Social media privacy statutes: Necessary protection, harmless posturing, or something else entirely?

Lois Yurow

July 2, 2015

Abstract

Twenty-two states and Guam have statutes that make it unlawful for a party with power (usually an employer or a school) to demand social media log-in credentials from an individual with less power (an employee, job applicant, student, or student applicant). Social media privacy legislation is pending in eight more states. There is no directly comparable federal statute, but there have been at least seven failed attempts to enact such legislation and one bill is pending.

Although the sentiment these statutes express—that we usually are entitled to keep our private social media activity private—is laudable, it wasn't necessary to enshrine that sentiment in legislation. First, the notion was not under serious attack. There have been instances where people—mostly applicants for security-oriented jobs—were asked for their user names and passwords, but the practice is not as common as the steady stream of legislation would suggest. Second, it is likely the federal Stored Communications Act imposes adequate restraints on overreaching employers and schools. Third, and perhaps most important, there are plenty of practical reasons, such as the risk of a discrimination action or a public relations backlash, that employers and schools should be wary of prying into employee or student social media accounts.

State social media privacy statutes impose restrictions that are inconsistent from state to state, and they are superfluous as a deterrent. Accordingly, these statutes are neither necessary protection nor harmless posturing.

Introduction

When almost half of the country's legislatures decide in a span of three years to pass a law banning a particular activity, one might expect the prohibited conduct is either rampant or extraordinarily dangerous. On the contrary, although twenty-two states and Guam have statutes that protect one or more classes of people—generally employees, job applicants, students, and prospective students—from demands, or even requests, for their social media log-in credentials, it is possible these laws are a reaction to a handful of widely publicized cases of employer (or school) overreach (Meyer, 2015). Indeed, even without these laws, there are plenty of reasons for careful employers and schools to avoid delving into an employee's or student's social media accounts (Segal, 2014). That is not to diminish the policy these statutes represent—just to point out that they may be largely irrelevant (Jackson, 2014). That is probably a good thing. If employers with multi-state operations really were looking to social media privacy statutes to guide their conduct, they would find a patchwork of restrictions (Dipietro, 2015; Davis, 2014) with no apparent reason for the state-by-state variations.

This paper has five parts. I look at the state social media privacy statutes currently in effect, highlighting their commonalities and differences; review efforts at the federal level to pass a similar law, or to mold existing law to fit password demands; consider the underlying reasons so many state statutes have been enacted so quickly; explain why employers and schools should be wary of looking at social media accounts, even in states where there is no social media privacy statute; and conclude that social media privacy statutes are neither necessary nor harmless.

State laws regulating demands for social media log-in credentials

Maryland was the first state to enact a social media privacy statute, in 2012, and Connecticut is the most recent, with a statute that goes into effect on October 1. Eight additional states have

statutes pending, and legislatures in two states have ordered studies of social media and privacy in employment and education contexts. The current statutes are discussed below, and summarized in Appendix I.

Statutes relating to employment

All of the social media privacy statutes follow similar patterns, but each state has opted to include different restrictions and exceptions.

Scope. Rhode Island's statute (Employee Social Media Privacy, 2014) has the typical scope. The Employee Social Media Privacy law (2014) applies to any employer, including the state and its agencies, and protects both current employees and job applicants with regard to their "social media accounts." For purposes of the statute, a social media account includes "electronic content [such as] videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online service or accounts, or internet website profiles." There are several variations on this scope. For example, the Illinois statute expressly excludes email from the definition of "social networking website" (820 Ill. Comp. Stat. Ann. 55/10); the Wisconsin statute also applies to landlords (Wis. Stat. § 995.55); and the statutes in Colorado (Col. Rev. Stat. 8-2-127, 2014), New Jersey (N.J. Stat. § 34:6B-5 et. seq., 2013), and New Mexico (N.M. Stat. § 50-4-34, 2013) do not apply to law enforcement and corrections agencies. In addition, the statute in New Mexico (N.M. Stat. § 50-4-34, 2013) only protects job applicants, not current employees.

Restrictions. Rhode Island's Employee Social Media Privacy law (2014) also incorporates the most common restrictions. Specifically, Rhode Island employers may not:

1. "require, coerce, or request" disclosure of social media log-in credentials from an employee or applicant;

2. "require, coerce, or request" that an employee or applicant access a social media account in the employer's presence (known as "shoulder surfing");
3. "require or coerce" an employee or applicant to disclose the contents of a social media account;
4. "compel" an employee or applicant to add a representative of the employer as a social media connection; or
5. "cause" an employee or applicant to adjust privacy settings to make a social media account more accessible.

As shown in Appendix I, every state statute includes the first restriction set forth above; most also include one or two others. Oregon is an outlier. A bill that goes into effect on January 1 amends Oregon's current statute (which includes restrictions numbered 1, 2, and 5 above) to provide that employers also cannot require employees or applicants to establish personal (as opposed to business) social media accounts or to permit the employer to advertise on their personal social media accounts (Oregon State Legislature, 2015).

To buttress these restrictions, most states make it unlawful for an employer that presumably has made a prohibited request to take disciplinary action if the request is refused. For example, in Rhode Island, an employer may not "[d]ischarge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize" an employee who will not cooperate with the employer's desire to access a social media account, and may not "[f]ail or refuse to hire any applicant" under the same circumstances (Employee Social Media Privacy, 2014). Illinois (820 Ill. Comp. Stat. Ann. 55/10), New Mexico (N.M. Stat. § 50-4-34, 2013), and Guam (22 GCA § 3501) do not have these extra restrictions. New Hampshire prohibits disciplining current

employees (Use of Social Media and Electronic Mail, 2014), but does not have similar protection for job applicants.

Exceptions. The statutes in New Hampshire (Use of Social Media and Electronic Mail, 2014), Oklahoma (40 Okla. Stat. § 173.2, 2014), and Wisconsin (Wis. Stat. § 995.55, 2013) include all of the most common exceptions to the restrictions described above. Specifically, in those states:

1. Employers are not liable if they "inadvertently" acquire social media log-in credentials because an employee has accessed social media using an employer-provided device or a system the employer monitors, so long as the employer does not actually use the credentials to access the social media account.
2. Employers are free to look at any information an employee or applicant makes public.
3. Employers that are subject to regulatory requirements, such as financial institutions, may monitor employee social media accounts as necessary to meet their legal obligations.
4. Employers can investigate specific allegations of wrongdoing (such as work-related misconduct or theft of the employer's proprietary information) by an employee. States handle this in different ways. For example, in Wisconsin an employer can demand cooperation in an investigation, including an opportunity to shoulder surf, but still cannot demand the employee's log-in credentials (Wis. Stat. § 995.55, 2013).
5. Employers can demand log-in information for accounts that employees use as part of their jobs (such as a company's social media manager) and for devices and accounts provided and paid for by the employer.
6. Employers can monitor and restrict use of the employer's network and communication devices.

As shown in Appendix I, most state statutes contain at least three of these exceptions.

Enforcement. Social media privacy statutes are enforced, or not, in a variety of ways. Many states (California, for example) are silent on the question of whether there is a penalty or remedy for an employer's improper request. Others (such as Connecticut) provide that an aggrieved employee or applicant can file a complaint with the state's labor commissioner (or similar authority, depending on the state), who is authorized to investigate and, if warranted, impose civil penalties on the employer, as well as equitable relief if the aggrieved party is an existing employee (2015 Senate Bill 425, Act 16). Still other states (such as Michigan) make improper requests a misdemeanor subject to a fine, and also create a civil cause of action, with a limit on money damages, for the aggrieved party (Internet Privacy Protection Act of 2012).

Limitations on liability. There is one more interesting feature that appears in several social media privacy statutes. Some states added a provision that expressly exempts an employer from liability for *failing* to monitor employee and applicant social media accounts or failing to request access to those accounts (La. Rev. Stat. § 51:1951 et seq., 2014; Internet Privacy Protection Act of 2012). One can only imagine these provisions were designed to protect businesses from suits arising out of infractions, such as harassment, their employees might commit online (Davis, 2014).[1] Alternatively, the provisions may be intended to protect employers from "negligent hiring" claims that are based on the theory that social media would have revealed potentially dangerous flaws in an employee or applicant (Borman, 2014).

Statutes relating to schools

The statutes that regulate conduct by schools follow the same general patterns as the statutes regulating employers. Most social media privacy statutes apply only to institutions of higher

[1] On the subject of schools monitoring student online activity, one lawyer explained the risk clearly: "'What if the University of Virginia had been monitoring accounts in the Yeardley Love case and missed signals that something was going to happen?'" (Sullivan, 2012).

education, but the statutes in Louisiana (La. Rev. Stat. § 51:1951 et seq., 2014) and Michigan (Internet Privacy Protection Act of 2012) apply to all schools. Some states have different restrictions and exceptions for schools than they do for employers—both in terms of what the school can ask for and what the school can do if a request is refused—but the distinctions are not great enough to warrant discussion here.

Federal law

No current federal law addresses this specific issue. Senators Schumer (D.-NY) and Blumenthal (D.-CT) introduced the Password Protection Act of 2012 after some of the first news reports about employers asking for passwords (Blumenthal, 2012b), but the effort was unsuccessful. Rep. Perlmutter (D.-CO) has, on five occasions, introduced a "password privacy" measure—first by attempting to amend the FCC Reform Act of 2012 (Perlmutter, n.d.a) and the Cyber Intelligence Sharing and Protection Acts of 2011 (Perlmutter, n.d.b) and 2013 (Perlmutter, n.d.c), and then by introducing stand-alone bills, the Password Protection Acts of 2013 (Perlmutter, n.d.d) and 2015 (Perlmutter, n.d.e). The 2015 bill is pending, with little likelihood of success (GovTrack, 2015); all the other attempts have failed. Finally, Rep. Engel (D.-NY) twice introduced the Social Networking Online Privacy Protection Act (Engel, 2013; Engel, 2012), but neither effort succeeded.

Shortly before Senators Schumer and Blumenthal introduced the Password Protection Act of 2012, they sent joint letters to the Equal Employment Opportunity Commission and the Department of Justice (Blumenthal, 2012a). The letter to the EEOC requested an investigation into whether employers who requested social media passwords were violating federal law, especially by using the information they find to discriminate against employees and applicants (Blumenthal, 2012a). In response, the EEOC held a public meeting, entitled "Social Media in the

Workplace: Examining Implications for Equal Employment Opportunity Law" (EEOC, 2014). The Senators' letter to the Attorney General requested an investigation into "whether this practice violates the Stored Communication Act or the Computer Fraud and Abuse Act" (Blumenthal, 2012a). There is no evidence the Justice Department took any responsive action.

The Stored Communications Act ("SCA"), which predates social media, may very well offer nationwide protection against overreaching employers and schools (Segal, 2014). The SCA provides:

> whoever [other than a user with respect to a communication intended for that user]— (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a . . . communication while it is in electronic storage in such system shall be punished. (18 U.S.C. § 2701)

Several courts have held that personal websites and social networking sites like Facebook and MySpace are within the scope of the SCA (Jackson, 2014; Jeon, 2011), and that getting coerced "authorization" to access these sites does not make the intruder's conduct lawful (Beadle, 2012). The question whether an employer can use the log-in credentials of Employee A to access private areas on the social media accounts of her friend, Employee B, is unsettled (*Pietrylo v. Hillstone Restaurant Group*, 2009; *Konop v. Hawaiian Airlines*, 2002).

The Computer Fraud and Abuse Act ("CFAA") is a criminal statute primarily designed to address hacking, or theft of financial information or trade secrets (Office of Legal Education, 2010). However, the statute has a very broad section that provides: "Whoever—(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . .

(C) information . . . shall be punished" (18 U.S.C. §1030(a)(2)). Someone can violate the CFAA simply by observing (not even stealing) data stored electronically on a computer that is connected to the Internet (Office of Legal Education, 2010). In addition to criminal penalties, the CFAA provides a civil cause of action, so theoretically an aggrieved employee or applicant could sue an employer under the CFAA for accessing a social media account. There are no published cases involving such claims.

Is this really a thing?

One speaker at the EEOC's 2014 meeting declared:

> Regardless of the applicable laws, employers accessing the non-public portions of applicants' social media profiles is a non-issue. I have seen no evidence—anecdotal or otherwise—indicating that private-sector employers are trying to gain such access. I have not encountered a single client who is doing so. When I speak about these laws to clients and other human resources professionals, they indicate that they don't have the need, desire, or time to gain such access. (Jackson, 2014)

Why are there so many statutes addressing this purported "non-issue"?

The country's first social media privacy statute was triggered by the story of a wronged employee who went public. When Robert Collins, a Maryland correctional officer, returned to work after a leave of absence, his employer required him to divulge his Facebook user name and password, supposedly so the agency could check for gang affiliations (Valdes & McFarland, 2012). Naturally, by logging on to Facebook as Collins, the corrections agency representative could—and did—review not just Collins' own social media activity, but also the postings of Collins' family and friends (Peorio & Johnson, 2012). Collins felt pressured to provide log-in

credentials because he needed his job, but he was upset. He contacted the ACLU, and the organization complained to Collins' employer (Jeon, 2011) and lobbied for the Maryland statute (Borman, 2014). Notably, "[t]here are no other publicly reported cases in Maryland where an employer asked for access to a person's social networking account" (Borman, 2014, p. 130).

It is not clear what inspired twenty-one other states to follow Maryland's lead. There are plenty of press accounts that portray employers and schools as hungry for social media log-in credentials. For example, in addition to Mr. Collins, the ACLU cites the cases of a New York statistician (applying for a job at an unnamed employer); the Norman, Oklahoma police department; the city of Bozeman, Montana; and "many students" (ACLU, 2015). *The Seattle Times* adds to that list the sheriff's departments in McLean County, Illinois and Spotsylvania County, Virginia (Valdes & McFarland, 2012). *NBC News* and *USA Today* both say the demands are particularly common for college athletes (Dame, 2014; Sullivan, 2012). But these same stories (particularly the ones about the statistician and Mr. Collins) are repeated over and over (Gaydos, 2012). For every such report, there is another pointing out that these are isolated cases, mostly involving employers charged with public safety (Israel, 2012), arguing that hastily enacted social media privacy statutes are "both unwarranted and dangerous" (Davis, 2014, p. 254), or simply calling the statutes "a solution in search of a problem" (Meyer, 2015).

In light of their persistence, one would think that Reps. Perlmutter and Engel would have files of stories to share. Rep. Perlmutter insists that "[m]ore and more employers want to access your Facebook and social media accounts with your password for job screening purposes" (Perlmutter, n.d.a; Perlmutter, n.d.b; Perlmutter, n.d.e), and Rep. Engel says "[t]here have been a number of reports about employers requiring new applicants to give their username and password as part of the hiring process" (Engel, 2012). Still, neither legislator's website offers

supporting examples—or really any discussion of the bills they sponsored beyond general press releases.[2]

And that odd Oregon statute, prohibiting employers from requiring employees to have personal social media accounts? Here's the backstory:

> The bill's primary sponsor's wife had a friend, a Navy veteran, who returned from service and applied for a job . . . and the company called him and advised that he had left his Facebook account blank on the application. When he advised that he did not have a Facebook account, the company allegedly told him they would not interview him unless he had one. (Freedman, 2015)

That is certainly an unfortunate story and an odd hiring policy, but one has to wonder if it merited a legislative response.

There is a more compelling, though disheartening, potential rationale for the cascade of state social media privacy statutes: political opportunism. "Of all the urgent things that US Senators [Blumenthal and Schumer] could bring to the attention of the Justice Department . . . this seems to me to have been a very strange selection" (Israel, 2012). But the issue must be very tempting because it would be difficult to find anyone (read, "any voter") who argues with the general proposition that we don't want employers looking at our private social media pages any more than we want them reading our diaries or searching our bedrooms (Gaydos, 2012).

[2] I spoke with a staffer in Rep. Perlmutter's office who assured me that "we don't introduce legislation for no reason," but declined to make supporting material available (L. Yurow, personal communication, June 25, 2015).

Implications for employers and schools

If social media privacy statutes did not exist, there would still be plenty of things to deter an employer or school from looking at private social media accounts. The five most obvious considerations are discussed below. (To avoid unwieldy sentences, this discussion focuses on employers and employees, but the same principles apply to situations involving students, job applicants, and student applicants.)

First, looking at the social media account of an employee may reveal things the employer is not permitted to consider. For example, in his written response to the letter from Senators Schumer and Blumenthal described above, a representative from the EEOC explained that, although "EEO laws do not address the legality per se of requesting and using social network passwords," an employer could not discriminate if an employee's social media accounts revealed something the employer found unfavorable about the employee's religion, medical history, disability, or age (Miaskoff, 2014). Other things one might discover on social media include sexual orientation, number of children, and political affiliation—all of which the employer would be prohibited from considering. From an EEOC perspective, the problem isn't so much "looking" at information, but "using" it (Segal, 2014). However, a plaintiff in a Title VII discrimination case does not need to prove discrimination; the burden is merely to present enough evidence "to give rise to an inference" that the employer considered the plaintiff's protected status when taking an adverse action (Davis, 2014, p. 259). Can an employer really learn enough useful information from social media to warrant that risk?

Second, by gaining access to social media *as* an employee, the employer also gets access to the social media accounts of the employee's contacts. As discussed above, even if an employee is willing to permit a supervisor to review her own social media postings, it is not clear whether

that will protect the employer from liability under the SCA for having accessed the social media postings of the employee's friends and family.

Third, let's think back to the limitation on liability in the Louisiana and Michigan statutes discussed above. Does an employer that gains access to social media accounts lose that safe harbor? Would an employer that demanded log-in credentials once be assuming an ongoing obligation to monitor social media, and to be aware, for example, that an employee was stalking his ex-wife?

Fourth, social media can lack context and nuance. A manager who isn't privy to the backstory may not accurately interpret an employee's Facebook postings. Employers that take social media at face value might be making serious misjudgments (Davis, 2014).

Finally, any employer—especially one in the private sector—that requires social media log-in credentials from employees and applicants is sure to lose candidates and employees, and likely will suffer a brutal public relations backlash (Gaydos, 2012; Jeon, 2011).

Conclusion

So, are social media privacy statutes necessary protection, harmless posturing, or something else entirely? I believe they are the latter.

These statutes aren't "necessary" for three reasons: they address situations that are infrequent; they ban conduct that arguably is prohibited by the SCA (and other federal law that is beyond the scope of this paper); and any employer or school that tried to demand social media log-in credentials today without a very good reason would suffer more from the bad publicity than they would from a misdemeanor charge or statutory penalty.

At the other end of the spectrum, these statutes aren't completely "harmless." They impose requirements that employers and schools must understand so they can ensure that even innocent actions (say, a supervisor asking to "friend" an employee with whom he socializes) don't violate the law. Moreover, like the dozens of futile Congressional attempts to repeal the Affordable Care Act, drafting, debating, and voting on these statutes consumes legislative time and resources that would be better used elsewhere.

It is perfectly reasonable for a state to announce—perhaps by means of a governor's executive order—that it is against public policy to require employees and students to divulge their social media log-in credentials. Turning that policy statement into a legislative mandate is overkill.

References

American Civil Liberties Union. (2015). *Employers, schools, and social networking privacy*. Retrieved from https://www.aclu.org/employers-schools-and-social-networking-privacy?redirect=free-speech/employers-schools-and-social-networking-privacy.

Beadle, N.D. (2012). A risk not worth the reward: The Stored Communications Act and employers' collection of employees' and job applicants' social networking passwords. *American University Business Law Review, 1*(2), 397-412.

Blumenthal, R. (2012a, March 25). Blumenthal, Schumer: Employer demands for Facebook and email passwords as precondition for job interviews may be a violation of federal law; Senators ask feds to investigate [Press release]. Retrieved from http://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-schumer-employer-demands-for-facebook-and-email-passwords-as-precondition-for-job-interviews-may-be-a-violation-of-federal-law-senators-ask-feds-to-investigate.

Blumenthal, R. (2012b, May 9). Senators and congressmen introduce Password Protection Act of 2012 [Press release]. Retrieved from http://www.blumenthal.senate.gov/newsroom/press/release/senators-and-congressmen-introduce-password-protection-act-of-2012.

Borman, A. (2014). Maryland's social networking law: No "friend" to employers and employees. *Journal of Business & Technology Law 9*(1), 127-50.

Computer Fraud and Abuse Act, 18 U.S.C. §1030 (2010).

Dame, J. (2014, January 10). Will employers still ask for Facebook passwords in 2014? *USA Today*. Retrieved from http://www.usatoday.com/story/money/business/2014/01/05/facebook-passwords-employers/4327739/.

Davis, M. (2014). Too much too soon? A case for hesitancy in the passage of state and federal password protection laws. *Journal of Technology Law & Policy XIV*(Spring), 253-72.

Dipietro, B. (2015, May 28). Laws try to resolve employer-employee social media conflicts. *The Wall Street Journal*. Retrieved from http://blogs.wsj.com/riskandcompliance/2015/05/28/laws-try-to-resolve-employer-employee-social-media-conflicts/.

Employee Social Media Privacy, R.I. Gen. Laws § 28-56-1 to -6 (2014).

Engel, E. (2012, April 27). Rep. Engel seeks to protect personal online content [Press release]. Retrieved from http://engel.house.gov/latest-news1/rep-engel-seeks-to-protect-personal-online-content/.

Engel, E. (2013, February 6). Reps. Engel, Schakowsky, Grimm seek to protect online content [Press release]. Retrieved from http://engel.house.gov/latest-news1/reps-engel-schakowsky-grimm-seek-to-protect-online-content/.

Equal Employment Opportunity Commission (EEOC). (2014, March 12). *Meeting of March 12, 2014 - Social media in the workplace: Examining implications for equal employment opportunity law*. Retrieved from http://www.eeoc.gov/eeoc/meetings/3-12-14/index.cfm.

Freedman, L. (2015, June 4). Oregon social media law signed by Governor. *Data Privacy + Security Insider*. Retrieved from http://www.dataprivacyandsecurityinsider.com/2015/06/oregon-social-media-law-signed-by-governor/.

Gaydos, E. (2012, May 15). Relax – You'll never, ever be asked for a Facebook password. Retrieved from http://www.eremedia.com/tlnt/relax-youll-never-ever-be-asked-for-a-facebook-password/.

GovTrack. (2015). *H.R. 2277: Password Protection Act of 2015*. Retrieved (July 2, 2015) from https://www.govtrack.us/congress/bills/114/hr2277.

Internet Privacy Protection Act of 2012, Mich. Comp. Laws § 37.271 to 37.278 (2012).

Israel, Shel. (2012, March 25). The great Facebook employee password non-issue. *Forbes*. Retrieved from http://www.forbes.com/sites/shelisrael/2012/03/25/the-great-facebook-employee-password-nonissue/.

Jackson, R. (2014, March 12). Written testimony: Meeting of the Equal Employment Opportunity Commission on social media in the workplace. Retrieved from http://www.eeoc.gov/eeoc/meetings/3-12-14/jackson.cfm.

Jeon, D. (2011, January 25). Letter from ACLU of Maryland to Maryland Department of Public Safety and Correctional Services. Retrieved from http://www.aclu-md.org/uploaded_files/0000/0041/letter-_collins_final.pdf.

Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002).

Meyer, E. (2015, May 27). Those without Facebook accounts need not apply. Well, maybe not in one state. Retrieved from http://www.theemployerhandbook.com/2015/05/those-without-facebook-accounts-need-not-apply-well-not-in-one-state.html.

Miaskoff, C. (2014, March 12). Written testimony: Meeting of the Equal Employment Opportunity Commission on social media in the workplace. Retrieved from http://www.eeoc.gov/eeoc/meetings/3-12-14/miaskoff.cfm.

National Conference of State Legislatures. (2015, June 4). *Access to social media user names and passwords*. Retrieved (June 21, 2015) from http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

Office of Legal Education, Executive Office for United States Attorneys. (2010). Prosecuting Computer Crimes, pp. 1-57. Retrieved from http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

Oregon State Legislature. (2015). *2015 Regular session; SB 185A*. Retrieved (June 21, 2015) from https://olis.leg.state.or.us/liz/2015R1/Measures/Overview/SB185.

Peorio, J.M. & Johnson, B.L. (2012, September 1). Social media accounts in the workplace: Employers need to proceed smartly in the face of new law. *Employee Relations Law Journal 38*(2), 63-67.

Perlmutter, E. (n.d.a). Perlmutter introduces password privacy measure [Press release]. Retrieved from http://perlmutter.house.gov/index.php/media-center/press-releases-86821/1060-perlmutter-introduces-password-privacy-measure.

Perlmutter, E. (n.d.b). Perlmutter re-introduces Facebook password privacy measure, precludes government from establishing Chinese-style "great internet firewall" [Press release]. Retrieved from http://perlmutter.house.gov/index.php/media-center/press-releases-86821/1075-perlmutter-re-introduces-facebook-password-privacy-measure-precludes-government-from-establishing-chinese-style-qgreat-internet-firewallq.

Perlmutter, E. (n.d.c). Perlmutter re-introduces password privacy measure [Press release]. Retrieved from http://perlmutter.house.gov/index.php/media-center/press-releases-86821/1185-perlmutter-re-introduces-password-privacy-measure.

Perlmutter, E. (n.d.d). FACEBOOK: LIKE IT! Perlmutter, Welch introduce password protections for employees [Press release]. Retrieved from http://perlmutter.house.gov/index.php/media-center/press-releases-86821/1199-facebook-like-it-perlmutter-welch-introduce-password-protections-for-employees.

Perlmutter, E. (n.d.e). Perlmutter re-introduces password protection act [Press release]. Retrieved from http://perlmutter.house.gov/index.php/media-center/press-releases-86821/1516-perlmutter-re-introduces-password-protection-act.

Pietrylo v. Hillstone Restaurant Group, 2009 WL 3128420 (D.N.J. 2009).

Segal, J. (2014, March 12). Written testimony on behalf of the Society for Human Resource Management: Meeting of the Equal Employment Opportunity Commission on social media in the workplace. Retrieved from http://www.eeoc.gov/eeoc/meetings/3-12-14/segal.cfm.

Stored Communications Act, 18 U.S.C. §§ 2701 et seq. (2006).

Sullivan, B. (2012, March 6). Govt. agencies, colleges demand applicants' Facebook passwords. *NBC News*. Retrieved from http://www.nbcnews.com/business/consumer/govt-agencies-colleges-demand-applicants-facebook-passwords-f328791.

Use of Social Media and Electronic Mail, N.H. Rev. Stat. § 275:74 (2014).

Valdes, M. & McFarland, S. (2012, March 20). Employers ask job seekers for Facebook passwords. *The Seattle Times*. Retrieved from http://www.seattletimes.com/nation-world/employers-ask-job-seekers-for-facebook-passwords/.

Appendix I
Summary of state laws

State	Statute(s)	Restricted entities	Protected persons	What is restricted?*	Exceptions**
Arkansas	Ark. Code § 11-2-124 and § 6-60-104	Employers, institutions of higher education	Current and prospective employees, current and prospective students	A, B, C, J, K, L, M	1, 2, 3, 4
California	Calif. Lab. Code § 980 and Calif. Ed. Code § 99121	Employers, institutions of higher education	Current and prospective employees, current and prospective students	A, D, E, J, K, L, M	4, 5
Colorado	C.R.S. 8-2-127	Employers (other than law enforcement and corrections agencies)	Current and prospective employees	A, B, C, J, K	3, 4, 5
Connecticut (effective 10/1/15)	2015 S.B. 425, Act 16	Employers	Current and prospective employees (other than applicants to law enforcement agencies)	A, B, E, J, K	3, 4, 5, 6
Delaware	14 Del. Code § 8103	Institutions of higher education (pending bill would apply to employers)	Current and prospective students	A, B, E, F, G, L, M	4
Guam	22 GCA § 3501	Employers	Current and prospective employees	A	3
Illinois	820 ILCS 55/10, and 105 ILCS 75/10	Employers, institutions of higher education	Current and prospective employees, students and their	A	2, 3, 7, 8 4 (for students)

			parents/guardians		
Louisiana	La. Rev. Stat. § 51:1951-1954	All schools and employers	Current and prospective employees, current and prospective students	A, J, K, L, M	1, 2, 3, 4, 5, 6
Maryland	Md. Labor and Emp. Code § 3-712	Employers (pending bill would apply to institutions of higher education)	Current and prospective employees	A, J, K	3, 4, 5
Michigan	MCL § 37.271-37.278	All schools and employers	Current and prospective employees, current and prospective students	A, E, J, K, L, M	2, 3, 4, 5, 6, 7
Montana	2015 H.B. 343, Chap. 263	Employers	Current and prospective employees	A, D, E, J, K	3, 4, 5, 6
Nevada	NRS § 613.135	Employers	Current and prospective employees	A, J, K	3, 6
New Hampshire	N.H. Rev. Stat. § 275:74	Employers	Current and prospective employees	A, B, C, J	1, 2, 3, 4, 5, 6, 7
New Jersey	N.J. Stat. § 34:6B-5 through 6B-10 and N.J. Stat. § 18A:3-29 through 3-32	Employers (other than law enforcement and corrections agencies), institutions of higher education	Current and prospective employees, current and prospective students	A, J, K, L	3, 4

New Mexico	N.M. Stat. § 50-4-34 and N.M. Stat. § 21-1-46	Employers (other than law enforcement agencies), institutions of higher education	Prospective employees, current and prospective students	A, L, M	2, 7
Oklahoma	40 Okla. Stat. § 173.2	Employers	Current and prospective employees	A, E, J, K	1, 2, 3, 4, 5, 6, 7
Oregon	O.R.S. § 659A.330, 2015 S.B. 185, O.R.S. § 326.551	Employers, institutions of higher education	Current and prospective employees, current and prospective students	A, B, E, H, I, J, K, L, M	1, 2, 3, 4, 6 7 (for students only)
Rhode Island	R.I. Gen. Laws § 28-56-1 to -6, R.I. Gen. Laws § 16-103-1 to -6	Employers, institutions of higher education	Current and prospective employees, current and prospective students	A, B, C, D, E, J, K, L, M	3, 4, 6 (for employees) 2 (for students)
Tennessee	Tenn. Code §§ 50-1-1001 to -1004	Employers	Current and prospective employees	A, B, E, J, K	2, 3, 4, 5, 6, 7
Utah	Utah Code § 34-48-201 et seq and Utah Code § 53B-25-101 et seq.	Employers, institutions of higher education	Current and prospective employees, current and prospective students	A, J, K, L, M	2, 3, 4, 5, 6, 7
Virginia	2015 H.B. 2081, Chapter 576	Employers	Current and prospective employees	A, B, J, K	1, 2, 3, 4, 5, 6
Washington	RCW §§ 49.44.200	Employers	Current and prospective employees	A, B, C, E, J, K	1, 3, 4, 5, 6, 7

Wisconsin	Wis. Stat. § 995.55	Employers, institutions of higher education, landlords	Current and prospective employees, current and prospective students, tenants	A, E, J, K, L, M (similar restrictions respecting discrimination against a tenant or prospective tenant)	1, 2, 3, 4, 5, 6, 7 (employees) 2, 5, 6 (students) 2 (tenants)

***Restrictions**

A restricted entity cannot require (request, suggest, or cause) a protected person to:

A. Disclose the user name and password for a social media account
B. Add a designated person from the restricted entity as a connection on a social media account
C. Change privacy settings on a social media account
D. Disclose the postings on a social media account
E. Log in to a social media account and permit someone from the restricted entity to review its contents

A restricted entity cannot:

F. Track a protected person's electronic communications (by installing software on a device or using remote tracking technology).
G. Access a protected person's social media account or profile indirectly (by using the account of someone else with whom the protected person is connected).
H. Require a protected person to establish a social media account.
I. Require a protected person to permit the restricted entity to advertise on the protected person's social media account.
J. [for employers] Take or threaten disciplinary action against an existing employee (including denial of a promotion) because the employee refuses to comply with a request the employer was not permitted to make anyway.
K. [for employers] Refuse to hire a job applicant because the applicant refuses to comply with a request the employer was not permitted to make anyway.
L. [for schools] Penalize a student, or refuse to let a student participate in extracurricular activities and other school-sponsored programs, because the student refuses to comply with a request the school was not permitted to make anyway.
M. [for schools] Refuse to admit an applicant because the applicant refuses to comply with a request the school was not permitted to make anyway.

****Exceptions**

1. A restricted entity is not liable for inadvertently getting social media log-in credentials through a device provided by that entity and used by a protected person, or through a program that monitors the restricted entity's network, but cannot use the information to gain access to the account.
2. Restricted entities can view information that is publicly available online.
3. Restricted entities can do what is necessary to comply with other legal requirements (such as securities regulations).
4. Restricted entities can demand access (but not necessarily log-in credentials) in connection with (and for the limited purpose of) an investigation of misconduct involving the protected person.
5. Restricted entities can demand log-in credentials to any device or system they provide to protected persons.
6. Restricted entities can demand log-in credentials to accounts a protected person uses for the restricted entity's business (or academic) purposes.
7. A restricted entity can monitor usage on, and control access to, its own internal systems.
8. E-mail expressly is not considered "social media." (Many of the definitions specifically include e-mail; others are open to interpretation.)

Georgia, Hawaii, Maine, Massachusetts, Missouri, New York, Pennsylvania, and Texas all have bills pending.

Two states, Maine and Vermont, ordered studies into whether this kind of legislation is necessary.