Onboarding of Social Media

Establishing Policies and Procedures:
Are You Asking Employees for Facebook Passwords

Katherine D. Hoke

Part 2 of 3

There are several potential risks in asking employees for their passwords to their personal social media pages. Companies can open themselves up to claims of unlawful discrimination or even unlawful activity.

SHIELDS LEGAL GROUP

972-788-2040
shieldslegalgroup.com
16301 Quorum Drive, Suite 250B Addison, TX 75001

COMPANIES CAUGHT IN THE LINE OF FIRE

Recently, a plethora of articles have overwhelmed the Internet

on whether employers are violating privacy as well as other laws, by demanding Facebook and e-mail passwords from their employees or job applicants, and then using those passwords to peruse employee postings. While public outrage is high, this practice is continuing with seeming impunity. Recently, it was reported that a Michigan teacher's aide was terminated for refusing a school administrator's request for her Facebook password after she allegedly posted a photo that prompted a parent's complaint to the school district.

Facebook's Stand

On March 23, 2012, Facebook itself took a stand against this practice, threatening possible legal action. Erin Egan, Facebook's Chief Privacy Officer, posted the following,

> "In recent months, we've seen a distressing increase in reports of employers … seeking to gain inappropriate access to people's Facebook profiles … If you are a Facebook user, you should never have to share your password … Facebook takes your privacy seriously. We'll take action to protect the privacy and security of our users, whether by engaging policymakers or, where appropriate, by initiating legal action …"

THE HOUSTON'S RESTAURANT CASE

Legislative Action

Now, legislators are decrying the practice and working to pass a bill that will ban the practice. Just days after Facebook posted its public statement, U.S. Senators Charles E. Schumer (NY) and Richard Blumenthal (CT) issued letters to the Justice Department and EEOC complaining about the practice, and demanding that the Justice Department investigate whether requesting and using employees' social network passwords violates the Stored Communications Act (18 U.S.C. § 2701, et seq.) or the Computer Fraud and Abuse Act (18 U.S.C. § 1030).

Legislators are now decrying the practice.

Few courts have considered the matter to date. In 2009, a New Jersey federal court declined to grant a new trial to a restaurant employer found by a jury to have violated the Stored Communications Act. *Pietrylo v. Hillstone Restaurant* Group, 2009 WL 3128420 (D. N.J. 2009) (not published). The central issue was whether the restaurant employer's access to a chat group on the social networking website MySpace was "authorized," and therefore not in violation of the statute. The evidence showed that the employee voluntarily gave her restaurant manager her MySpace.com password, and that the restaurant manager and other managers used that password on multiple occasions to gain access to postings in the chat group which were highly critical of managers and workplace conditions. The court found that there was sufficient evidence to uphold the jury's finding that the access was not authorized because the employee testified that she gave the password under duress:

The employee voluntarily gave her restaurant manager her password.

> "She felt she had to give her password to [the manager] because she worked at [the restaurant for the manager]." She also testified that she "felt that [she] probably would have gotten in trouble," if she did not furnish the password.

THE HAWAIIAN AIRLINES CASE

In another case, a pilot filed suit against his employer for *inter alia*, violations of the Stored Communications Act stemming from the employer's use of a co-worker's log-in information to gain access to the pilot's secure website, which contained bulletins critical of his airline employer. *Konop v. Hawaiian Airlines*, 302 F. 2d 868 (9th Cir. 2002). The evidence showed that two fellow pilots consented to furnishing the airline's management with their log-in information, and that management used the log-in information to access the pilot's secure website several times. The district court granted the airline summary judgment on a number of claims, including violations of the federal Wiretap Act and the Stored Communications Act.

Two fellow pilots consented to furnishing their log-in information.

On appeal, the Ninth Circuit affirmed summary judgment on the Wiretap Act claim, but reversed summary judgment on the claim for violation of the Stored Communications Act. The appellate court found that the airline had not established that it was exempt from liability under the Act on the basis that its third party access to the secure website was authorized by a "user of the service." In that regard, the appellate court held that there was no evidence in the record showing that the two pilots who had furnished their log-in information to the airline were, in fact, "users" of the pilot's secure website.

The airline had not established that it was exempt from liability.

YOUR BUSINESS IMPACT

The following information is provided as a general guideline and should not be taken as legal advice or counsel.

While the courts continue to grapple with whether employer liability exists under the Stored Communications Act or Computer Fraud and Abuse Act, employers should be aware of other potential risks arising from the practice as well:

- Claims of unlawful discrimination based upon an employee's or applicant's disclosed status on a social networking site (e.g. age, religious beliefs, marital status, health status, pregnancy, sexual orientation, political views, etc.)
- Claims of unlawful discrimination with respect to the employer's implementation of the practice (e.g. only certain classes or types of employees or applicants are asked to furnish their passwords)
- Employer's duties/obligations in the event an employee's or applicant's social networking postings suggest involvement in unlawful activity (e.g. unlawful pornographic material)

BOTTOM LINE

Companies who ask current employees or job applicants to furnish their social network passwords should reconsider this controversial employment practice and evaluate whether the potential liability risks outweigh the benefits.

ABOUT THE AUTHOR

Katherine D. Hoke

Because of Katherine D. Hoke's 24 years of legal experience representing businesses in various litigation matters and disputes, she has the unique talent for understanding the ultimate goals of a business. Rather than simply responding to the typical process of legal procedures, she leads SLG's traditional legal services team as a partner in handling client legal activities. Ms. Hoke counsels clients on matters involving contract disputes, complex commercial and real estate litigation, and creditors' rights and collections.