STAY CURRENT
A Client Alert from Paul Hastings

PAUL HASTINGS

May 2012

Lawmakers Defending Password-Protected Employee Accounts: Employers Need to Proceed Smartly

BY MARK POERIO & BARBARA JOHNSON

"Mortified" is the reported reaction of Robert Collins, a former corrections officer with the Maryland Department of Corrections (DOC), when DOC requested his Facebook username and password about a year ago. After Collins gave that information to a DOC interviewer in connection with its "re-certification" process, the interviewer logged on to his account and reviewed the content, including posts of Collins' family and friends.

The term "mortified" may well describe the reaction of lawmakers, as well, because protective legislation recently passed in Maryland, is pending in at least 10 other states, and just surfaced in the U.S. Congress. Meanwhile, Facebook has warned its users that "you should never have to share your password,"[1] and LinkedIn has been alive with questions such as "*Could employers in the UK demand your Fbook password?*"[2] Worldwide, employers should proceed with caution.

Maryland's New Law

In Maryland, the General Assembly passed the User Name and Password Privacy Protection Act (SB 433/HB 964) (the "Maryland Law") in April 2012. That legislation will take effect October 1st provided Maryland's Governor Martin O'Malley signs it, as expected this month. The Maryland Law prohibits an employer from requesting or requiring "that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service" such as Facebook, LinkedIn, or Twitter.

Specifically, employers doing business in Maryland (including units of state or local government) may not "discharge, discipline, or otherwise penalize" employees for refusing to disclose their personal information for an account accessed through a computer, telephone, or other electronic communications device. Nor may employers make hiring decisions on the basis of such a refusal. Threats of punitive action would also violate the Maryland Law.

Employers in Maryland may nevertheless require that an employee disclose "any user name, password or other means for accessing . . . the employer's internal computer or information systems." Furthermore, the Maryland Law allows an employer to access an employee's personal electronic accounts for the limited purposes of investigating information that the employer received about –

(1) the employee's unauthorized downloading of the employer's proprietary or financial data to the employee's personal website, web-based account, or similar account; or

(2) the employee's personal use of a personal website, web-based account, or similar account for business purposes, provided the employer's investigation is "for the purpose of ensuring compliance with applicable securities or financial law, or regulatory requirements."

The latter authorization appears to reflect a few reported cases in which employers have had to sue former employees in order to obtain access to the account information for the employer's website. Note that the Maryland Law does not allow employers to access password-protected employee accounts for the sole purpose of investigating possible tortious or illegal actions that do not fall into one of the two categories noted above. On the other hand, the Maryland Law does not forbid an employer from asking an employee to privately access personal accounts so that the employer may view activity. Employers should nevertheless be careful to consider the legal and business implications of any such possible conduct.

Other Legislative Efforts

Legislation similar to the Maryland law is currently pending in 10 states, including California, Illinois, Massachusetts, Michigan, New York, South Carolina, and Washington.[3] Most recently, on April 27, 2012, Rep. Eliot Engel (D-N.Y.) and Rep. Jan Schakowsky (D-Ill.). took this effort to the federal level, by introducing "The Social Networking Online Protection Act" in the U.S. House of Representatives. All of these bills essentially reflect the rationale that Rep. Schakowsky set forth for the federal legislation:

> No one should have to worry that their personal account information, including passwords, can be required by an employer or educational institution, and if this legislation is signed into law, no one will face that possibility.[4]

There is likely to be U.S. Senate support for legislation given that a March 25, 2012 press release by Sen. Blumenthal (D-CT) states: "A ban on these practices is necessary to stop unreasonable and unacceptable invasions of privacy. An investigation by the Department of Justice and Equal Employment Opportunity Commission will help remedy ongoing intrusions and coercive practices, while we draft new statutory protections to clarify and strengthen the law. With few exceptions, employers do not have the need or the right to demand access to applicants' private, password-protected information."

Potential Employer Liability?

Although the Maryland Law does not provide expressly for sanctions on misbehaving employers, a New Jersey District Court and the Ninth Circuit Court of Appeals have previously found viable causes of action, under the Stored Communications Act, in cases involving employees who complained of having their secure websites accessed by supervisors to view postings critical of the employer.[5]

Protecting Business Interests

Employers should take note that the Maryland Law and similar proposals generally distinguish between the personal accounts of employees and those connected to the employer's business. If employees are or will be using social media for work-related purposes, employers should be vigilant to position themselves to protect their interests in the employer's website and related social media accounts (together, "***Employer Media***"). For example, a concerned employer should consider –

(1) identifying Employer Media as being affiliated with and owned by the employer;

(2) controlling the password for Employer Media accounts, and changing it when employees depart;

(3) establishing "use policies" to designate which employees have authority to access the Employer Media, and what they may do;

(4) requiring that key employees execute written agreements acknowledging that, for purposes of the 1976 Copyright Act, the content within Employer Media is "work for hire" and owned by the employer, and

(5) addressing, also in written agreements, the obligations of a departing employee both as to Employer Media and other business-oriented contacts (such as those made through LinkedIn).

A recent California case suggests the complexities that litigation about Employer Media may spur. Phonedog, an online company whose business is reviewing mobile, hired Kravitz as an independent contractor to use Twitter @PhoneDogNoah and other social media to discuss mobile products and services. From then until he left in October 2010 he built up a following of 17,000 readers. When he left, reports THE NATIONAL LAW JOURNAL, "the company asked him to stop using the account. But Kravitz continued to use it, changing its handle to #noahkravitz." In July 2011, Phonedog sued him, contending misappropriation of trade secrets, conversion, interference with prospective economic advantage and negligent interference with prospective economic advantage. It is requesting $2.50 for each of the 17,000 followers, framing the entity as a type of "customer list." The court has denied Kravitz's motion to dismiss

Quoting from a recent article: "The problem with the PhoneDog vs Noah Kravitz case is that, while the Twitter account bore the PhoneDog name, and Kravitz's position as editor-in-chief no doubt earned him more exposure, the account was maintained entirely by Kravitz personally."[6] Nevertheless, PhoneDog succeeded in avoiding dismissal of its complaint, with the court noting that resulting economic damages were sufficiently alleged:

> Due to Kravitz's alleged conduct, "there is decreased traffic to [the] website through the Account, which in turn decreases the number of website pageviews and discourages advertisers from paying for ad inventory on PhoneDog's website." FAC ¶ 36. "As a direct and proximate result of Defendant's wrongful acts, PhoneDog has suffered damage to is business by way of lost advertising revenue . . . ." FAC ¶ 38.[7]

Conclusion

Given the legislative groundswell in favor or protecting personal electronic media accounts, employers should tread carefully before taking employment-related actions that involve accessing the password-protected electronic media accounts of employees and job applicants. Nevertheless, as the Maryland Law indicates, employers have a legitimate business interest in preserving their rights to business-related electronic media accounts.[8] The smartest employers will act preemptively to protect their trade secrets and key relationships, yet will be alert to public sensitivities and potential liabilities for pushing beyond the developing boundaries for employer action.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

J. Mark Poerio
1.202.551.1780
markpoerio@paulhastings.com

Barbara L. Johnson
1.202.551.1716
barbarajohnson@paulhastings.com

[1] See "Facebook Firmly States Employers and Schools May Not Access Password Protected Content," Shear on Social Media Law, 3/23/2012.

[2] LinkedIn posting in European Employment Lawyers (4/16/2012), at http://www.linkedin.com/groupItem?view=&gid=2011010&type=member&item=107974680&qid=d699e0b9-4864-463b-9282-26ac2e915b72&trk=group_most_popular-0-b-ttl&goback=%2Egmp_2011010.

[3] See "Employer Access to Social Media Usernames and Passwords," maintained by the National Conference of State Legislatures.

[4] Quoted within "SNOPA bill seeks to keep employers out of private social networks" (Los Angeles Times, 4/30/2012).

[5] See *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 (D.N.J. 2009); *Konop v. Hawaiian Airlines Inc.*, 302 F.3d 868 (9th Cir. 2002).

[6] "

[7] *PhoneDog v. Kravitz,* N.D.CA (1/30/2012), available here.

[8] *See* Poerio & Sherwood, "The Impact of Social Networks on Restrictive Covenants: Why Rapid Change Should Meet Rapid Improvement" (Bloomberg BNA, 2/17/2012).

Stay*Current* is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2012 Paul Hastings LLP.

IRS Circular 230 Disclosure: As required by U.S. Treasury Regulations governing tax practice, you are hereby advised that any written tax advice contained herein or attached was not written or intended to be used (and cannot be used) by any taxpayer for the purpose of avoiding penalties that may be imposed under the U.S. Internal Revenue Code.