Thursday, September 5, 2013

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

Trials & TRIBULATIONS

Importance of employer policies on technology

Federal, state laws govern the use of employer networks and workplace recording

From alleged NSA email access to Google's recent defense of the purported data-mining of emails sent and received through its email services, third-party access to electronic communications has been the subject of recent media reports, discussion and litigation.

Moreover, devices and applications make it easier for employees to record others in the workplace. Given the current public debate and the advent of new technologies, this is an opportune time to highlight the importance of employer policies governing the use of employer equipment and networks and employee use of recording devices in the workplace.

By SARAH MERKEL
Daily Record Columnist

Policies governing the use of the employer's equipment and networks

Generally speaking, a private employer has a right to access and control use of its systems and networks. However, personal email accounts and "company" accounts created on third-party providers such as Gmail and Yahoo can create legal issues for the unwary employer.

Both federal and New York laws protecting electronic communications have application in the workplace. At the federal level, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2511, established criminal penalties and the right to file a civil action against persons who "intercept" electronic communications, see *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F.Supp.2d 548 (SDNY 2008).

Section 2511(1)(a) provides that, with certain exceptions, anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any ... electronic communication" violates the ECPA. New York law likewise prohibits the interception of electronic communications. However, neither the ECPA nor New York law is violated when a party consents to the interception, 18 U.S.C. § 2511(2)(d); N.Y. Penal Law §§ 250.00(5) & (6), 250.05.

While Sections 2510 and 2511 do not apply to email communications that have already been received by the user's system, the Stored Communications Act (SCA), 18 U.S.C. § 2701, et seq., added criminal penalties as well as a private right of action to the ECPA for the unauthorized accessing of stored electronic communications.

It is a violation of the SCA to access, without authorization, any "electronic communication while it is in electronic storage in such system," 18 U.S.C § 2701(a). This section does not apply to conduct authorized "by the person or entity providing a wire or electronic communications service" or "by a user of that service with respect to a communication of or intended for that user," 18 U.S.C. § 2701(c)(1) & (2).

Thus, under New York and federal law, a private employer's rights to access communications on its own systems are relatively clear. Even if employer access to emails on its system could be considered an "interception," an employee sending or receiving email under an employer's domain name consents to the "interception" of that communication.

Likewise, an employer cannot violate the SCA by accessing stored communications on its own internally-administered system, see *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-115 (3d Cir. 2003) (also noting that "interception" under the ECPA must occur contemporaneously with transmission); *Freedom Calls Foundation v. Bukstel*, 2006 U.S. Dist. Lexis 19685 (EDNY March 7, 2006).

The analysis is more complex when the employee is using a business account created on a third-party service, such as Gmail. In the case of third-party accounts, ownership of the account may be determined in accordance with state law. For example, an Indiana employer ultimately brought a counterclaim alleging that a former employee improperly accessed a Gmail account created by the employee.

Continued ...

Thursday, September 5, 2013

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

Continued ...

The email account was created by the employee without the employer's authorization, and used the employer's name as part of the email address, *Rene v. G.F. Fishers, Inc.*, 2012 U.S. Dist. LEXIS 151225 (S.D. Ind. Oct. 22, 2012). In addressing the plaintiff's motion to dismiss, the court allowed the counterclaim, noting that "property disputes" are governed by state law, and the employer had sufficiently pled ownership of the account.

The employer's argument would have been strengthened by an employer policy clearly dictating that employees were not authorized to create separate email accounts relating to their employment and that any such accounts were the property of the employer. Moreover, to protect the employer from claims of unauthorized access, any policy should include express employee consent to employer interception or access of any such accounts.

Private employee accounts that are accessed through an employer's device or equipment can also create issues for employers. While personal emails already stored on an employer's device may be fair game, an employer may not obtain an employee's password and begin secretly accessing the employee's personal email account, *Pure Power Boot Camp*, 587 F.Supp.2d 548.

Indeed, an employer that discovers nefarious actions through unauthorized access may be barred from using evidence discovered in a subsequent proceeding.

In *Pure Power Boot Camp*, the owner was able to access a former employee's email through passwords saved on the former employee's work computer. She was then able to monitor new personal email messages stored on a third-party server, a violation of the SCA. Even though the former employer uncovered clear wrongdoing, the court precluded, except for impeachment purposes, the use of these communications.

Importantly, although the Pure Power Boot Camp employee handbook did contain language indicating that employees have no right of privacy in materials "stored in, created on, received from, or sent over the system ... includ[ing] the use of personal email accounts on Company equipment," *Id.* at 552 (emphasis in original), the court determined that this policy did not constitute authorization to view personal emails maintained by outside entities such as Microsoft or Google, *Id.* at 559. Moreover, there was no evidence that the communications were "created on, sent through, or received" on the plaintiff's computers, since many of the emails were created subsequent to the defendant's termination, *Id.*

Likewise, an employer doing business as Verizon Wireless discovered the perils of employee personal email stored on a device provided by the employer. A former employee claimed that she mistakenly failed to delete her personal email account before she returned her company-issued BlackBerry device.

The plaintiff alleged that her former supervisor began accessing and reading hundreds of emails that loaded onto the device, for up to 18 months after her departure. The District Court refused to dismiss the employee's ECPA and SCA claims, finding in part that the employee did not give express or implied consent to access her personal emails, L*azette v. Kulmatycki*, 2013 U.S. Dist. Lexis 81174 (N.D. Ohio June 5).

These employers' defenses to any claims of unauthorized access would have been strengthened had the employees expressly agreed to a policy indicating that if an employee chose to add a personal email account to an employer-owned device, or to access a personal email address from the employer's equipment, the employee consented to any interception or access of that account.

Workplace recording

Smartphones and other devices make surreptitious recording in the workplace easier than ever. At least one new iPhone application, aptly named "Heard," allows the user to constantly temporarily record the last five minutes of sound or conversation. Users can then elect to permanently save any activity recorded during that period.

Under New York and federal law, a conversation can legally be recorded as long as one party to the conversation consents, N.Y. Penal Law §250.00(2) & 250.05; 18 U.S.C. § 2511(2)(d). Someone who records a conversation while he or she is not present, and without the consent of at least one conversant, has committed a crime. Users of an application such as Heard could run afoul of the law if they leave their device unattended, with the application running, thus recording a conversation where no party present consented to the recording.

Even without special applications, covert recording in the workplace by employees contemplating litigation has become easier. An employer that wishes to prevent workplace recording should create a clear policy prohibiting such recording, and ensure that it is uniformly enforced.

In such circumstances, terminating an employee for making unauthorized recordings can provide a legitimate, non-discriminatory or non-retaliatory basis for the employee's termination, see *Chyrianne H. Jones v. St. Jude Medical S.C., Inc.*, 504 Fed. Appx. 473 (6th Cir. 2012).

Employer workplace policies

At a minimum, employers should have policies clearly governing the use of employer email and equipment. In addition to simply notifying employees that they have no expectation of privacy when using employer email, equipment, and servers, employers should clearly communicate that the employer's email system is the employer's property, and any communications can be searched or reviewed. Where an employer is using a third-party domain for work email, the employer should clearly state that any email address created or used by the employee is the employer's property, and that the employee expressly consents to the employer's inter-

Continued ...

Thursday, September 5, 2013

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

Continued ...

ception or access of these communications.

Employee access of personal email can be problematic, especially where a former employee leaves behind stored passwords. Creating a policy, signed by the employee, which clearly indicates that an employee who accesses personal email accounts on employer equipment expressly consents to employer interception or access of those accounts, provides some measure of protection for an employer. However, as a matter of course, employers should always exercise caution and consult counsel before directly accessing an employee's personal email account.

Given the ease with which employees can record in the workplace, a neutral employer policy preventing such recording is important. Such a policy serves to protect employer trade secrets, preserve customer privacy, and can provide protection for the employer when an employee claims that any disciplinary measures imposed were a pretext for discrimination or retaliation.

Technological advances frequently outpace jurisprudence. While good employer policies are not a panacea, they can provide valuable protection in the event of litigation.

Sarah Snyder Merkel is a partner with The Wolford Law Firm LLP, a firm focused exclusively in the area of litigation. The firm handles both civil and criminal matters.