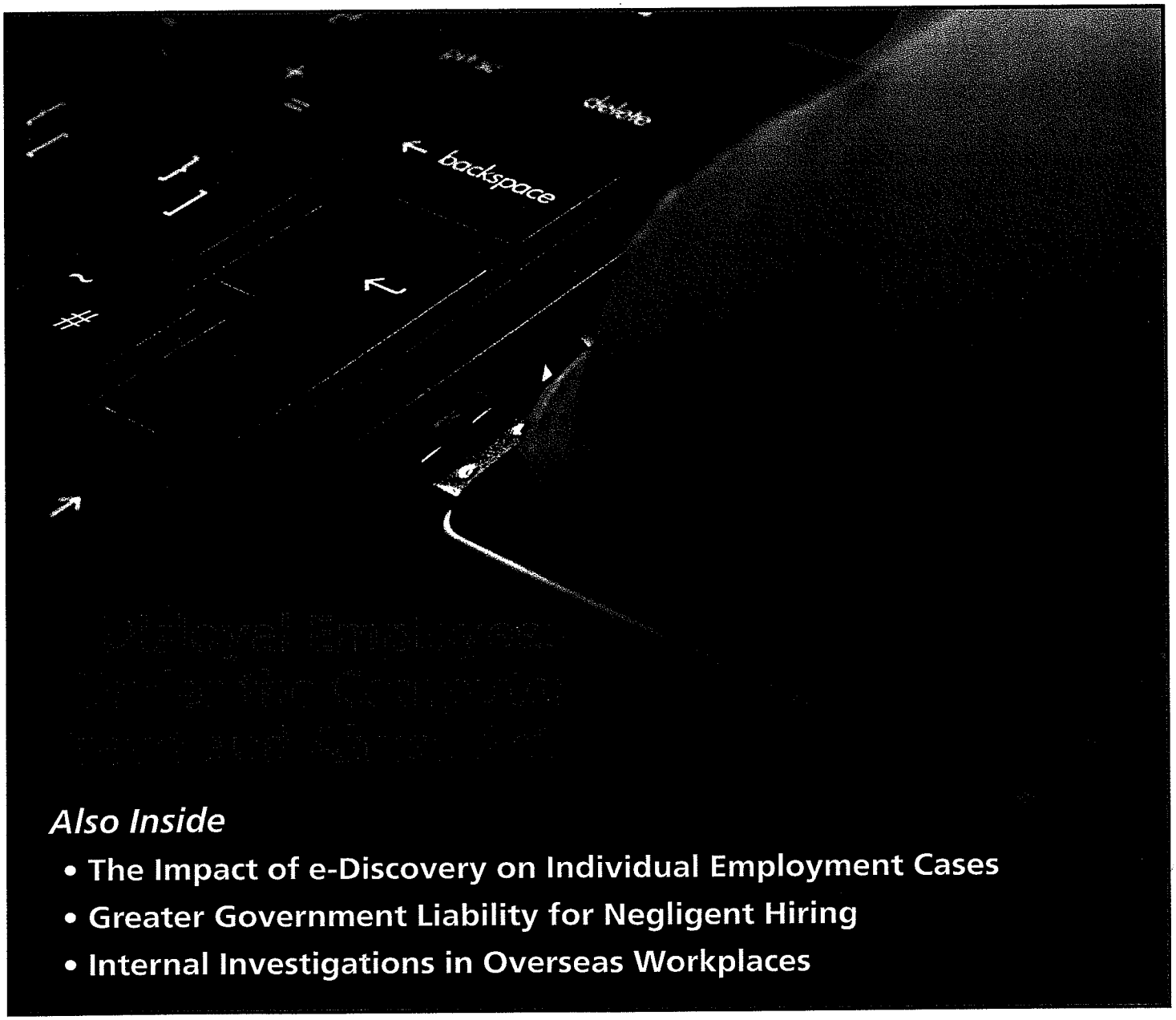
NYSBA SUMMER 2013 | VOL. 38 | NO. 2

Labor and Employment Law Journal

A publication of the Labor and Employment Law Section
of the New York State Bar Association



Also Inside

- The Impact of e-Discovery on Individual Employment Cases
- Greater Government Liability for Negligent Hiring
- Internal Investigations in Overseas Workplaces

NYSBA

Disloyal Employees Under the Computer Fraud and Abuse Act: Recent Splits of Authority Within the Second Circuit

By Stephen W. Aronson and Ian T. Clarke-Fisher

The Computer Fraud and Abuse Act (CFAA or "the Act")[1] is mainly a federal criminal anti-hacking statute enacted in the 1980s to provide federal court jurisdiction to prosecute attacks from computer hackers.[2] The Act prohibits a list of computer crimes involving the unauthorized access to computer systems.[3] In addition to its criminal provisions, the Act also provides a civil cause of action.[4] Employers have been asserting civil CFAA claims against former employees, alleging that those employees violated the Act by accessing and retaining information to be used to compete against the former employer in the future. The Act's civil provisions enable employers to bring what essentially are common law misappropriation claims in federal court. Using the Act to prosecute disloyal employees arguably tests the boundaries of the Act, calling for examination of its purpose and targeted audience.

I. CFAA's Apparent Ambiguity

An increasing number of employers are filing claims for CFAA violations in situations where employees allegedly took confidential information from their employers' computer systems, where the employees allegedly lacked authorization to access such information or exceeded their authority in accessing such information. Although the Act was designed to prohibit third-party hacking, CFAA also may apply to an individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains...information from any protected computer."[5] A computer is a "protected computer" under the Act when it "is used in or affecting interstate or foreign commerce."[6] Given this definition, many employers' computers will qualify as protected computers under the Act. As applied to employees, CFAA seemingly imposes liability against an employee who acts "without authorization" or who "exceeds authorized access"[7] when accessing his employer's computers. The Act defines "exceeds authorized access" as "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."[8] The Act does not, however, define "without authorization." The apparent ambiguity of these terms ("without authorization" and "exceeds authorized access") as defined by the Act has led to a split among the federal circuit courts. The courts have wrestled with these terms, trying to balance the Act's focus on third party hackers with the plain meaning of "without authorization" and "exceeds authorized access." In applying the Act to the employer-employee relationship, the courts have reached conflicting results.

II. Circuit Split

The federal circuit courts that have considered CFAA in the employment context may be grouped into those favoring a broad application and those favoring a more narrow application. The First, Fifth, Seventh, and Eleventh Circuits have ruled that the language of the Act is broad enough to encompass "the situation in which an employee misuses employer information that he or she is otherwise permitted to access."[9] The Fourth and Ninth Circuits have ruled "that the statute does not reach the mere misuse of employer information or violations of company policies."[10] These two sets of rulings have been coined the "broad approach" and the "narrow approach," respectively.

The courts applying the "broad approach" have relied on "agency" principles to rule that the Act applies when employees use their access to their employers' computers in contravention of their employers' interests.[11] According to those courts, an employee who uses his authorized access for purposes other than those aligned with his employer's interests is accessing his employer's computers without authorization. Stated differently, the courts applying the "broad approach" have determined that employees who violate their duty of loyalty to their employers also have violated CFAA.[12] Other courts have applied the "broad approach" when an employee is alleged to have violated his employer's computer use policy or employee handbook, determining that such actions are deemed to exceed the employee's authorized access under the Act.[13] This latter interpretation arguably poses a significant floodgate issue for the federal courts because routine computer use by employees may exceed their authorization under their employers' computer use policies.[14] Whatever the rationale, the "broad approach" permits the application of CFAA to current and former employees who were authorized to access their employers' computers during the term of their employment but who, as alleged by their employers, exceeded their authorized access.

Conversely, the courts applying the "narrow approach" have relied on three general rationales in declining to extend CFAA to employees. First, the courts have differentiated initial access from later use, determining that CFAA does not prohibit misuse or misappropriation; rather, it merely prohibits improper access by employees. Second, since CFAA is primarily a criminal statute, courts have noted that ambiguities should be interpreted narrowly pursuant to the rule of lenity.[15] Third, courts applying the narrow approach point out that the plain language of the statute and the legislative history show that Con-

gress intended to address outside computer hacking and not to provide federal jurisdiction to protect trade secrets or address misappropriation of properly obtained materials.[16] Thus, the "narrow approach" confines the application of the Act to those more egregious instances where a former employee truly went outside the scope of his authorization or was never authorized to begin with, and differentiates between an employee's access and later use of appropriated information.

While the current split among the circuit courts is clear and the potentially broad application of CFAA to virtually every employee who uses a computer is recognized, neither the United States Supreme Court nor Congress has yet to address these issues. In fact, following a recent Ninth Circuit decision the U.S. Solicitor General declined to petition for certiorari. Following the Fourth Circuit decision, a petition for certiorari was filed but, in January of 2013, the petition was dismissed at the parties' request as they apparently reached a settlement. In the Second Circuit, the scope of CFAA remains undecided and the Act's application continues to be a tool, at least at the pleading stage, for employers to bring actions in federal courts and to address alleged employee wrongdoing with respect to the employers' computer systems.

III. Recent District Court Decisions Within the Second Circuit

While the Second Circuit has not yet ruled on the scope of CFAA in the employment context, district courts within this Circuit have done so with increasing frequency and varied results. Some district courts have used the "broad approach" and permitted claims under CFAA for alleged violations of an employer's computer usage policies, while other courts have adopted the "narrow approach" and prohibited such claims against former employees sounding primarily in misuse and misappropriation.[17]

In March 2013, district courts within the Second Circuit issued two decisions, one in the U.S. District Court for the District of Connecticut and the second in the U.S. District Court for the Southern District of New York, which interpreted CFAA in differing and, arguably, conflicting manners.[18] In *Amphenol Corp. v. Paul*,[19] the Connecticut court denied a former employee's motion to dismiss his former employer's claim, ruling that CFAA could apply to an employee who allegedly misappropriated computer information even though he had authorization through the course of his employment to access such information (the "broad approach"). In *JBCHoldings NY LLC v. Pakter*,[20] the New York court granted the defendant employee's motion to dismiss, ruling that CFAA could not apply to the mere misuse of employer information or violations of an employer's computer policies (the "narrow approach").

In *Amphenol Corp. v. Paul*, the plaintiff employer alleged that the defendant former employee accessed confidential information in violation of a written Intellectual Property Agreement (the "IPA") which included language that the employee "shall have access to such confidential information solely for performing the duties of [the employee's] employment...."[21] There was no dispute that the former employee had permission to access his employer's computers during his employment. The employer argued that, even though the employee had lawfully accessed the employer's computers during his employment, his retention of information following the end of his employment resulted in a violation of the IPA, and effectively retroactively rescinded the employee's once lawful access. Essentially, the employer argued that any actions taken by the employee after his employment that were not solely for his employer were in violation of the IPA. Thus, such actions were without authorization or in excess of the employee's authorized access. The alleged breach of the IPA was determined by the court to satisfy CFAA.

In reaching its decision to apply the "broad approach," the *Amphenol* court explained: "[Employee] did not hack into [employer's] computer system to obtain information nor did he access [employer's] information in the ordinary course of his duties. Until the second circuit determines that the CFAA does not encompass this alleged misconduct [misappropriation], the court concludes that it is appropriate to deny the motion to dismiss."[22] Notably, this holding references the varying decisions and rationales among the district courts within the Second Circuit and beyond, and in so doing, applied the "broad approach" without explicitly weighing the merits of either approach.

In contrast, the *JBCHoldings* court, which issued its decision only a week before the *Amphenol* decision, analyzed the varying approaches of CFAA as applied to employee misappropriation cases, determined under similar facts that the narrow approach should apply, and dismissed the CFAA count.[23] The relevant facts are similar to the allegations in *Amphenol*: the defendants allegedly misappropriated information from their employer in violation of the employer's electronic media policy.[24] The court decided to apply the "narrow approach" based not only on Congressional intent and the plain language of the Act, but also on general policy considerations. The court explained that applying CFAA in such a broad-based manner so as to encompass allegations of employee misuse is unnecessary as there exist multiple claims that cover these areas, both in contract and tort, and "because computers today are ubiquitous, the broad reading of the CFAA would permit such localized wrongs—breaches of contract, in form or substance—to be litigated in federal court."[25] The court concluded that the alleged actions, although arguably in violation of the plaintiff's computer media policy, did not amount to a claim under CFAA "because an employee does not 'exceed authorized access' or act 'without authorization' when she misuses information to which she otherwise has access."[26]

IV. Consequences and Application

As a clear split of authority exists in the Second Circuit, and among other circuits, employers, employees, and their legal counsel are left with continued ambiguity and varied approaches to addressing the scope of CFAA in employment disputes. If the "broad approach" is applied, such as in the recent Connecticut decision, employers have a direct route to federal court where claims related to violations of CFAA, such as breach of written confidentiality agreements, conversion, and misappropriation, increasingly will be litigated. In addition, although not addressed in this article, the "broad approach" may lead to the application of the Act's criminal penalties to disloyal employees who are found liable under the Act. To take full advantage of the broad approach as it presently exists, employers may benefit from implementing or revising their computer use policies, either through general usage policies or in non-compete/confidentiality agreements. Employers may establish boundaries to address unfaithful employees and to provide a foundation for asserting claims under CFAA. If the "narrow approach" is applied, however, such as in the recent New York decision, employers may have to rely on common law contract and tort claims, primarily in state court, as they have in the past, and will not have a direct route to the federal courts. In any event, employers should be wary of granting access to their employees, securely store confidential information, and continue to establish proper usage policies and employment agreements to protect themselves regardless of the eventual interpretation of CFAA.

Endnotes

1. 18 U.S.C. § 1030 (2009).
2. H.R. Rep. No. 98-894, at 10-11 (1984) (The purpose of the Act is to address hackers who trespass into computer systems.).
3. 18 U.S.C. § 1030 (a)(1)-(7).
4. 18 U.S.C. § 1030 (g).
5. 18 U.S.C. § 1030 (a)(2).
6. 18 U.S.C. § 1030 (e)(2).
7. 18 U.S.C. § 1030 (a)(2), (4).
8. 18 U.S.C. § 1030 (e)(6).
9. *JBCHoldings NY, LLC v. Pakter*, 2013 U.S. Dist. LEXIS 39157, at *13 (S.D.N.Y. Mar. 20, 2013); *see United States v. John*, 597 F.3d 263, 271-72 (5th Cir. 2010) (employee "exceed[ed] authorized access" when he used employer information, to which he had access for other purposes, to perpetrate a fraud); *United States v. Rodriguez*, 628 F.3d 1258, 1263-64 (11th Cir. 2010) (employee "exceed[ed] his authorized access" when he accessed information for a non-business reason in violation of employer policy); *Int'l. Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (based on principles of agency, employee's authorization to use employer's laptop ended once he violated duty of loyalty to employer, and thus employee accessed computer "without authorization"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir. 2001) (disloyal employee "exceed[ed] authorized access" when he breached employer confidentiality agreement by helping competitor obtain proprietary information).
10. *JBCHoldings*, 2013 U.S. Dist. LEXIS at *14; *see WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 203-07 (4th Cir. 2012) (rejecting agency-based theory and holding that employee who downloaded an employer's confidential information, emailed it to his personal account, and provided that information to employer's competitor was not liable under CFAA); *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (ruling that "the CFAA does not extend to violations of [employee] use restrictions," where employee of executive search firm used employer's information, in violation of a non-compete agreement, to set up competing executive search firm).
11. *See Int'l. Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006).
12. *Id.* at 420-21.
13. *United States v. Rodriguez*, 628 F.3d 1258, 1263-64 (11th Cir. 2010); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir. 2001).
14. The criminal component of the act has likewise received significant press in recent months following the tragic suicide in January, 2013, of Aaron Swartz, an internet activist, who was facing felony charges under the CFAA as a result of attempts to download academic articles from JSTOR. Following Mr. Swartz's death, there has been an outcry among certain communities and groups, including the ACLU, to reconsider the CFAA. *See* https://www.aclu.org/secure/help-protect-the-next-aaron-swartz.
15. The rule of lenity directs courts to construe statutory ambiguities in criminal statutes in the defendant's favor. *See U.S. v. Bass*, 404 U.S. 336, 347 (1971).
16. *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 383-84 (S.D.N.Y. 2010).
17. *Compare Advanced Aerofoil Techs., AG v. Todaro*, 2013 U.S. Dist. LEXIS 25711 (S.D.N.Y. Jan. 30, 2013) (narrow approach); *Westbrook Techs., Inc. v. Wesler*, 2010 U.S. Dist. LEXIS 70901 (D. Conn. July 15, 2010) (narrow approach); *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378 (S.D.N.Y. 2010) (narrow approach), *with Mktg. Tech. Solutions, Inc. v. Medizine LLC*, 2010 U.S. Dist. LEXIS 50027 (S.D.N.Y. May 18, 2010) (broad approach); *Starwood Hotels & Resorts Worldwide, Inc. v. Hilton Hotels Corp. n/k/a Hilton Worldwide, et al.*, 2010 U.S. Dist. LEXIS 71436 (S.D.N.Y. June 16, 2010) (broad approach).
18. *Schaeffer v. Kessler*, 2013 U.S. Dist. LEXIS 38781 (S.D.N.Y. Mar. 20, 2013), presents a third CFAA/employee decision in the Second Circuit during the month of March; however, the allegations in that complaint include the destruction of computer files, making the decision inapposite from the two discussed.
19. *Amphenol Corp. v. Paul*, No. 3:12-cv-543 (D. Conn. Mar. 28, 2013) (Doc. 143).
20. *JBCHoldings NY, LLC v. Pakter*, 12-Civ. 7555, 2013 U.S. Dist. LEXIS 39157 (S.D.N.Y. Mar 20, 2013).
21. *Amphenol, supra* note 19, at 4.
22. *Id.* at 14.
23. *See JBCHoldings, supra* note 20, at *16-17 ("This Court finds the narrow approach to be considerably more persuasive: When an employee who has been granted access to an employer's computer misuses that access, either by violating the terms of use or by breaching a duty of loyalty, the employee does not 'exceed authorized access' or act 'without authorization.'").
24. *Id.* at *24-27.
25. *Id.* at *24.
26. *Id.* at *25.

Stephen W. Aronson is a partner and Ian T. Clarke-Fisher is an associate in the Labor & Employment Practice Group of Robinson & Cole LLP in Hartford, Connecticut. Their practice includes the representation of companies in federal and state courts and before administrative agencies in the full range of employment law claims.