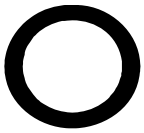

ORRICK

Investigations by Employers and their Attorneys: Traversing the Minefield of Legal and Ethical Restrictions in Cyberspace

Presented by

Julie A. Totten
Orrick, Herrington & Sutcliffe, LLP

Co-written by David Spencer

ABA Section of Labor and Employment Law
2010 Annual Meeting

———

San Francisco, CA

400 Capitol Mall, Suite 3000
Sacramento, CA 95814-4407
Telephone 916 329 4908
Facsimile 916 329 4900
e-mail: jatotten@orrick.com

Investigations by Employers and their Attorneys:
Traversing the Minefield of Legal and Ethical Restrictions in Cyberspace

In the age of electronic communications and social networking websites, employers and their attorneys have a treasure trove of information available to them for conducting workplace investigations. But before utilizing this information, employers must be aware of the legal restrictions on viewing their employees' electronic communications. Attorneys for employers must also be cognizant of several applicable rules of professional ethics when seeking informal access to the electronic communications of parties and relevant non-parties to a lawsuit.

1. Employer Best Practices: Monitoring Employees Without Fear of Liability

Employers should be aware of several bodies of law that may limit their ability to peruse the electronic communications of their employees. Employers should know their rights and obligations under the federal Stored Communications Act ("SCA")[1] and parallel state stored communications laws. Employers should also be wary of the common law torts of invasion of privacy and wrongful termination. Finally, public employers must understand their obligations under the Fourth Amendment. Because all of these bodies of law only apply when the employee has a reasonable expectation of privacy (with the exception of the SCA, which contains a "consent" exemption), employers should develop, and require employees to sign, a comprehensive electronic communications policy. Although such a policy may not be determinative in every case, in many others it will.

a. The Stored Communications Act ("SCA")

In two frequently cited decisions, *Konop v. Hawaiian Airlines, Inc.*,[2] and *Pietrylo v. Hillstone Restaurant Group*,[3] courts have found employers to have violated the SCA by obtaining unauthorized access to their employees' password-protected websites. The SCA prohibits, in relevant part, "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ing] . . . access to a wire or electronic communication while it is in electronic storage in such system."[4] The SCA exempts from liability "conduct authorized . . . by a user of that service with respect to a communication

---

[1] 18 U.S.C. § 2701 *et seq.* Although several employees have also claimed that their employers violated the federal Wiretap Act, 18 U.S.C. § 2510–22, by accessing their electronic communications, courts have almost universally rejected these claims because they have read the statutory term "intercept" to encompass only acquisitions that are contemporaneous with the transmission. *See, e.g., Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003); *but cf. U.S. v. Szymuszkiewicz*, 2009 WL 1873657 at *7–13 (E.D. Wis. 2009) (assuming the contemporaneous standard would apply, but expressing disapproval with it). Because e-mail messages are only in transit for a few seconds, and then reside in temporary storage until accessed by the recipient, the effect of the narrow interpretation courts have given to the Wiretap Act's "interception" requirement is that e-mails and other electronic communications are governed almost exclusively by the SCA, and not the Wiretap Act's more protective regime.

[2] 302 F. 3d 868, 881 (9th Cir. 2002).

[3] 2008 WL 6085437 (D. N.J. July 24, 2008).

[4] 18 U.S.C. § 2701(a).

of or intended for that user."[5] Because courts have interpreted this "consent" exemption narrowly, employers should make certain that they have authorization before accessing an employee's webpage that is protected by privacy controls.

i. *Konop v. Hawaiian Airlines, Inc*.

In 2002, the Ninth Circuit addressed a claim by Hawaiian Airlines ("Hawaiian") pilot Robert Konop that his employer violated the SCA by viewing his secure website without authorization. Konop had created the website at issue in the case as a forum for posting bulletins critical of his employer and union. He restricted access to the site by creating an eligibility list, which contained mostly fellow Hawaiian pilots and employees. Only these eligible individuals could create a username and password, and thereby obtain access. Before accessing the site, a new user had to read and agree to certain terms and conditions of use. These terms and conditions prohibited access by Hawaiian management and forbade users from disclosing the contents of the website to anyone else.[6]

Despite the measures Konop took to keep the website private, Hawaiian Vice President James Davis was able to view the website by using the login information of two different Hawaiian pilots who agreed to help him obtain access. Konop discovered Davis had accessed the website when he received an admonitory telephone call from the chairman of the pilots' union. After this call, Konop began to monitor the viewing records of the two pilots who had cooperated with Davis. In this way Konop determined that Davis logged into the website more than 30 times. Konop then sued, alleging, *inter alia*, violations of the SCA.[7]

The district court granted Hawaiian summary judgment on the ground that it was statutorily exempt from liability because Vice President Davis had obtained authorization from a website "user."[8] The Ninth Circuit reversed. According to the Ninth Circuit, a triable issue of material fact existed with regard to whether the pilots who authorized Vice President Davis to access the website were "users." In making this determination, the Ninth Circuit emphasized that the record indicated only that these pilots were eligible to view the website, not that they ever actually did.[9]

ii. *Pietrylo v. Hillstone Restaurant Group*

Six years after *Konop*, a federal district court in New Jersey rejected an employer's motion for summary judgment under the SCA on a very similar set of facts. The plaintiff-employee, Brian Pietrylo, created a MySpace group called the "Spec-Tator" as a forum in which he and other present and former employees of Houston's restaurant could "vent about any BS we deal with out [*sic*] work without any outside eyes spying in on us." The group was private, and only invitees could visit it. Once an invitee accepted his or her invitation, an icon for the group appeared on the new member's MySpace page. Group members could read existing postings and add postings of their own. The posts on the Spec-Tator included jokes about Houston's

---

[5] 18 U.S.C. § 2701(c)(2).
[6] *Id.* at 872–73.
[7] *Id.* at 873.
[8] *Id.* at 880 (citing 18 U.S.C. § 2701(c)(2)).
[9] *Id.* at 880.

customer service specifications ("specs"), references to violence and illegal drug use, and inappropriate sexual comments about management and customers.[10]

The contents of the Spec-Tator eventually found their way into management's hands through Spec-Tator member and Houston's hostess Karen St. Jean. While dining at the home of a Houston's manager, St. Jean showed him the Spec-Tator group on his home computer. Upon request, St. Jean also furnished her MySpace username and password to another Houston's manager, so he could view the Spec-Tator. St. Jean testified that the sole reason she permitted management to access the MySpace group was because she feared that if she had not she "would have gotten in some sort of trouble." Houston's managers testified that they found the Spec-Tator posts "offensive" and inconsistent with the restaurant's four core values: professionalism, positive mental attitude, aim-to-please approach, and teamwork. Houston's terminated Pietrylo and another employee shortly after management discovered the MySpace group. Both asserted several claims against Houston's, including for its alleged violation of the SCA.[11]

Houston's moved for summary judgment based on the same theory as Hawaiian in *Konop*. Houston's argued that the SCA exempted it from liability because St. Jean was an authorized "user" who permitted management to view the Spec-Tator webpage. The court held, however, that a genuine issue of material fact existed regarding whether or not St. Jean had "authorized" management to view the MySpace group. The determinative factual issue for the court was whether or not St. Jean gave "voluntary" consent to management to access and view the Spec-Tator.[12] The case later went to trial the jury determined there was a violation of the SCA and awarded plaintiffs $2,500 and $903 in compensatory damages. The jury also found that the employer's conduct was malicious and awarded punitive damages to the plaintiffs.[13]

iii. Complying with the SCA

Employers and their attorneys can draw several lessons from the *Konop* and *Pietrylo* decisions. Most importantly, employers should be extremely cautious about independently seeking access to any web-based communications of their employees that are password-protected or subject to privacy controls. From a doctrinal perspective, *Konop* teaches that employers must obtain consent from an actual user of the employee's communication, and *Pietrylo* teaches that that consent must be voluntary. But on a deeper level, these decisions suggest that courts are highly skeptical of an employer's claims to have obtained authorization to view an employee's personal, password-protected webpage. Both the *Konop* and *Pietrylo* courts stretched their reasoning to allow the employees to proceed with their SCA claims.[14]

---

[10] *Pietrylo*, 2008 WL 6085437 at *1–2.
[11] *Id.*
[12] *Id.* at *3–4.
[13] *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 at *1 (D. N.J. Sept. 25, 2009).
[14] It is certainly not an obvious conclusion that an individual who is one of a limited number of eligible users of a website, but who may not have actually visited the website, is not a "user" for purposes of the act. Nor is it transparent that a voluntariness requirement should be read into the SCA's "authorization" exemption for third parties. And that is not all. *Pietrylo* insinuates that another court might even go so far as to rule *as a matter of law* that an employee cannot authorize his or her supervisor to view such a website. The *Pietrylo* court did not expressly reject plaintiff's argument that "in an employer-employee relationship, there is a threat inherent in any demand made on an employee by management." *Id.* at *4.

But employers should be equally attuned to what *Konop* and *Pietrylo* do *not* say. Neither case involved a publicly accessible webpage, a private webpage to which the employee invited his supervisor, or even a private webpage to which the supervisor merely requested access. Accordingly, these cases should not cause alarm for employers who use internet search engines to find publicly available information about their employees. Nor should supervisors fear SCA liability for sending "friend" requests to their subordinates on social networking sites.[15]

b. State Tort Law

Employers that wish to monitor their employees' electronic communications must also take care lest they subject themselves to tort liability. In *Pietrylo*, for instance, the terminated employee brought tort claims against Houston's for invasion of privacy and wrongful termination in violation of his right to privacy.[16] Nevertheless, because the elements of the invasion of privacy tort are exceedingly difficult to meet,[17] employers should have little to fear so long as they do not take extreme and unnecessary measures to pry into the private communications of their employees.

c. The Fourth Amendment

Public employers may also be liable for improper investigations under 42 U.S.C. section 1983 and the Fourth Amendment. The Supreme Court's recent ruling in *City of Ontario v. Quon*[18] provides the most current guidance for public employer searches. It also contains dicta that may provide some clues about how the Supreme Court will decide future cases involving the application of the Fourth Amendment to public employer searches of electronic communications.

Quon principally involved a city police officer's section 1983 action against his employer for violation of his Fourth Amendment rights. Respondent Jeff Quon alleged that the Ontario Police Department ("OPD") unconstitutionally seized and reviewed private text messages that he had

---

[15] Employers should be aware, however, that legal issues could potentially surface down the road. For instance, "employers are generally prohibited from engaging in surveillance of union organizing activities." *Konop*, 302 F.3d at 884 (citing *Cal. Acrylic Indus. v. NLRB*, 150 F.3d 1095, 1099–1100 (9th Cir. 1998)). Supervisors should also consider etiquette and interpersonal dynamics before "friending" their subordinates. *See* Jared Sandberg, *OMG – My Boss Wants to 'Friend' Me On My Online Profile*, WALL ST. J., July 10, 2007, *available at* http://online.wsj.com/article/SB118401324654861242.html.

[16] *Pietrylo*, 2008 WL 6085437 at *1.

[17] *See* Sarah DiLuzio, Comment, *Workplace E-Mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741, 749–51 (2000) (observing that the "intrusion of seclusion" tort requires an employee to meet the high bar of establishing, among other elements, a reasonable expectation of privacy and that the employer's conduct was "highly offensive to the average reasonable person"); *see also* Corey A. Ciocchetti, Comment, *Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 0026 (observing that the elements of invasion of privacy claims are very difficult to meet and concluding, accordingly, that "employers acting reasonably under the circumstances have little to fear from these common law causes of action").

[18] *Quon*, 2010 WL 2400087 (U.S. June 17, 2010).

sent from his OPD pager. The Court held unanimously that OPD's investigation was permissible.[19]

Although the Court's holding in *Quon* was exceedingly narrow,[20] the case contains dicta that is highly instructive for employers. Specifically, the Court lent credence to, while explicitly declining to adopt, the framework set fourth by a four-Justice plurality in *O'Connor v. Ortega*.[21] Public employers should therefore continue to assess the constitutionality of their workplace monitoring procedures under that standard. Thus, employers must determine: (1) whether the employee has a reasonable expectation of privacy given the "operational realities of the workplace"; and (2) if so, whether the employer's search was reasonable under all the circumstances — particularly with regard to its objectives and scope.[22]

The Court in *Quon* also gave indication that it generally prefers an incremental, even *ad hoc*, approach to defining the reach of the Fourth Amendment with respect to emerging technology. "The judiciary risks error," opined the Court, "by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." [23] Nevertheless, the Court did offer one bit of concrete guidance that both public and private employers should find helpful. The Court signaled that in the future it will likely give considerable deference to employer policies, which it declared "will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."[24]

Accordingly, employers should review and update their electronic communications policies. These policies should be clearly written and should specify all applicable forms of communication that could be subject to search.

2. Ethical Considerations for Employer Attorneys

In addition to knowing the legal requirements with which employers must comply when conducting informal investigations, attorneys that represent employers must be careful to follow certain professional ethics rules.

a. No Deception Means . . . No Deception

Attorneys need to be aware that they can commit ethics violations if they use deception to attempt to obtain access to the electronic communications of an opponent or third party. Rule 4.1(a) of the ABA Model Rules of Professional Conduct prohibits a lawyer from "[i]n the course of representing a client . . . knowingly . . . mak[ing] a false statement of material fact or

---

[19] *Id.* at *4, 14.
[20] *Quon* held, under settled principles of law, that OPD's search was "reasonable." Accordingly, the Court made clear that its discussion of Quon's reasonable expectations is merely speculation and non-binding on lower courts. *Id.* at *8–11.
[21] 480 U.S. 709 (1987).
[22] *Id.* at 718, 725–26.
[23] *See Quon*, 2010 WL 2400087 at *9 (Justice Scalia did not join this part of the Court's opinion).
[24] *Id.*

law to a third person." Rule 8.4(c) makes it "professional misconduct" to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Last year, the Philadelphia Bar Association's Professional Guidance Committee ("the Committee") determined in an advisory opinion that an attorney would violate Pennsylvania's version of these rules if he asked a third party, who would not disclose his affiliation with the attorney, to send "friend" requests to an opposing party's witness on Facebook and MySpace.[25] The attorney hoped to view the witness's profiles to find information to impeach her deposition testimony at trial. The attorney stated that the witness tended to grant access to anyone who asks, but was unsure if she would allow him access if he asked her directly.[26]

The Committee's conclusion in this inquiry is intuitive, and seemingly a simple and straightforward application of Pennsylvania's professional ethics rules. Nevertheless, the opinion contains some additional helpful guidance for attorneys who wish to obtain information from a nonpublic profile on a social networking website. For instance, the opinion does not address the propriety of the lawyer directly requesting access to the witness's profile. Rather, the Committee strongly suggests that such an approach would be entirely ethical.[27] The Committee also helpfully identifies disagreement among states regarding whether or not a lawyer is absolutely barred from using deception in all circumstances. Some states, such as Colorado, adhere to an absolutist interpretation of the no-deception bar, while others, such as Oregon, permit deception in a very limited set of circumstances.[28] Attorneys should consult the specifics of their state's rules before engaging in borderline conduct, but a good (and safe) rule of thumb is simply to eschew deception at all times.

b. Respecting the Venerable Privilege: What To Do With Employee-Attorney Communications Sent Via Employer Computers

Attorneys for employers also need to have a game plan for how to handle lawyer-client communications that turn up in an investigation of an employee's on-the-job internet usage. Even if the employer's search is perfectly lawful, an employee's communications with his or her attorney may still be privileged. The question is whether an employee waives the privilege by communicating with his or her attorney on the employer's computers, internet server, or e-mail system. The law is murky on this question.

---

[25] Philadelphia Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (March 2009).

[26] *Id.*

[27] *Id.* ("The fact that the inquirer asserts he does not know if the witness would permit access if he simply asked in forthright fashion does not remove the deception. The inquirer could test that by simply asking the witness forthrightly for access.") It could at least be argued that the Committee's inclusion of the adverb "forthrightly" might require a lawyer to disclose his professional relation to the witness when seeking access to her nonpublic profiles. Otherwise, the witness might not remember why she recognizes the attorney, and grant access without full knowledge of the relevant facts. Such "permission" would be based on a milder, but no less real, form of deception than the inquiring attorney's proposed course of conduct.

[28] Oregon permits an attorney to engage in "covert activity" to investigate unlawful activity if the lawyer believes in good faith that such activity "has taken place, is taking place or will take place in the foreseeable future." *See id.*

Nevertheless, a few broad generalizations can be made. First and foremost, it is risky given the current state of the law for an employer to read attorney-client communications sent to or from an employee's personal, web-based e-mail account. Several courts have found that an employee waived the privilege when the attorney-client emails were sent to or from the employee's *work* account,[29] but no recent decisions have held the privilege to be waived when the employee used his or her *personal* e-mail account on the employer's computer.[30] Second, employers fare much better in these cases when they maintain, enforce and regularly remind employees about their electronic communications policies. To shield an employer from liability, a well-crafted policy should state that employees: (1) should not use the employer's computers or servers for personal use; (2) should have no expectation of privacy or confidentiality in their usage of the employer's systems; and (3) should be on notice that the employer retains and exercises the right to monitor its employees' usage of such systems. The policy should also define any potentially vague terms, such as "computers," "servers," and "systems."

Employer attorneys should be highly sensitive towards an employee's attorney-client communications. In *Stengart v. Loving Care Agency, Inc.*,[31] an employee sent emails from her private, password protected email account, on a computer owned by her employer. The employer retrieved the emails from the computer following the employee's termination, and the emails were subsequently read by the employer's counsel in the course of defending a sexual harassment action. The New Jersey Supreme Court found that an employer's counsel violated the state's Rule of Professional Conduct 4.4(b) for reviewing attorney-client e-mails that the employer recovered from its former employee's computer, and for waiting months before contacting the employee or the court about the e-mails.[32] The court remanded the case for the trial court to determine if the attorney's conduct warranted sanctions or disqualification from the case.[33] If an employer's attorney discovers an employee's potentially privileged e-mails, he or she should check the rules of the jurisdiction in which he or she practices to determine if there is any direct authority on point and proceed with caution. If litigation is ongoing or imminent, the best practice may be to refrain from reading the e-mails, notify the employee, and seek a court order permitting the employer to review the e-mails.

---

[29] *See*, *e.g.*, *Alamar Ranch, LLC v. County of Boise*, 2009 WL 3669741 (D. Idaho Nov. 2, 2009) (employee waived privilege by communicating with her attorney over her work e-mail account when employer's policy clearly notified employees of its right to monitor e-mails); *Scott v. Beth Israel Medical Center, Inc.*, 17 Misc.3d 934, 847 N.Y.S.2d 436 (N.Y. Sup. Ct. 2007) (same); *Kaufman v. SunGuard Inv. System*, 2006 WL 1307882 (D. N.J. May 10, 2006) (same).

[30] *See*, *e.g.*, *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010) (employee did not waive privilege when she communicated with her attorney from a personal, password-protected, web-based e-mail account despite accessing the e-mails from her work computer and despite the employer's electronic communications policy that arguably notified employees of its right to monitor all employee computer activity); *Curto v. Medical World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (no waiver of the privilege where employee e-mailed her attorney from her personal, web-based e-mail account via her employer's laptop notwithstanding computer usage policy that would have permitted access to the employer).

[31] 990 A.2d 650 (N.J. 2010).

[32] *Id.* at 665. Under Model Rule 4.4(b), after which the parallel New Jersey rule is patterned, "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."

[33] 990 A.2d at 665–66.

3. Conclusion

Employers should pay particular attention to their potential liability under the Stored Communications Act. As a general practice, employers should respect the privacy controls that employees place on their private websites. Employers should also refrain from pressuring employees to surrender login information to their password-protected websites.

In addition, employers should review, update, and periodically remind employees about their electronic communications policies. Because the employee's reasonable expectations are the touchstone of much of employment privacy law, employment policies will continue to play an important role in shaping this area of the law, as the Supreme Court acknowledged in its recent *Quon* decision.

Finally, employer attorneys need to be informed about how ethical rules apply to electronic communications. One important rule of thumb is that attorneys should never conceal their identity in seeking access to webpages with privacy controls (most likely profiles on social networking websites such as Facebook or LinkedIn). Such conduct violates the ethical rules against deception. Employer attorneys should also be cautious about reading an employee's e-mails or other electronic communications with his or her attorney if they turn up in a workplace computer search. Attorneys are ethically bound to notify the employee of such communications if the employee has not waived the attorney-client privilege.