New Jersey Law Journal

VOL. CXCVI – NO. 7 - INDEX 422 MAY 18, 2009 An incisivemedia publication

COMPLEX LITIGATION & *E-Discovery*

The Company Fink Goes Online: Employer Surveillance of Employee Social Networking Groups

By James M. Hirschhorn

The popular social networking sites, My Space and Facebook, were just getting started in 2002 and 2003. They and other less well-known online discussion forums allow like-minded people to form groups to discuss questions of common concern and to limit the membership to trusted individuals. One irresistible subject of common concern is how things are going on the job. Thanks to online social networking sites, gripes, complaints and mockery that used to be uttered around the coffee pot, in the lunch room and over beers after work are now exchanged electronically.

While the Internet is new, some things never change. There have always been bosses who don't like what they consider malcontents and are willing to fire them. There have always been co-workers who talk indiscreetly, and others who carry tales for a whole range of reasons. But social networking sites now create an indisputable record of ephemeral remarks that used to disappear deniably. If an employer gets access to an online discussion group of critical employees who feel safe using their real names, those employees can find themselves facing disciplinary action or discharge. Depending on how the employer has gotten access, however, it may be in violation of federal and state law protecting the privacy of stored electronic communications.

That's what happened in *Pietrylo v. Hillstone Restaurant Group*, a case now pending in the U.S. District Court for the District of New Jersey. A restaurant worker started an invitation-only MySpace discussion group for selected co-workers "to vent about any BS we deal with at work without any outside eyes spying in on us." Unfortunately, one of the group members showed the group to a manager on the manager's home computer while dining at his home. The manager asked for the employee's username and password, and she provided it, knowing that once she turned it over all managers would have access to the site. Managers used the employee's username and password to lurk in the group. Eventually, the employer terminated the organizer of the group and one other group member, who were both at-will employees. They sued, alleging violation of the federal Stored Communications Act (SCA), 18 U.S.C. Section 2701(a), and its New Jersey counterpart, N.J.S.A. 2A:156-27, as well as wrongful discharge in violation of public policy and common-law invasion of privacy. The employer moved for summary judgment, arguing that its access to the MySpace page was "authorized by a user of that service with respect to a communication of or intended for that user," i.e., with the employee's consent, as permitted by 18 U.S.C. Section 2701(c).

The district court dismissed the wrongful discharge claim, holding that no public policy restricted an employer from discharging at-will employees overheard complaining to each other about working conditions, and specifically rejecting the employees' claim that the First Amendment limited a private employer's right to discharge. However, the court denied summary judgment on the SCA and invasion-of-privacy claims, holding that the consent would be invalid if coerced, and that there is a triable issue of fact whether the employee was coerced to provide the username and password by which the company accessed the site.

The key to the district court's analysis in *Pietrylo* is consent. Under Section 2701(c), as under similar language in the federal Wiretap Act, 18 U.S.C. Section 2511(2)(d), a party to an electronic communication may record, access and disclose it voluntarily, even if that disclosure betrays the trust of another party to the communication. The court read the statutory consent exception into plaintiffs' common-law invasion of privacy claims, holding that there would be an actionable intrusion into private matters if, but only

Hirschhorn is a member of Sills Cummis & Gross in Newark. The views and opinions expressed in this article are those of the author and do not necessarily reflect those of the firm.

if, the employer coerced the one employee to provide the means of access to the site. Under this analysis, an employer who recruits a truly voluntary informer to provide access to an employee Web site has not violated the Stored Communications Act. However, one court has held that the consent must be provided by an actual user, i.e., an employee who has not merely been invited into the group but who has joined and made use of the Web site. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002)

While the district court analogized the authorized access exception to the Stored Communications Act to the consent exception to the Wiretap Act, the exception in the Stored Communications Act is broader. Under Section 2511(2)(d), a private party violates the Wiretap Act if it intercepts an electronic communication, even with consent, "for the purpose of committing any criminal or tortious act" under federal or state law. The tortious act must be independent of the interception and recording itself. *See Sussman v. American Broadcasting Companies, Inc.*, 186 F.3d 1200 (9th Cir. 1998). However, Section 2701(c) does not contain a similar restriction. Accordingly, it has been held that a party with authorized access to a stored communication did not violate the Stored Communications Act by disclosing confidential stored information for an unauthorized purpose. See, e.g., *Intl. Assn. of Machinists v. Werner-Matsuda*, 390 F. Supp. 2d 479 (D. Md. 2005). If an employer has gained access to an employee site by valid consent, therefore, it would follow that use of the information to take adverse action against employees would not violate the Stored Communications Act, even if it did violate federal or state labor law.

The district court's analysis in *Pietrylo* also leaves open the question of what constitutes voluntary consent. This issue has been extensively litigated under the Wiretap Act provision, 18 U.S.C. § 2511(2)(c), which allows law enforcement officers to intercept a conversation with the consent of a party. Consent must be voluntary and uncoerced, but the threshold of voluntariness is low. Frequently, law enforcement will catch one violator and turn him against others, obtaining consent by the promise of leniency or immunity from prosecution in return for cooperation. That kind of pressure, it has been often held, does not invalidate the informer's consent as long as no express threat of prosecution has been made. For example, in *U.S. v. Antoon*, 933 F.2d 200 (3d Cir. 1990), the Court of Appeals held that an individual who knew that he could be prosecuted for drug offenses, and felt threatened by the situation, had nevertheless voluntarily consented to wear a wire. While it may be true that he felt trapped (although he never used that word himself), the court concluded, "there is no indication that [the informant] did anything but knowingly and intentionally choose between two unpleasant alternatives." *Antoon* relied on a line of prior decisions holding that consent was voluntary where the individual expected to benefit from cooperation.

Pietrylo presents the same kind of ambiguities as *Antoon*. The employee who turned over her password testified at her deposition that although no one told her that she would be fired or ordered her to turn over the password, she had the "overwhelming feeling" that she could lose her job if she didn't cooperate. By holding that this testimony posed a triable issue of fact as to voluntariness, the district court reserved decision as to whether the law enforcement standards of voluntariness under the Wiretap Act would apply here. The issue will be revisited if the case goes to trial and perhaps on appeal.

One issue that *Pietrylo* did not raise is whether the employer would have implied consent to access the Web site if the employees had accessed it through work computers. Section 2701(c)(1) of the SCA allows the provider of an electronic communications service to access communications stored on that service. One court has held that this authorized a police department to scrutinize officers' personal communications on the department's instant messaging service. *Bohach v. City of Reno*, 923 F. Supp. 1232 (D. Nev. 1996). This result is consistent with New Jersey law that an employer may monitor employees' e-mail and Internet access in the workplace if it has a clearly enunciated policy to that effect. *See Doe v. XYC Corp.*, 887 A.2d 1156 (N.J. App. 2005); *accord State v. M.A.*, 954 A.2d 503 (N.J. App. 2008). Whatever privacy rights the SCA confers on otherwise private discussion groups appear to be limited if employees use the workplace computer system as their channel of communication.

The Stored Communications Act and Wiretap Act do not mark the limit of potential employer liability, however. Such employees Web sites may be go beyond mere informal griping and become instruments of self-organization or union activity. At that point, the long-standing prohibitions of the National Labor Relations Act against coercive surveillance by the employer would come into play. See, e.g., *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), in which the Court of Appeals held that employer access to a dissident union faction's Web site raised a triable fact issue of unlawful coercion under the Railway Labor Act.

In conclusion, there are limited but significant risks if an employer tries to monitor online employee discussion groups through a cooperating employee. At the very least, the employer must take care that it obtains access through the noncoerced consent of an actual authorized member of the group. Even access authorized under the Stored Communications Act may independently violate federal labor law governing the surveillance of employee self-organization or union activity. ■