

Employment

Communications

Litigation

Social Media, Entertainment
& Technology

Privacy, Data Security
& Information Use

June 11, 2012

Employ Me, Don't Friend Me: Privacy in the Age of Facebook

By James G. Gatto, Julia Judish, Amy L. Pierce and Meighan E. O'Reardon*

With the unprecedented popularity of social media, individuals have increasingly been willing accomplices in undermining their own privacy. Few would have predicted that millions of people would voluntarily log onto the Internet and share detailed private information about themselves, their friends, family and employers. Users of social media have implemented varying privacy safeguards from unrestricted blogs to Facebook posts limited to a customized list of friends. Even those who seek privacy, however, must contend with a growing practice by employers and others of requesting access to password-protected social media accounts. Social media users have lost jobs and educational opportunities as a result of the increased scrutiny of these private postings. Maryland recently became the first state to enact a law prohibiting this practice; several other states and the U.S. Senate and House have similar legislation under review.

The inherent risks of posting personal information on the Internet have been recognized at the highest level of our government: in an address to schools in September 2009, President Obama warned students to "be careful what you post on Facebook. Whatever you do, it will be pulled up again later somewhere in your life." It is too late for many to heed this warning, and many social media users are reluctant to limit their self-expression. To protect these individuals' privacy, several states and the U.S. Congress are considering legislative action that would prohibit employers and educational institutions from requiring access to password-protected content on social media sites.

From the viewpoint of employers and educational institutions, access to the social media websites of applicants, employees, and students may be regarded as part of their due diligence in making selection decisions. Prospective employers may use social media sites to verify claims in resumés and job applications. (The "Info" tab on Facebook, for example, can reveal a wealth of information about employment and educational history.) Many may also believe that they can assess whether a prospective employee is likely to be reliable based on whether the applicant's posted photos depict frequent drunken partying or other

*The authors thank summer associate Nicole Mortorano for her assistance on this alert.

conduct that may be reflective of poor judgment. Similarly, employers may wish to check up on whether the status updates and other postings of their employees reveal that the employee is bad-mouthing the employer or taking an unapproved beach vacation on a day that the employee called in sick.

Accessing social media sites, however, also comes with potential legal pitfalls. If, for example, an employer learns about an applicant's pregnancy, disability or religious beliefs through trolling the Internet, that may set the employer up for a potential discrimination lawsuit if the employer then rejects the applicant. In addition, because not all individuals post online with equal abandon, an employer may treat applicants or employees inconsistently, based on uneven access to information – or may be misled by an individual's selective posting of photographs and information. The hallmark of most employment laws is that employers must limit employment selection decisions to legitimate job-related factors. By opening the door to a flood of potentially extraneous information, employers may find it tempting to stray from that principle.

Regardless of the benefits or risks to employers of accessing individuals' social media sites, such access violates the widely held belief that employees and students are entitled to privacy in their personal lives, as long as their personal conduct does not adversely affect their job or school performance. Opponents of employer access to social media sites compare such investigations to the intrusiveness of an employer demanding entry into an applicant's or employee's house to look through photographs and read the individual's personal letters. Many states and the U.S. Congress appear to agree, recently introducing bills prohibiting employers, and in some cases post-secondary educational institutions, from requesting or requiring current or prospective employees or students to disclose the usernames and passwords of their social media accounts, or to otherwise provide them with access to these accounts. At least one state is considering a bill to prohibit employers from asking if a current or prospective employee has any social media accounts. Many of these bills, if enacted, would become effective immediately. As of the date of this Alert, states considering social media privacy legislation include California, Delaware, Illinois, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, South Carolina and Washington. The attached chart includes more detail about the Maryland law and other pending legislation.

The current legislation highlights one of the many emerging issues that employers and educational institutions face as a result of the rapidly growing use and popularity of social media. Employers and educational institutions should consider avoiding or discontinuing the practice of requesting access to password-protected social networking sites of their applicants, employees, and students, especially in locations where social media privacy laws have been enacted or where such legislation is pending. While a review of publicly available information would not violate these privacy laws, employers should remember that use of any third-party to conduct background checks triggers the authorization and disclosure requirements of the federal Fair Credit Reporting Act and its state law counterparts. All types of entities should ensure that they develop and frequently update comprehensive social media policies and ensure employees' compliance with those policies.

If you have questions please contact the Pillsbury attorney with whom you regularly work, or the authors:

James G. Gatto (bio)
+1.703.770.7754
james.gatto@pillsburylaw.com

Julia E. Judish (bio)
+1.202.663.9266
julia.judish@pillsburylaw.com

Amy L. Pierce (bio)
+1.916.329.4765
amy.pierce@pillsburylaw.com

Meighan E. O'Reardon (bio)
+1.202.663.8377
meighan.oreardon@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.
© 2012 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.

State and Federal Social Media Bills (as of June 4, 2012)

State	Bill No.	Act, Statutory Reference	Signed Into Law	Proposed or Actual Effective Date	Applies To ¹		Prohibits ²		
					Employers	Educational Institutions ⁵	Confirmation of Social Media Account(s) ⁶	Username(s)/ Password(s)	Access to Social Media Account(s)
					Requesting ³ or Requiring ⁴				
CA	SB 1349	Social Media Privacy Act, Cal. Ed. Code § 99120, <i>et seq.</i> , & Lab. Code § 980, <i>et seq.</i>				✓	✓	✓	✓
CA	AB 1844	Lab. Code § 980, <i>et seq.</i>				✓		✓	
DE	HB 308	Workplace Privacy Act, Del. Code tit. 19, § 710				✓		✓	✓
IL	HB 3782	Right to Privacy in the Workplace Act, 820 ILCS § 55/10				✓		✓	✓
MA	Dkt. No. 04323	Mass. Gen. Laws ch. 149, § 189				✓		✓	✓
MD	SB 433, HB 964	Md. Code, Lab. & Empl. § 3-712	05/02/12	10/01/12		✓		✓	✓
MI	HB 5523	Social Network Account Privacy Act				✓	✓	✓	✓
MN	HF 2963 HF 2982 SF 2565	Minn. Stat. § 181.53				✓		✓*	✓*
MO	HB 2060	Mo. Rev. Stat. § 285.600				✓		✓	✓
NJ	AB 2878					✓	✓	✓*	✓*
NY	SB 6938	N.Y. Lab. Law § 215-d				✓		✓*	✓*
OH	SB 351	OH Rev. Code § 4112.02, <i>et seq.</i>				✓		✓	✓
SC	HB 5105	S.C. Code § 41-1-187				✓		✓	✓
WA	SB 6637	Wash. Rev. Code § 49.44				✓		✓*	✓*
Fed Law	HR 5050	Social Networking Online Protection Act				✓	✓	✓	✓
Fed Law	HR 5684	Password Protection Act of 2012, 18 U.S.C. § 1030				✓		✓	✓
Fed Law	SB 3074	Password Protection Act of 2012, 18 U.S.C. § 1030				✓		✓	✓

¹ Most of the bills govern current and prospective employees and/or students.

² Some states' bills permit employers to bar employees from accessing social networking sites during work hours. See, e.g., DE HB 308. Others permit employers to *request*, but not *require*, access to social media accounts in connection with formal investigations.

³ California SB 1349 prohibits requiring or "formally request[ing] in writing" a social media account username and account password.

⁴ Most of the bills expressly prohibit requiring and requesting the current or prospective employee or student to provide the employer or institution with social media account information. A ✓* indicates that the bill only expressly prohibits requiring this information.

⁵ Each states' bill that regulates educational institutions refers to the particular institution(s) intended to be governed by the new law.

⁶ Several states define terms, including the term social media account.