LeClairRyan Labor & Employment Law Newsbrief

Spring 2010

TABLE OF CONTENTS

The Computer Fraud and Abuse Act and Disloyal Employees

by Leslie Paul Machado, Esq.

In the ongoing battle between employers and disloyal employees, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA") is a powerful weapon increasingly used by employers. Interestingly, while several courts have endorsed claims under the CFAA, other courts have rejected employers' attempts to bring these claims in virtually identical cases. This article will briefly discuss the case law in this developing area and provide recommendations on how employers can best position themselves to assert a CFAA claim.

Typical Scenario

The fact scenario in the case law is virtually identical: an employee is given access to his company's files for use in the course of his daily work. At some point, he decides to open his own competing business or join a competitor. The employee downloads company files to a thumb drive and/or emails them to his personal email account. That information, which often includes customer lists, pricing schedules and/or marketing plans, is then used to compete with the former employer.

While the former employer may have a claim for breach of an employment agreement, tortious interference with ongoing and/or prospective opportunities, misappropriation of trade secrets, civil conspiracy, conversion and, potentially, breach of fiduciary duty (depending on the former employee's position), the employer may also have a claim under the CFAA, which would allow it to bring the suit in federal court. Additionally, because the CFAA also includes criminal penalties, a viable CFAA claim significantly increases a defendant's exposure and could encourage settlement.

The Computer Fraud & Abuse Act

The CFAA was passed by Congress in 1984 to combat hackers who accessed computers to steal information, as well as criminals who possessed the capacity to "access and control high technology processes vital to our everyday lives." H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 16, 1984). It provides that whoever "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" shall be punished. 18 U.S.C. § 1030(a)(4).

The statute also provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

Congress, however, did not define the term "without authorization" in the statute. Courts confronting a CFAA claim against a disloyal employee who was authorized to access company information, but exploited such permission to transfer his employer's information, have reached opposite conclusions.

The Expansive View of the CFAA

The leading case allowing a CFAA claim against a disloyal employee is *Intl. Airport Ctr. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). In that case, an employer loaned its employee a laptop to record data he collected in the course of his work. When the employee decided to open a rival company, he used the information on his laptop to benefit his new company. The *Citrin* court held that when the employee decided to act in his own interests, instead of his employer's interests, his "authority to access the laptop" ended (cont. page 2)

LECLAIRRYAN

WWW.LECLAIRRYAN.COM

CALIFORNIA \ CONNECTICUT
MASSACHUSETTS \ MICHIGAN
NEW JERSEY \ NEW YORK
PENNSYLVANIA \ VIRGINIA
WASHINGTON, D. C.

CFAA cont.

"because the only basis of his authority had been that relationship." *Id.* at 420-21. As such, the court held, he was "without authorization" as defined by the statute and the claim under the CFAA was proper. *Id.*

Numerous other courts have adopted *Citrin's* reasoning. *See, e.g., Boxes of St. Louis, Inc. v. Davolt*, 2010 U.S. Dist. LEXIS 12482, *8 (E.D. Mo. Feb. 12, 2010) (rejecting defendants' argument that CFAA does not apply to rogue employees who were granted access to employer's computer network, but exceeded authorized use to download files to compete with employer); *Ervin & Smith Adver. & Pub. Rels., Inc. v. Ervin*, 2009 U.S. Dist. LEXIS 8096, *22-23 (D. Neb. Feb. 3, 2009) ("This Court concludes that while the Defendants ordinarily may have been authorized to access the information they appropriated from Plaintiff, that authorization was terminated when Defendants destroyed the agency relationship by accessing and appropriating the protected information for their own personal gain and against the interest of their employer.")

The Narrower View of the CFAA

Other courts confronting the same fact situation reached contrary conclusions, however, holding that an employer could not assert a CFAA claim because the employee's access was "authorized" when the employer gave him/her access to the network. For example, in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the employee emailed confidential company documents to his personal email account and used that information to compete with his employer. The Ninth Circuit held that the district court correctly granted the employee's motion for summary judgment. It rejected the employer's argument "that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's intent." *Id.* at 1133. Rather, the court explained:

> when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations. It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or "without authorization." *Id.*

Similarly, in *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008), an employee emailed numerous documents to his personal email account containing his employer's confidential and proprietary information. He then left his employer and began working for a competitor, using the confidential and proprietary information. The court held that the employee could not have been "without authorization" when he accessed the confidential information because his employer had given him authorization to the files during his employment. Id. at 967. *See also Remedpar, Inc. v. Allparts Medical, LLC,* 2010 U.S. Dist. LEXIS 152, *23 (M.D. Tenn. Jan. 4, 2010) (granting motion to dismiss CFAA count because the complaint "makes it clear that Camacho was authorized to access all aspects of the ROCS application while he was engaged by RMP. RMP complains, not that Comacho went beyond his authorization to access information he was not entitled to see, but that he subsequently misused that information by sharing it with Allparts"); *U.S. Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1191-92 (D. Kan. 2009) (agreeing with defendants that "in committing the allegedly wrongful acts – obtaining confidential information on their work computers, e-mailing it to their personal emails, and later disclosing it to their new employer – they did not access plaintiffs' computers without authorization... because they were authorized to access that particular information in their employment with plaintiffs").

Recommendations

Ultimately, the split among the circuits will be resolved by the Supreme Court or clarified by Congress. Until then, however, an employer wanting to position itself to assert a CFAA claim should take several steps to strengthen its position. First, the employer should amend its employment manual to provide that any authorization to the company's network/files/data automatically terminates when the employee has been terminated, tenders his/her resignation or forms an intent to leave the employer for any reason, irrespective of whether the employer has actually blocked the employee's access.

While this language does not guarantee that the employer will be able to assert a claim under the CFAA, it would strengthen such a claim because it responds to those decisions which look to the authorization given to the employee. *See, e.g., LVRC*, 581 F.3d at 1136 ("we hold that a person uses a computer 'without authorization' . . . when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway").

An employer should also make clear in its employment handbook/manual or employment agreement that any authorization is only in furtherance of the employer's business purposes, and that any other access is unauthorized. Several courts have relied on such language to allow a CFAA claim. *See, e.g., Ervin & Smith Adver. & Pub. Rels., Inc. v. Ervin*, 2009 U.S. Dist. LEXIS 8096, *24 (D. Neb. Feb. 3, 2009) (relying upon language in employee handbook which provided that access to protected information was only for business purposes); *Modis, Inc. v. Bardelli*, 531 F. Supp. 2d 314, 319 (D. Conn. 2008) (same).

Several of the decisions also emphasize that employers allowed employees to retain access to the network or laptops after separation. *See, e.g., LVRC*, 581 F.3d at 1130 (employer did not change remote access password for several months after employee's termination); *Mintel Int'l Group, Ltd. v. Neergheen*, 2010 U.S. Dist. LEXIS 2323, *12 (N.D. Ill. Jan. 12, 2010) ("During his exit interview, Neergheen was not asked to return his laptop or his electronic storage drives, and he continued to use the laptop that he had received from Mintel to surf the web and check email [after his departure]"). Employers must remain vigilant to retrieve laptop computers from employees immediately after an employee gives notice and must change passwords and close remote access upon learning of an employee's intention to leave the company.

The author, Leslie Machado, can be reached at 202.659.6736 or leslie.machado@leclairryan.com.

New Set of EEOC Regulations Fleshes Out the ADA Amendments Act of 2008

by Michael G. Caldwell, Esq.

For two decades, the Americans with Disabilities Act (ADA) has governed many of the most common issues faced by employers. The ADA landscape is now changing, however. A law passed in 2008, and a set of regulations that will be issued shortly, are greatly expanding the set of impairments or conditions that constitute "disabilities" and trigger an employer's obligations to disabled employees. Employers should be aware of how the new regulations broaden their obligations.

In January 2008, Congress passed the ADA Amendments Act (ADAAA) in order to broaden the definition of "disability" under the ADA. The ADAAA directed the Equal Employment Opportunity Commission (EEOC) to flesh out the new definition of disability by issuing a set of interpreting regulations. Last September, the EEOC issued a Notice of Proposed Rulemaking to provide specifics about the new definition of "disability." The EEOC will almost certainly adopt these proposed regulations (29 C.F.R. § 1630) in roughly their present form. Employers, especially human resources professionals, need to understand how the definition of "disability" has been expanded.

The Origin of the EEOC's Proposed Regulations

The easiest way to understand these changes is to understand the history of the ADAAA and the new proposed regulations. When the ADA was passed in 1990, it defined a "disability" as a physical or mental impairment that substantially limits one or more of an individual's major life activities. However, it was not clear exactly what "impairment," or "major life activity," or "substantially limits" meant. Of course, some cases were easy, such as blindness, paralysis, or loss of a limb. But employees began to bring ADA lawsuits based on traits that were not classic disabilities — traits like diseases, infertility, allergies, and conditions that can be fully mitigated by medication. Thus the question of what constitutes a "disability" became a fertile source of litigation.

In the last decade or so, the courts began to narrow the definition of "disability." In 1999, the Supreme Court declared that a person is not disabled if mitigating measures can reduce or limit the person's difficulties. In 2002, the Supreme Court held that a person is not disabled unless the impairment "prevents or severely restricts the individual from doing activities that are of central importance to most people's daily lives." Some lower courts interpreted this standard strictly. As a result, much of the litigation in ADA cases centered on the question of whether the employee was disabled.

By January 2008, a broad political coalition had emerged to reverse the direction that the courts had taken and greatly broaden the set of employees who qualify as disabled. Disability advocates, civil rights groups, and even the U.S. Chamber of Commerce supported a new law on the subject, which later became the ADAAA. In fact, support was so broad that the House of Representatives passed the original version of the ADAAA by a vote of 402 to 17, and both the House and the Senate passed the final version by a voice vote.

Congress decided to speak in strong terms in the ADAAA. The ADAAA specifically states that it is intended to overturn the Supreme Court's decisions in the 1999 and 2002 cases, and that it is Congress's intention that "the question of whether an individual's impairment is a disability under the ADA should not demand extensive analysis."

The ADAAA establishes, among other things: (i) that an impairment need not prevent or severely restrict performance of a major life activity to be a disability; (ii) that many diseases are disabilities; (iii) that an impairment that is episodic or in remission can still be considered a disability; and (iv) that the effect of most mitigating measures, such as medications, should be ignored in deciding whether a person is disabled. Under the last heading, a person is disabled even if measures such as hearing aids, cochlear implants and low vision devices can eliminate the impairment (people with eyeglasses and contact lenses, however, are not necessarily disabled).

In the text of the new law, Congress stated that the current EEOC regulations create too high a standard for defining disability, and expressed its expectation that the EEOC will revise its regulations to make them consistent with the ADAAA. Congress granted the EEOC the authority to issue regulations implementing the new, broader definition of disability.

What the New Regulations Will Likely Say

The ADAAA, like all legislation, left many specifics undecided. The proposed regulations flesh out the Act. The proposed regulations include many provisions that clarify the new, broader definition of "disability." For example, they provide that:

1. Certain conditions will always be considered disabilities, including autism, cancer, cerebral palsy, diabetes, epilepsy, AIDS, multiple sclerosis, muscular dystrophy, major depression and bipolar disorder.
2. Disability will be determined by a comparison of the individual's limitation to the ability of most people in the general population, and this comparison may often be made by common sense, without scientific or medical evidence.
3. If an individual is substantially limited in a "major life activity," the individual is disabled whether or not he or she is limited in the ability to perform activities of central importance to daily life. The ADAAA contains a list of bodily functions that are considered to be "major life activities," and the regulations add a further list, including the cardiovascular and musculoskeletal functions.
4. An employee whose limitations have been completely eliminated by medication or treatment can still be considered disabled. In fact, an employee who has been completely cured is considered disabled if his or her condition previously qualified as a disability. For example, an employee whose cancer has been treated, and whose doctor says he no longer has cancer, is nevertheless covered by the ADA, because he or she has a "record" of being disabled.
5. An employee who has ever been "misclassified" as having a disability is covered by the ADA. For example, the regulations say that an employee who in the past was misdiagnosed with bipolar disorder and hospitalized after having a temporary reaction to medication she was taking is covered, (cont. page 4)

even if she never actually had bipolar disorder.

6. Certain impairments are disabilities for some people and not others. The list includes asthma, high blood pressure, learning disabilities, carpal tunnel syndrome and hyperthyroidism. For example, an employee with asthma may be disabled if the asthma causes the employee to have problems in the workplace with cleaning products, perfumes or cigarette smoke.
7. The ADA applies not just to discrimination based on a disability, but to discrimination based on symptoms, medication or treatment. For example, an individual who is not hired for a driving job because he takes anti-seizure medication has a disability. Thus, if an employer acts on the basis of a manifestation of the disability, it is no defense to say that the employer was not aware of the underlying disability. The regulations discuss the example of an employer who refuses to hire a person because that person has a facial tic. If the facial tic was caused by Tourette's Syndrome, it does not matter whether the employer knew that the person had Tourette's when it decided not to hire him. The fact that the employer acted on the basis of the facial tic is enough.

Understanding the New Proposed Regulations

The new proposed regulations establish just how broad the new definition of "disability" is. In discrimination cases, the focus will now likely be on whether the employer discriminated based on the trait, not on whether the trait is a disability. More employees will be entitled to request reasonable accommodations for their disabilities. The EEOC expects that there will be an increase in requests for accommodations resulting from the ADAAA and the regulations, which will come mostly from people with those impairments that are now automatically defined as disabilities, such as diabetes and bipolar disorder. In its Notice of Proposed Rulemaking, the EEOC estimated that there are 450,000 to one million workers in the United States who have conditions that will automatically be considered disabilities under the regulations.

It would be an exaggeration to say that the proposed regulations mean that any employee who claims a disability must be treated as disabled. For one thing, the proposed regulations provide that temporary impairments of short duration with little or no residual effect are not disabilities. The examples that the proposed regulations give include the common cold, seasonal influenza, sprained joints, and a broken bone that is expected to heal completely. However, an employer who is considering taking an adverse action against an employee (such as an unfavorable reassignment) because the employee has a condition like the flu or a broken bone should consult with an attorney about whether other laws, including state laws, prohibit the action.

There are other situations in which an employee who claims a disability is not disabled. An employer can defeat an employee's lawsuit by showing that the plaintiff's claimed disability is a fake. Further, the ADA still contains a list of conditions that can never be considered disabilities, such as compulsive gambling, kleptomania, and disorders arising from the current use of illegal drugs.

At first glance, the reader may think that the proposed regulations create a "once disabled, forever covered by the ADA" rule. In a sense, that is true. They define the set of people with a "record of impairment" as including anyone who ever had a covered disability, with no time limit. But the ADA only protects the employee from discrimination based on the disability at issue. An employee who had cancer twenty years ago does not have a special protected status, unless the employer takes an action because the employee had cancer twenty years ago.

Some readers may wonder why the person who recovered from cancer is covered, while the person who had a broken bone that healed is not. The key is how long the condition was expected to last when it was first diagnosed. The broken bone was expected to heal completely after a "short duration" when it was first diagnosed. The employee with the broken bone thus never met the definition of disability, and has no "record of impairment." The cancer, on the other hand, was expected to be of longer duration when it was diagnosed, rendering the ill employee disabled. Because that employee was once disabled, he or she is permanently covered.

What Employers Should Do

The proposed regulations' message to employers is clear: many conditions not covered before will now be disabilities under the ADA. Obviously, most employers, and even HR professionals, do not need to memorize all the specifics of the new proposed regulations. What employers do need to remember, whenever a disability issue arises, is that the category of "disabilities" covered by the ADA will now be extremely broad. Whenever an employee requests an accommodation, or an employer becomes aware of a potential discrimination issue, the employer should have an attorney or HR professional consult the ADAAA and the regulations before deciding whether the employee is considered disabled under the ADA, even if it seems like a stretch to call the employee's condition a disability.

The new regulations are available online at http://edocket.access.gpo.gov/2009/E9-22840.htm.

Also, since the ADAAA was passed, the Department of Labor's Job Accommodation Network (JAN) has updated the numerous fact sheets and other documents on its website (http://askjan.org), which are designed to help employers. The JAN has created fact sheets on a huge number of specific disabilities, as well as sample reasonable-accommodation request forms for employers. Nevertheless, the best way for an employer to find out whether an employee's condition is a disability under the new regulations is to consult an attorney who specializes in employment-discrimination matters.

The author, Michael Caldwell, can be reached at 203.672.3206 or michael.caldwell@leclairryan.com.

Employee's Retirement Forfeited USERRA Re-Hire Right, Court Rules

A federal district court in Norfolk, Virginia has ruled that a police officer who retired from the force when he received active duty orders from the Coast Guard had no right to re-employment by the department almost seven years later. In a decision exploring the limits of an employee's right to reinstatement under the federal statute protecting active duty service personnel, the court found that the employee had clearly expressed his intent to permanently retire from the police force and thus had forfeited his reemployment right.

According to the court's decision, written by U.S. District Judge Raymond A. Jackson, Paul Sutton was employed as a lieutenant by the Chesapeake Police Department from 1974 until January 1, 2001. Sutton had served in the Coast Guard since 1979, and on November 25, 2000, Sutton notified his supervisor by letter that he had received active duty orders from the Coast Guard. In the same letter, he indicated that he intended to retire, and did retire from the police department effective January 1, 2001. After serving nearly seven years with the Coast Guard, Sutton then sought reemployment with the police department pursuant to the Uniformed Services Employment and Reemployment Rights Act of 1994, 38 U.S.C. §§ 4301-4335 ("USERRA"). His request was denied because the police department found that he was no longer eligible for reinstatement. On December 19, 2007, Sutton retired from active duty with the Coast Guard because of a compulsory age requirement. After his request to rejoin the police department was denied, he volunteered for the Coast Guard until September 30, 2009. Beginning October 1, 2009, he became a civilian employee of the Coast Guard.

Sutton filed a complaint with the Department of Labor ("DOL") complaining that the department's failure to reinstate him violated USERRA, and the DOL found that Sutton's complaint had merit. Sutton then sued in federal court alleging that the city violated USERRA by failing to promptly reemploy him after receiving his request for reemployment, seeking lost benefits and wages and reinstatement to his prior status, seniority and pay.

In considering the City of Chesapeake and Plaintiff's cross motions for summary judgment, the district court noted that under USERRA, the general rule is that "any person who is absent from a position of employment by reason of service in the uniformed services shall be entitled to reemployment rights" so long as the following conditions are met: (1) the employee gives notice to his employer when leaving; (2) the absence is for less than five years as defined by USERRA; and (3) the employee timely applies for reemployment upon his return. 38 U.S.C. § 4312(a)(1-3). Sutton argued that he met these requirements, but the city argued that because he retired from the police department, he forfeited his right to reinstatement, or in the alternative, that more than five years had elapsed and thus he had no right to reinstatement.

The court noted that relevant to its inquiry is a DOL regulation which provides that even if an employee tells an employer before entering uniformed service that he does not intend to seek reemployment after completing the uniformed service, he does not forfeit his right to reemployment. 20 C.F.R. § 1002.88.

The court found, however, that USERRA's reemployment rights and the regulation at issue did not apply to Sutton. Although the law clearly specifies that an employee does not forfeit his right to reemployment by telling the employer that he does not intend to seek reemployment, the court noted, the law only applies to noncareer military service, and an employee can waive USERRA rights by abandoning his civilian career in favor of a military career.

"Simply put, USERRA only applies to military service members that have a civilian career," the court stated. By retiring from the Chesapeake Police Department, the court found that Sutton abandoned his civilian career in favor of a military career. The court found that Sutton expressed very clearly his decision to enter retirement, which was accepted by the Chief of Police Justice, and that Sutton applied for retirement benefits from the state retirement system, cashed in all of his unused vacation and sick leave, applied for retiree health benefits and participated in his retirement ceremony including attending a retiree banquet. This conduct, the court found, reached an entirely different level than a worker who temporarily retires or leaves employment for active service. His intent was to permanently retire. Any other interpretation would fail to further the purposes of USERRA, which requires the continuation of benefits under the employer's retirement plan as though the employee were still employed and not on military leave. Moreover, it would be unfair to allow an employee to fully retire from civilian employment and receive all retirement benefits, and then require the employer to hold open the position and rehire that worker.

The court also addressed the parties' arguments regarding whether Sutton had exceeded the five-year maximum absence to be eligible for reinstatement under USERRA, and found that Sutton had exceeded that time. Sutton had argued against counting his time of voluntary service toward the five-year maximum, which the court rejected, finding no factual basis for excluding any portion of the six years and seventeen days served by Sutton.

Paul F. Sutton v. City of Chesapeake, No. 2:09cv240 (E.D. Va. February 17, 2010).

Case Summary by Joan C. McKenna, Esq.

U.S. Supreme Court Takes Up 'Sexting' Case

As previewed in an earlier Client Alert, the U.S. Supreme Court recently began hearing arguments in the case of a California police officer who sent sexually explicit text messages on a department-issued pager. But while news reports about *Ontario v. Quon* tend to underscore its potential impact on private employers, it is by no means clear that this case will lead to a new "blueprint" for privacy rules in the American workplace. That is because the case, in which a police chief acquired and read transcripts of texts sent by his officers, involves public-sector employees who have constitutional expectations of privacy--such as those spelled out by the Fourth Amendment--that do not cover their private-sector counterparts.

The case hinges on whether the police chief in Ontario, California, violated the privacy rights of SWAT team member Jeff Quon and three other officers by acquiring and reading records of their texts, many of which turned out to be sexually explicit. The chief, who shared the texts with city officials, had sought to find out whether the officers were reimbursing the department for all personal messages sent from their pagers. The officers sued, and a panel of the U.S. Court of Appeals for the Ninth Circuit ruled in their favor.

While the public nature of this case might limit its ultimate impact on private employers, *Ontario v. Quon* nonetheless touches upon largely unexplored questions that are at the heart of the rapidly evolving field of cyber-liability. It will therefore be closely watched by the employment-law community.

Case Summary by Joseph P. Paranac Jr., Esq.

New Jersey High Court Issues Key Cyber-Liability Ruling—More on the Privacy Front

The New Jersey Supreme Court handed down an important decision in March that could begin the process of sketching out a "zone of privacy" for employees who use company-owned equipment for personal communications. The case, *Stengart v. Loving Care Agency Inc.,* centered on whether e-mails sent by an employee to her lawyer using a company-owned computer are protected by the attorney-client privilege and therefore off-limits from monitoring. It was among the first major rulings on cyber-liability in the private workplace to be issued by a state supreme court.

In its 7-0 ruling, the court said New Jersey-based Loving Care, which provides home-care nursing and health services, erred in retrieving attorney-client e-mails from former employee Martha Stengart's password-protected Yahoo account. Stengart, who had filed a discrimination lawsuit against Loving Care in 2008, sent the e-mails on her work computer before leaving the company, which subsequently took advantage of the information contained in the messages as it put together its legal defense.

Loving Care's attorneys argued that explicit policies in the company handbook notified employees that they had no right to privacy when using employer-owned equipment. But Supreme Court Justice Stuart Rabner wrote that the attorney-client privilege trumps the privacy policies developed by employers, no matter how clearly worded those policies might happen to be. The court also said Loving Care's attorneys broke professional conduct rules by failing to inform Stengart's lawyer of their discovery of these attorney-client communications.

The case highlights a simple truth about the modern American workplace: Over the past 10 years or so, the rise of digital technology has translated into an intertwining of personal and business-related communications that can be exceedingly difficult for employers to negotiate. In the years to come, the courts may well carve out a "zone of privacy" for private employees whereby certain types of communication may be deemed off-limits for use by employers or their legal counsel. The area of cyber-liability, however, is one of the least-defined forefronts in employment law, and is likely to continue to evolve rapidly as employees continue to use all-in-one smart phones and other high-tech devices for both personal and business communications. Meanwhile, customers, employers and employees alike will make increasing use of various social-networking media, in conjunction with their computers, pages and other devices.

The potential conundrums for employers are limited only by the imagination. And indeed, media reports regularly feature stories of the unintended consequences that can occur when employees or employers accidentally forward e-mails to the wrong parties, or inadvertently reveal personal or company information on social networking sites. Employers and their counsel clearly must pay close attention to this evolving trend, and adjust their policies and procedures in real time as case law and common best practices develop.

Case Summary by James P. Anelli, Esq.

Keeping Our Clients Current...

Share this newsletter with your colleagues or ask to add them to the distribution list at enewsbriefs@leclairryan.com.

Just type Employment Law News in the Subject line. The distribution list will also provide Client Alerts on recent cases or legislation and opportunities to train with LeClairRyan via the web or in person.

LeClairRyan's Labor & Employment Attorneys

Partners

Elizabeth K. Acee
James P. Anelli
Daniel J. Blake
Steven D. Brown
Evan A. Burkholder
Michael G. Caldwell
Laura H. Corvo
James K. Cowan, Jr.
Michael J. Dorney
Linda B. Georgiadis
Mark B. Goodwin
Brian S. Inamine
Robyn Gnudi Kalocsay
Christiane Cargill Kinney
Leslie P. Machado
Vijay K. Mago
Margaret P. Mason
Joan C. McKenna
Charles G. Meyer, III
Clinton S. Morse
Susan Childers North
Joseph P. Paranac
David E. Perry
Janet Barringer Pezzulich
Michael J. Plata
Bruin S. Richardson, III
Robert N. Saffelle
Peter B. Van Deventer, Jr.
Jeffrey A. Van Doren
Patrick T. Voke
Karol Corbin Walker

Associates

Barbara J. Bavis
Philip J. Bonoli
Elizabeth M. Ebanks
Sarah E. Moffett
Brian G. Muse
Allison M. Perry
Jill K. Rizzo
Suzette T. Rodriguez
Nancy B. Sasser
Alison D. Stuart

with offices in
Los Angeles, CA
San Francisco, CA
Detroit, MI
Boston, MA
Hartford. CT
New Haven, CT
Newark, NJ
New York, NY
Philadelphia, PA
Washington, DC
Alexandria, VA
Richmond, VA
Norfolk, VA
Virginia Beach, VA
Williamsburg, VA
Charlottesville, VA
Roanoke, VA
Blacksburg, VA