competitor in violation of the plaintiff's employment policies) *and United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (*en banc*) (affirming dismissal of CFAA indictment against employee who took information he had access to from his employer and shared it with a competitor) *with United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (affirming CFAA conviction against government employee who admitted at trial that he accessed information from his employer's database in violation of the employer's policies); *United States v. John*, 597 F.3d 263, 270-73 (5th Cir. 2010) (affirming CFAA conviction against bank employee who had access to customer account information and shared it with her brother, who used it to incur fraudulent charges; holding that "'authorized access' or 'authorization' may encompass limits placed on the use of information obtained by permitted access to a computer system"); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (reversing dismissal of CFAA suit and holding that when an employee breached his duty of loyalty to his employer, his agency relationship was terminated, thereby ending his authority to access company data); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581-84 (1st Cir. 2001) (holding that a former employee who scraped prices from his former employer for a competing student travel business exceeded his authorized access to information by violating his employer's confidentiality agreement).

for review by the *en banc* Second Circuit Court of Appeals or the United States Supreme Court. At present, however, the *Valle* decision likely removes a valuable weapon in a business's arsenal against those who would misappropriate its data, while providing some comfort to users of publicly accessible websites that a violation of posted terms will not by itself lead to CFAA sanctions in the Second Circuit.

The CFAA was enacted in the 1980s, before there were personal computers with Internet access on virtually all desks (and certainly those of every employee), and, at a time when hacking and data breaches did not grab headlines on a weekly basis. Nonetheless, the security of proprietary data can be threatened not only by technical hacking but by all manner of unauthorized use. The statute is undoubtedly due for an overhaul so that Congress can speak with more precision to the types of conduct it intends to penalize, in light of current circumstances and shifts in the technological, legal, and regulatory landscape.

In the interim, decisions such as *Valle* serve as a reminder for businesses to ensure that other data security measures are in place to protect information that they intend to share with limited groups of users and for limited purposes. These measures include comprehensive confidentiality and computer use policies for employees, clear and enforceable website terms and conditions, placing data behind affirmative assent walls (requiring the user to click "I agree" to obtain access), and robust contracts with subscribers and customers. Implementation of these types of policies and practices increase the ability of businesses to pursue remedies for breach of contract (or, in the case of misuse of information by employees, for breach of the duty of loyalty) in cases where the CFAA might have been applied in the past.

Lisa E. Cleary	**212-336-2159**	**lecleary@pbwt.com**
Jonah M. Knobler	**212-336-2134**	**jknobler@pbwt.com**
Robert W. Lehrburger	**212-336-2996**	**rwlehrburger@pbwt.com**
Robert P. LoBue	**212-336-2596**	**rplobue@pbwt.com**
Craig A. Newman	**212-336-2330**	**cnewman@pbwt.com**
Jeremy A. Weinberg	**212-336-2129**	**jweinberg@pbwt.com**