A Timely Analysis of Legal Developments

ASAP®

April 30, 2013

Social Media Password Protection and Privacy — The Patchwork of State Laws and How It Affects Employers

by Phillip L. Gordon, Amber M. Spataro and William J. Simmons

Introduction

Social media websites such as Facebook, Twitter, LinkedIn and others have become a part of daily life in the United States and abroad.[1] The unavoidable reach of social media into our personal lives has extended into our professional lives. Facebook claims to have more than 1 billion users. As of December 31, 2012, LinkedIn boasted more than 200 million registered users in over 200 countries and territories and that LinkedIn members performed "over 5.7 billion professionally-oriented searches on the platform in 2012."[2] It is reasonable to infer that those 5.7 billion searches were not limited to individuals seeking jobs, professional connections or merely long lost friends, but also included employer representatives searching for qualified candidates.[3]

The following statistics from 2012 illustrate just how intertwined social media have become with work:[4]

- In 2012, 52 percent of job seekers used Facebook to help find work (up from 48 percent in 2011), 38 percent of job seekers used LinkedIn to help find work (up from 30 percent in 2011), and 34 percent of job seekers used Twitter to help find work (up from 26 percent in 2011);
- 1 in 5 had a contact share a job on Facebook (same as 2011), 19 percent had a contact share a job on LinkedIn (versus 8 percent in 2011), and 11 percent had a contact share a job on Twitter (vs. 7 percent in 2011);

1 http://newsroom.fb.com/Key-Facts.

2 http://press.linkedin.com/about.

3 http://blog.reppler.com/2011/09/27/managing-your-online-image-across-social-networks/.

4 http://thenextweb.com/socialmedia/2012/10/08/over-half-of-american-job-seekers-use-facebook-to-help-find-work-linkedin-and-twitter-are-gaining/.

- 14 percent searched for jobs on Facebook, 11 percent searched for jobs on LinkedIn, 10 percent searched for jobs on Twitter;
- 17 percent of Facebook users provided their profile on a job application or during an interview, 9 percent of LinkedIn users provided their profile on a job application or during an interview, and 10 percent of Twitter users provided their profile on a job application or during an interview; and
- 24 percent of job seekers reported they have been asked for social media profiles during their interview process. As a result, 88 percent have at least one social networking profile, 64 percent have accounts on at least two networks, and 44 percent use three or more.

"With fierce competition for jobs, which now includes a majority of employed people on top of active job seekers, social media has become a critical tool for job hunting and career growth," Jobvite President & CEO Dan Finnigan declared in a recent statement.[5] "Maintaining your online presence and keeping employment top-of-mind at all times are vital to professional success. With technology and social networking rapidly evolving, those who don't engage through Facebook, LinkedIn and/or Twitter will quickly find themselves falling behind."[6]

In the last decade, most employers, at some point, have reviewed an employee's or applicant's emails, blogs or online social media postings, either in the capacity of "employer" or perhaps as a "friend." Social media monitoring service Reppler recently surveyed over 300 hiring professionals to determine when and how job recruiters are screening job candidates on different social networks.[7] The study found that more than 90 percent of recruiters and hiring managers have visited a potential candidate's profile on a social network as part of the screening process.[8] Moreover, 69 percent of recruiters have rejected a candidate based on content found on his or her social networking profiles—an almost equal proportion of recruiters (68%), though, have hired a candidate based on his or her presence on those networks.[9]

Employers' access to applicants' and employees' social media activity raises two separate but related questions. First, what social media sites can employers lawfully access to obtain information about applicants and employees? Second, to what extent can employers lawfully rely on information obtained through social media to make employment decisions? The second question raises the types of anti-discrimination concerns that employers have been confronting in the off-line world for decades. However, the first question exposes employers to a completely new legal landscape, one which just began to evolve in April 2012, when Maryland enacted the Nation's first "social media password protection law" and has expanded in the past year to include six additional states—California, Illinois, Michigan, New Jersey, New Mexico, and Utah. With password-protection legislation pending in over twenty state legislatures, this legal landscape undoubtedly will become more complex, especially for multi-state employers, over the next one to two years.

This paper explores the history and background of social media password protection legislation, the differences between the state laws, and how those differences create challenges for employer compliance. The paper concludes by describing the terms a model statute at the federal level should include to eliminate the existing and expanding patchwork of state laws.

State Laws Precluding Employer "Access" to Applicants' and Employees' Personal Password-Protected Social Media Accounts

Employers, like everyone else, indisputably can access information on social media that is publicly available. However, users of social media increasingly are resorting to the privacy settings to screen their social media activity from others, including employers. According to one study, 15 percent of Facebook users (or nearly 150 million users), 7 percent of LinkedIn users (or nearly 15 million users), and 5 percent of Twitter users (or more than 27 million) modified privacy settings specifically with work in mind.[10] These statistics do not encompass the tens of millions of other users who take advantage of privacy settings for other reasons.

Even though many, if not most, social media sites offer privacy settings that permit users to control access to their personal social media pages, legislators in over two dozen states apparently believe that privacy settings are insufficient to protect applicants and employees from

5 *Id.*

6 *Id.*

7 http://blog.reppler.com/2011/09/27/managing-your-online-image-across-social-networks/.

8 *Id.*

9 *Id.*

10 http://thenextweb.com/socialmedia/2012/10/08/over-half-of-american-job-seekers-use-facebook-to-help-find-work-linkedin-and-twitter-are-gaining/.

the supposedly prying eyes of employers and, therefore, have introduced and/or enacted social media password protection legislation. However, a closer analysis of both the anecdotal and empirical evidence demonstrates that these laws, in fact, are a solution looking for a problem. They not only are unnecessary, but they also radically rewrite decades of privacy law in the United States, and unfairly expose employers to potential liability.

A. Dubious History of Social Media "Password Protection" Legislation

The story went viral, and legislators around the country caught the virus. On March 21, 2012, the Associated Press reported a few incidents where employers had requested or required log-in credentials from applicants or employees to access their personal social media account. Over the next three weeks, more stories were published; some regurgitating the incidents originally reported by the A.P., and others reporting on additional, alleged inquiries.[11] It was reported that some employers were stopping just short of asking for applicants' passwords and, instead, were asking applicants to log into their profiles and click through private messages, photos, wall posts, and other items as the interviewer watches. Called "shoulder surfing," the ACLU initially contended that, even though it is technically voluntary, it is a gross violation of one's privacy.[12] As the *Daily Mail* noted, sharing passwords is actually a violation of Facebook's terms.[13] Facebook's policy on registration and account security reads "you will not share your password… let anyone else access your account, or do anything that might jeopardize the security of your account."[14] Facebook spokesman Fred Wolens told PCMag in a statement: "Under our terms, only the holder of the email address and password is considered the Facebook account owner. We also prohibit anyone from soliciting the login information or accessing an account belonging to someone else."[15]

The media frenzy stoked public outrage. Facebook threatened to take legal action against employers who required applicants to turn over their Facebook passwords in order to get a job. On Friday, March 23, 2012, Facebook Chief Privacy Officer Erin Egan wrote, "We'll take action to protect the privacy and security of our users, whether by engaging policymakers or, where appropriate, by initiating legal action, including by shutting down applications that abuse their privileges."[16] Notably, we are aware of no such lawsuit having been filed by Facebook to date. Legislators around the country and in Congress sought to ride the wave of public sentiment by introducing legislation to slam the door on the perceived abuse.

1. Why Social Media "Password Protection" Laws Are Unnecessary

Neither the A.P. article nor any other article from a major U.S. news outlet comprising the media frenzy of spring 2012 cites a single study proving that private employers routinely ask applicants or employees for log-in credentials to their personal social media accounts. A careful review of the anecdotal "evidence" contained in these news stories demonstrates that the exact opposite is true. All of the media coverage combined reported *one* instance in which a private employer requested log-in credentials. All but this one reported incident involved public employers, such as corrections departments and police forces. The overwhelming buzz drowned out this critical distinction.

The only empirical data of which we are aware is fully consistent with this anecdotal evidence demonstrating that private employers do *not* ask for log-in credentials. Littler Mendelson's Executive Employer Survey Report, published in June 2012, asked nearly 1,000 C-suite executives, corporate counsel, and human resources professionals from corporations throughout the United States and ranging in market capitalization from less than $1 billion to more than $4 billion the following question: "Has your organization requested social media logins as part of the hiring or onboarding process?"[17] The response: *99% of respondents answered the question in the negative*.

At least as far as private employers are concerned, there is no proven need for password protection laws. Both the available anecdotal and empirical evidence, albeit limited, compel the conclusion that private employers are not asking applicants or employees for personal social media log-in credentials.

---

11 http://www.dailymail.co.uk/news/article-2111059/Colleges-jobs-asking-Facebook-email-passwords-job-interviews.html?ito=feeds-newsxml.

12 http://www2.timesdispatch.com/news/2012/mar/28/aclu-warns-state-police-social-media-checks-applic-ar-1798387/.

13 http://www.dailymail.co.uk/news/article-2111059/Colleges-jobs-asking-Facebook-email-passwords-job-interviews.html?ito=feeds-newsxml.

14 http://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057.

15 http://www.pcmag.com/article2/0,2817,2401254,00.asp.

16 http://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057.

17 Littler Mendelson Executive Employer Survey Report (June 2012), *available at* http://www.littler.com/content/littler-mendelson-executive-employer-survey-report-2012.

2. How Social Media "Password Protection" Legislation Radically Rewrites the Common Law of Privacy

The state password protection laws that have been enacted generally prohibit employers from requesting or requiring that employees or applicants provide the log-in credentials for a personal social media account. The underlying premise of these laws is that an employer invades an applicant's or employee's privacy by viewing content on a restricted access social media account without the voluntary consent of the account holder. Digging one step deeper, these laws, at their core, assume that the content of a restricted access social media account is private no matter how many people the user invites to view that content and regardless of the relationship between the user and the viewer. Put more plainly, these laws are based on the belief that, for example, a Facebook user who has more than 500 "Friends," including current and former supervisors and other executives at his current employer, can establish the "privacy" of his content by using Facebook's privacy settings to restrict access to "Friends Only."

No court has ever construed the tort of invasion of privacy by intrusion upon seclusion so broadly. That tort requires a "private fact" which can be the subject of an intrusion. The vast majority of courts have held that, if the fact that is the subject of the claim has been disclosed to even a few people not under a legal or contractual obligation of confidentiality, the fact is not private and the intrusion upon seclusion claim fails.[18] To be sure, a few cases have permitted an intrusion upon seclusion claim to proceed even though the plaintiff had shared the private fact with others. However, in virtually all of these cases, the private fact was shared within a group that had a specific relationship with the plaintiff, such as coworkers or co-participants in an *in vitro* fertilization program.[19] We are not aware of any case holding that facts disclosed to dozens or hundreds of people who do not form a cohesive group are "private facts," especially when that group includes management-level employees of the employer who is the defendant on the privacy claim. In sum, the password protection laws create a "ring of privacy" with a circumference far larger than any court has recognized to date.

Notably, the one reported case where a jury considered whether an employer committed an intrusion upon seclusion by accessing two employees' restricted-access social media sites resulted in a verdict on that claim f*or the employer*. In that case, *Pietrylo v. Hillstone Restaurant Group*, a group of employees at a Houston's restaurant (the chain owned by the Hillstone Restaurant Group) established an invitation-only, password-protected MySpace page.[20] In the words of the site's founder, the page would permit group members to "vent about any BS we deal with [at] work without any outside eyes spying in on us." The founder emphasized in his first post that "[t]his group is entirely private." The employer accessed the site after a group member shared her log-in credentials with a member of management. After viewing the rants about the company, management and customers, Houston's fired the site's founder and another group member. Both responded by suing the employer for, among other claims, violating the federal Stored Communications Act (SCA) and common law invasion of privacy.

While the jury's verdict for the fired employees on their SCA claim has received substantial press and academic attention, the jury's verdict *for* Hillstone on the invasion of privacy claim seems to have been lost in the shuffle. The jury's verdict form reveals the jury rejected the employees' invasion of privacy claim based on its finding that the fired employees did not have a reasonable expectation of privacy in the content they posted on their site. The jury reached this conclusion despite the password protection, despite the invitation-only rule, and despite the founder's pronouncement that the site was "entirely private." A fair inference is that the jurors believed the fired employees could not reasonably expect privacy in content available to numerous group members and that could be further disclosed by any group member to anyone, including journalists, without restriction.

Legislators, of course, are free to create a public policy that overturns decades of common law jurisprudence, particularly when necessary to address new technology not yet considered by common law courts. However, the validity of any new public policy should be closely scrutinized when there is no apparent need for it, it is so broad that it leads to absurd results, and, it potentially exposes all private employers to substantial

18 *See, e.g., Duran v. Detroit News, Inc.*, 200 Mich. App. 622 (1993) (intrusion claims failed because the information defendants obtained was either available via public record or had been disclosed by plaintiffs such that it was "open to the public eye"); *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 877-78 (8th Cir. 2000) (intrusion claim failed where plaintiff asserted a privacy interest in the medical fact that she had a staph virus at the time of her employment termination because plaintiff revealed this information to her co-workers); *cf. Nader v. Gen. Motors Corp.*, 25 N.Y.2d 560, 568-69 (1970) (intrusion claim was unsupported by allegations that defendants interviewed people who knew plaintiff and thereby obtained information of a private nature because plaintiff assumed the risk that those he confided in may breach that confidence; plaintiff's claim was supported on other grounds such as unauthorized wiretapping).

19 *See, e.g., Sanders v. Amer. Broadcasting Cos.*, 20 Cal. 4th 907 (1999) (even though the plaintiff's conversation could be seen and overheard by co-workers, plaintiff's intrusion claim could proceed where media reporter covertly taped plaintiff's conversation). *Cf. Y.G. v. Jewish Hosp. of St. Louis*, 795 S.W.2d 488, 502 (Mo. Ct. App. 1990) (plaintiffs use of *in vitro* fertilization was a private matter even though they attended a social function for participants in the hospital's *in vitro* fertilization program).

20 *Pietrylo v. Hillstone Rest. Group*, No. 2:06-cv-05754-FSH-PS (D.N.J. 2008).

liability. State and federal legislators should recognize that they may have "jumped the gun" by relying on hype rather than facts in their hurried attempt to get ahead of a public outcry. At this point, there is no empirical data suggesting that private employers are routinely or even occasionally requesting or requiring personal social media log-in credentials. Consequently, it was unnecessary to enact legislation that would radically expand the definition of "privacy" and substantially impede employers' ability to investigate potentially unlawful and even criminal conduct.

B. State Laws Precluding Employer "Access" to Applicant and Employee Personal Password Protected Accounts

The legal environment surrounding access to employees' and applicants' social media (or any password-protected Internet activity) is changing dynamically and in troubling ways, especially for multi-state employers. Seven states have enacted laws regulating employer activity in this space, with many more states, and even Congress, considering such laws. These laws, however, do not follow a model with identical or nearly identical terms. Instead, they create a complex patchwork that makes it virtually impossible for a multi-state employer to establish a uniform policy:

- Each state uses its own key terms (some of which are defined, some of which are not);
- Each state defines its own scope of coverage (some as narrow as prohibiting only seeking login information from applicants, some as broad as prohibiting employers from requiring employees to disclose any internet content to their employers); and
- Each state defines its own remedial scheme (some silent on remedies, some providing for a private right of action, and some requiring administrative enforcement).

A description of each social media password protection law enacted to date follows below:

1. California

On September 27, 2012, California Governor Jerry Brown signed into law the Nation's third law that generally prohibits employers from requiring or requesting that an employee or applicant provide access to personal social media content.[21] The law, entitled "Employer Use of Social Media," went into effect on January 1, 2013.

The California law prohibits employers from requesting or requiring that applicants or employees to: (a) disclose social media log-in credentials; (b) access personal social media in the employer's presence, *i.e.*, allow the employer to "shoulder surf;" or (c) "[d]ivulge any personal social media content."22 The third prohibition is particularly broad, apparently barring an employer from asking an employee to provide the personal social media content of a coworker who is a Facebook friend.

Unlike the Illinois and Maryland laws, California's law embodies a more balanced approach, taking into account employers' legitimate business interests. The law contains a relatively broad exception that permits employers to ask an employee to divulge personal social media content that the employer "reasonably believe[s] to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations."

California's password protection law also prohibits an employer from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee or applicant for refusing to comply with an employer's request or demand for access to a personal social media account.[23] At the same time, the law expressly states that California's Labor Commissioner is not required to investigate complaints that the law has been violated, and the law does not create a private right of action for an employee to prosecute violations of the law. Consequently, it remains to be seen what remedies an employee could pursue in the instances where the Labor Commissioner declines to investigate complaints of violations.

---

21 http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201120120AB1844.

22 *Id.*

23 *Id.*

2. Illinois

On August 1, 2012, Illinois Governor Pat Quinn signed into law a bill modifying Illinois' Right to Privacy in the Workplace Act to limit both public and private employers' access to applicants' and employees' restricted social media accounts.[24] Illinois's new law (which became effective January 1, 2013) makes it unlawful for an employer to: (a) "request or require any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website"; or (b) "demand access in any manner to an employee's or prospective employee's account or profile on a social networking website."[25] This language prohibits not only direct requests for log-in credentials, but also "shoulder surfing," *i.e.*, viewing social media content over an applicant's or employee's shoulder without asking for log-in credentials, and requests that an employee print screen shots of a coworker's social media posts.

The Illinois law has no exceptions, but does expressly state that it does not apply to "information that is in the public domain," *i.e.*, social networking sites for which the account holder has not used privacy settings to restrict access. However, this limitation provides little aid to employers as applicants increasingly activate privacy settings to restrict access to their social media accounts. Further, because Facebook settings can be modified to permit different people access to different information, it is not clear what information will be considered to be in the "public domain."

The Administration and Enforcement Section of the Right to Privacy in the Workplace Act, which was amended by this new law, provides that an employee or applicant for employment may file a complaint with the Illinois Department of Labor.[26] If the Department fails to file a civil action, the employee or applicant may commence an action in Circuit Court. A successful plaintiff may be awarded actual damages, plus costs, and a penalty may issue against the employer of $200 per violation for a willful and knowing violation.

3. Maryland

Maryland was the first state to pass a law, the User Name and Password Privacy Protection Act (UNPPPA), which banned employers from asking employees and applicants for social media passwords and login information.[27] Under the UNPPPA, which took effect on October 1, 2012, Maryland employers are prohibited from requiring, or even asking, that applicants or employees disclose their user names or passwords for "any personal account or service" accessed through "computers, telephones, personal digital assistants, and other similar devices."[28] The UNPPPA contains exceptions for investigations by employers in suspected securities fraud violations and suspected misappropriation of trade secrets.

Significantly, the law does not authorize applicants or employees to sue an employer that violates the UNPPPA. It is possible that an employee terminated in violation of the law could have a claim for wrongful discharge in violation of public policy because the law prohibits an employer from taking or threatening any form of adverse action based on an employee's or applicant's refusal to provide a user name or password to a personal account accessed through a communications device.[29]

4. Michigan

Michigan's social media password protection, dubbed the "Internet Privacy Protection Act" (IPPA), went into effect on December 28, 2012.[30] The new law provides three prohibitions. First, employers cannot ask applicants or employees for the user name and password or other log-in credentials to gain access to the individual's personal, Internet-based accounts, *i.e.*, an account for which the user restricts access to content

---

24 David B. Ritter, *New Illinois Law Bars Employer Access to Social Media Accounts*, Business Management Daily, http://www.businessmanagementdaily.com/33277/new-illinois-law-bars-employer-access-to-social-media-accounts.

25 http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2398&ChapterID=68.

26 *Id.*

27 Sarah Breitenbach, *Md. Becomes First to OK Password Protection Bill*, Associated Press (Apr. 20, 2012) *available at* http://news.yahoo.com/md-becomes-first-ok-password-protection-bill-113022373.html.

28 *Id.*

29 *Id.*

30 http://www.legislature.mi.gov/(S(z3ba3a45eaypfnjfkykzfobj))/mileg.aspx?page=BillStatus&objectname=2012-HB-5523.

by way of log-in credentials. Second, the IPPA bars employers from asking applicants or employees to "allow observation of" their account, making it illegal to "shoulder surf." Third, the IPPA prohibits employers from asking applicants or employees to "grant access to" their personal accounts, thereby barring employers from reviewing content without asking for log-in credentials and without shoulder surfing. All employers, regardless of size, are subject to the IPPA's restrictions.

However, the IPPA does not prohibit an employer from asking an employee to help the employer view content in another employee's or in an applicant's personal social media account.[31] The IPPA prohibits access only to the personal content of the applicant or employee who is the subject of the request. Given that employees routinely report social media conduct of coworkers that violates corporate policy or is suspected to be unlawful, this limitation is critical for employers seeking to investigate an employee's Internet misconduct or compromising Internet postings by a job applicant. Importantly, the IPPA's prohibitions do not apply when an employer has a duty under federal law, or to comply with a self-regulatory scheme established under the Securities and Exchange Act, to screen applicants or monitor or retain certain employee communications.

The IPPA exposes individual employees to criminal prosecution for a misdemeanor offense, but the punishment is limited to a fine of not more than $1,000. Similarly, the IPPA's civil remedy provisions caps damages at $1,000 and an award of attorneys' fees and costs. Potential plaintiffs must serve a written demand on the employer at least 60 days before asserting the claim. This provision gives employers the opportunity to forestall a claim by offering $1,000 in response to a demand.

5. New Jersey

New Jersey's General Assembly passed its bill on March 21, 2013.[32] New Jersey's law is more pro-employee/applicant than any such law enacted to date, providing the broadest protections, the narrowest exceptions, and the most generous remedies. As of this writing, the bill is awaiting the Governor's signature.

Specifically, the New Jersey bill prohibits an employer from requesting or requiring, as a condition of employment, that a current or prospective employee "provide or disclose any user name or password, *or in any way provide* the employer access to," *any* personal social networking account, service or profile. The italicized language appears to prohibit New Jersey employers not only from "shoulder surfing," but also from asking an employee who complains about the social media activity of a coworker, such as online sexual harassment, for access to the complaining employee's personal social media account to observe what the alleged harasser posted. Unlike the laws in California, Michigan, and Utah, the New Jersey bill contains no exception for workplace investigation into suspected unlawful conduct or violations of employer policies. Notably, the New Jersey bill does not contain a narrower exception, such as the one in Maryland's law, which includes a carve-out for investigations into suspected violations of securities laws or regulations or into suspected misappropriation of trade secrets.

The New Jersey bill adds a new prohibition not seen in any prior law that could be detrimental to job applicants and employees. Employers cannot "[i]n any way require or request that a current or prospective employee disclose whether the employee has a personal account." Were an employer to search publicly available social media content for information about an employee or applicant and discover negative information that might relate to the applicant or employee, such as racist comments or a predilection for sex with minors, the employer could not ask whether the account where the content is posted is the applicant's or employee's personal account. If the employer inquires and the applicant or employee refuses to confirm or deny whether he or she posted the offensive social media content, New Jersey's law would make it a violation for the employer to then take adverse action based on the individual's refusal to respond. In other words, the employer would be worse off if it tried to "do the right thing" and attempted to verify the authenticity of information that, if true, would lead to an adverse employment action. The New Jersey bill also has the most generous remedial scheme. The New Jersey bill confers a private right of action on applicants or employees to recover unlimited compensatory and consequential damages, and there is no administrative exhaustion requirement.

---

31 *Id.*

32 http://www.njleg.state.nj.us/2012/Bills/A3000/2878_R3.PDF. Technically, the law is not yet effective, because the Governor has not yet signed it as of the date of this writing, but the bill passed both houses of New Jersey's legislature with near unanimity—therefore, it is practically certain that the law will ultimately become effective.

6. New Mexico

On April 5, 2013, New Mexico passed a bill captioned "No Social Media Access for Employers."[33] The law provides that "[i]t is unlawful for an employer to request or require a prospective employee to provide a password in order to gain access to the prospective employee's account or profile on a social networking web site or to demand access in any manner to a prospective employee's account or profile on a social networking web site." The law does not define "employer" or "prospective employee" but does define "social networking website" to mean "an internet-based service that allows individuals to: (1) construct a public or semi-public profile within a bounded system created by the service; (2) create a list of other users with whom they share a connection within the system; and (3) view and navigate their list of connections and those made by others within the system." Importantly the law applies only to individuals who are "***prospective employees***," *i.e.* applicants for employment, not current employees. The law does not prohibit employers from accessing any information in the "public domain" although it does not define that term. The New Mexico law contains no remedial provisions or provide for a private right of action.

7. Utah

On March 26, 2013, Utah enacted the "Internet Employment Privacy Act," ("IEPA"), effective May 14, 2013.[34] The IEPA generally prohibits all employers from requesting an employee or an applicant for employment to disclose a username and password, or a password that allows access to the employee's or applicant's "personal Internet account." It also prohibits employers from retaliating against an employee or applicant for employment for refusing to disclose their username or password to their "personal Internet account."

The law has a broad investigation exception. It permits employers conducting an investigation to require employees to share content on their personal Internet accounts, where the investigation is related to workplace misconduct, legal compliance, or unauthorized transfer of the employer's proprietary, confidential, or financial information, and the employer has specific information that activity on the employee's personal Internet account is involved. Relatedly, the law expressly permits employers to discipline an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal Internet account without the employer's authorization.

Notably, internet accounts created, maintained, used, or accessed by an employee or applicant for business-related communications or for a business purpose of the employer are not covered by the law's prohibitions. For instance, if an employer asks an employee to create or use an existing business LinkedIn account to search for job applicants, the employer could freely obtain the password or username to that account. Moreover, from the plain language of the law, it would appear that if an employee admitted that he or she was using an account originally created for personal use for business-related communications with colleagues, the account might lose protection.

The IEPA crates a private right of action for aggrieved individuals, but the available remedy is limited—"if the court finds a violation of this chapter, the court shall award the aggrieved person not more than $500."

C. Comparing and Contrasting Coverage of State Laws to Date

The password protection laws enacted to date overlap, but also contradict each other, in a variety of ways, as described below:

Laws Restricting Employers from Seeking Applicants' Social Media Log-In Information: Every law enacted to date (Maryland, Illinois, California, Michigan, Utah, New Mexico, and New Jersey) prohibits employers from seeking applicants' social media login information.

Laws Restricting Employers from Seeking Current Employees' Social Media Log-In Information: Every law enacted to date except for New Mexico (Maryland, Illinois, California, Michigan, Utah, and New Jersey) prohibits employers from seeking current employees' social media login information.

Laws Prohibiting "Shoulder Surfing" or Other Access to Employee Social Media Even Absent Login Information: Several states' laws (Illinois, California, Michigan, and New Jersey) go beyond the original stated purpose of these laws to prohibit requiring an employee to allow even informal access to social media or other internet information.

---

33 http://www.nmlegis.gov/Sessions/13%20Regular/final/SB0371.pdf.

34 http://le.utah.gov/~2013/bills/hbillenr/HB0100.pdf (will create Utah Ann. Code §34-48-101 *et. seq.*) The same Bill also enacted the "Internet Postsecondary Institution Privacy Act," covering postsecondary institutions' conduct toward students' internet accounts, which is not addressed herein.

Laws with Exceptions to Their Prohibitions for Employer Investigations: California and Utah have at least explicitly allowed some exceptions to their prohibitions in cases of employer investigations, although the scope of those exceptions differs by law. Michigan does not contain an explicit exception for investigations, but does not prohibit an employer from asking an employee to help the employer view content in another employee's or in an applicant's personal account, which will help Michigan employers conduct investigations despite the law. New Mexico's law does not apply to current employees, so this should not be an issue for most investigations.

Laws Providing for a Private Right of Action: Only a few laws provide for a private right of action and some require exhaustion of other steps before suing—Illinois (but only after an administrative exhaustion requirement); Michigan ($1000 damages cap plus attorneys' fees, but requires notice to employer and opportunity to correct before bringing suit); Utah ($500 damages cap); New Jersey (unlimited damages).

The laws truly create a "patchwork" of requirements and exemptions from requirements that, as further described below, cause significant challenges for multi-state employers. As additional laws are considered and no doubt passed by other states, the potential for confusion and administrative difficulty will only increase.

Legal and Practical Challenges Plague Employers as a Result of Social Media Password Protection Legislation

Legislators appear to have been so swept up by the media frenzy over the perceived, but unproven, injustice of private employers asking for personal social media log-in credentials that they drafted legislation with little consideration of employers' legitimate interests. Several of the laws will impede employer's ability to investigate potential workplace violence incidents revealed by posts in a personal social media accounts and work-related harassment and cyberbullying conducted through personal social media accounts. Even where the laws have an exception for workplace investigations, their terminology will breed confusion as social media technology changes and the laws' terminology become outdated.

A. Difficulties Presented When Investigating Alleged Employee Misconduct

1. Workplace Violence Investigations May Be Hampered.

In Illinois, Maryland and New Jersey, employers could not fully investigate potential workplace violence revealed in a social media post. These password protection laws would prohibit an employer from going to the source if an employee were to report that a coworker had posted on his restricted-access social media account the following: "I'm so angry I want to kill my boss" or "I hate work. I'm gonna blow the place up." Thus, the employer would lose the benefit of critical information, such as the context of the post and other indicia of the seriousness of the threat revealed by the actual content.

It is unclear whether the survivors of murdered employees could hold the employer legally responsible in this scenario for failing to investigate the incident adequately, but no one wants to see a test case. Critically, these examples are not hypothetical hyperbole. According to one of the foremost experts in the field of workplace violence, James Turner, Ph.D., it is not uncommon for those planning to commit murder to provide clues to their homicidal intent in Internet postings before they pull the trigger. For example, a gunman wrote a series of posts to an online bulletin board, the last of which stated "It's time," before murdering seven people in a Tokyo shopping mall.[35] Another gunman posted "I wonder if I'd make the six o'clock news if I just starting popping people off" before killing three guards and wounding a fourth on the University of Alberta campus.[36]

2. Workplace Harassment Investigations May Be Impaired

The Illinois, Maryland and New Jersey laws also thwart investigations into workplace harassment. It would be naïve to believe that the bullying which used to happen on the shop floor or in the break room has not moved to social media. The California Court of Appeals recently affirmed

35 Norimitsu Onishi, *Man who killed 7 in Tokyo left online warnings*, N.Y. TIMES (June 9, 2008), http://www.nytimes.com/2008/06/09/world/asia/09iht-09tokyo.13575210.html.

36 Michelle McQuigge, *Chilling Facebook comment preceding armed guard murders stokes employee online privacy debate*, THE CANADIAN PRESS (June 23, 2012), http://news.nationalpost.com/2012/06/23/chilling-facebook-comment-preceding-armed-guard-murders-stokes-employee-online-privacy-debate/.

a jury's verdict holding an employer responsible for its employees' bullying of a coworker with a disfigured hand. The court relied heavily on coworkers' scathing blog posts that referred to the employee as "The Claw" and ruthlessly ridiculed him because of his disability.[37] In the California case, the employee was able to discover and report the bullying to his employer because the blog posts were public. Password protection laws, however, would throw a cloak of secrecy around this type of illegal conduct when conducted through a restricted-access social media account.

As with the workplace violence scenario, it is unclear whether an employer could be held responsible for work-related harassment that is inaccessible to the employer. The plaintiffs' bar can be expected to try. Putting aside legal liability, workplace harassment and threats of workplace violence that are visible to co-workers, but invisible to the employer, will have intangible costs for the workplace, such as undercutting employee morale, causing tension among coworkers, and distracting employees from their work. Given the absence of any proof that private employers are asking for social media log-in credentials, there is no justification for legislatures to impose on employers those costs or the potential liability arising from an inadequate investigation of employees' unlawful work-related social media conduct.

B. Complications Regarding the Vetting of Applicants

While the risks arguably are not as serious, the application process still can present situations where an employer justifiably seeks access to content posted on a restricted-access social media account. For example, if a current employee informed her human resources manager that she had seen content on an applicant's "friends-only" Facebook page that raises serious questions about the applicant's suitability for employment with the employer, the employer should be able to gain access to that information whether by asking the applicant or the employee for log-in credentials, for permission to "shoulder surf," or for a hard copy or screen shot of the content in question.

One of the most frequent reasons employers cite for conducting Internet background searches, and social media searches is fear of a negligent hiring claim, particularly for an employee who subsequently engages in violence. The common law of practically every state recognizes the tort of negligent hiring, whereby an employer is responsible for an injury caused by the negligent or intentional conduct of one its employees.[38] In a negligent hiring case, the injured plaintiff must show that the employer knew or should have known that the employee was not fit to be hired for the job because it was foreseeable that the employee might harm someone like the plaintiff. It is unclear whether an employer could invoke a social media password protection law as a defense to a claim that the employer conducted an inadequate investigation into an applicant who as an employee engaged in workplace violence.

C. Technological Advances and Changes Blur the Public and Private When It Comes to Social Media Profiles and Accounts

The password protection laws speak of "passwords" and employer "access" to private social media accounts, but what does "access" to "private" information mean when the social media websites themselves keep changing the privacy settings and, hence, the definition of when content is private versus public?

Most social network sites, like Facebook, give users the ability to control how their information is shared amongst users. For example, Facebook's privacy policy[39] and MySpace's privacy policy[40] both contain options such as allowing users to choose who can view their profile, post on their wall, or see their personal information. While Facebook and MySpace have policies that allow users control over who views their information, Twitter seems to take the opposite approach. Twitter's privacy policy states:

> Our Services are primarily designed to help you share information with the world. Most of the information you provide to us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you

37 *Espinoza v. County of Orange*, No. G043067 (consol. with G043345) (Cal. Ct. App. 2012).

38 *See* Lex K. Larson, *State-by-State Analysis, Employment Screening* (MB) pt. 1, ch. 11 (2010).

39 http://www.facebook.com/about/privacy/ (last visited April 22, 2013). Sharing and Finding You On Facebook Section states: "Always think before you post. Just like anything else you post on the web or send in an email, information you share on Facebook can be copied or re-shared by anyone who can see it."

40 MySpace Privacy Policy, MySpace, http://www.myspace.com/index.cfm?fuseaction=misc.privacy (last visited April 22, 2013).

> create, the people you follow, the Tweets you mark as favorites or Retweet and many other bits of information. Our default is almost always to make the information you provide public...[41]

Twitter's approach to privacy may be attributable to the fact that it is more of a blogging site than a social networking site, like Facebook, LinkedIn or MySpace. While Twitter allows users to share messages with their "followers," the default privacy setting on Twitter is that all messages posted using the site are public and available to any user of Twitter.[42]

The next logical question is whether users truly have knowledge or a clear understanding of the privacy policies or settings applicable to their own social media accounts. In a prepared statement to Congress, Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, remarked:

> I have listened to Facebook experts discuss the privacy settings who quickly became confused. I even heard Facebook founder Mark Zuckerberg describe the new changes to his company's privacy settings only to learn, unexpectedly, that some of his college photos were now available to "everyone." I am convinced that not even Facebook understands how its own privacy settings operate. And if Facebook cannot understand the privacy settings, how can the users?[43]

Just a few months ago, on December 26, 2012, Mark Zuckerberg's sister, Randi, who is the former Marketing Director for Facebook, fell victim to the den of confusion that is Facebook's privacy policy when a photo she posted for her Facebook "friends" was shared publicly over Twitter. [44]Ms. Zuckerberg expressed her displeasure with the photo being shared publicly on Twitter: "Not sure where you got this photo. I posted it to friends only on FB. You reposting it to Twitter is way uncool," Zuckerberg tweeted to @cshweitz, according to a screenshot of the tweet grabbed by BuzzFeed.[45] The Twitter user was a "friend of a friend" of Ms. Zuckerberg and claimed the photo popped up on her News Feed.[46] Turns out, photos that have been tagged are visible to friends of every user in the photo, not just the friends of the user who posted it. It is one of the "loopholes" in Facebook's privacy policy.[47]

As the number of social networks grows and the number of individuals utilizing the services increases at record speeds, questions remain and new questions arise. For example, is an employer representative sending an employee a "Friend" request on Facebook the equivalent of asking for a password? Or what if the employee's Facebook privacy settings were such that any "Friend" of a "Friend" could also access and view her wall (even if that was not her intent)?

Assume that, using this privacy configuration (and with no knowledge of whether the employee knew of this additional layer of access or not), an employer representative who was a "Friend" of a "Friend" accessed the employee's wall inadvertently and read offensive posts made by the employee about the company because such posts appeared on her Facebook "News Feed"? Assume the supervisor then completely and voluntarily showed her superiors the posts via the access she had through the "Friend" of the "Friend" of the employee. Could such access by the employer be deemed prohibited access within the meaning of any of these laws simply because the employee did not intend the employer to have access and only intended to grant access to her "Friends" (which the employer was not)? Or was the employer's access permissible—or as the Illinois law states: "in the public domain"—because it occurred via mechanisms in the Facebook privacy settings which were in effect for the applicant's account (whether or not the employee was aware the employer could have such access)?

In sum, as the technology changes and advances, the terminology used in the recently enacted password protection laws may become obsolete or inapplicable rendering employer compliance with these laws difficult, particularly where the line between private and public becomes blurred by the technology itself.

---

41 Twitter Privacy Policy, Twitter, http://twitter.com/privacy (last visited April 22, 2013).

42 *Id.*

43 Online Privacy, Social Networking and Crime Victimization: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 111th Cong. 5 (2010) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center).

44 http://www.latimes.com/business/technology/la-fi-tn-randi-zuckerberg-facebook-privacy-20121226,0,4097460.story.

45 *Id.*

46 *Id.*

47 *Id.*

Could a Model Federal Statute Alleviate These Concerns?

As discussed herein, no password protection laws are needed at all. However, there does not appear to be any end in sight to the rash of legislation, as Utah and New Mexico joined New Jersey in enacted such legislation only last month. Legislation is needed at the federal level that will pre-empt all state legislation covering the subject matter to prevent the patchwork of state laws from becoming even more complex and even more unwieldy.

In addition to express preemption, federal legislation should include the following elements, and these elements should provide a model for future state legislation:

1. Any model legislation should **solely** prohibit employers from **requiring** (not merely "requesting") as a condition of employment that applicants or employees: (a) disclose social media log-in credentials to accounts belonging to the employee or applicant; or (b) access personal social media accounts belonging to the employee or applicant in the employer's presence, (*i.e.*, require the applicant or employee to allow the employer to "shoulder surf").
2. "Social media" would be defined to include only personally owned and operated social media services and accounts. All employer owned and operated accounts would be excluded.
3. As provided for in California's law, employers would be permitted to ask an employee to divulge personal social media content (but not log-in credentials) when the employer reasonably believes the content is relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations.
4. As provided by Utah's law, employers could request log-in credentials when they reasonably believe that an employee has transferred the employer's confidential business information to the employee's otherwise private accounts.
5. Also as provided by Utah's law, the employee would waive any protections under the law where the employee used an otherwise private account for business-related purposes, or accessed the account using the employer's electronic resources or an employer-owned electronic device.
6. The law would also prohibit employers from taking an adverse employment action against an employee or applicant for refusing to comply with any demand that the statute makes unlawful.
7. The law would provide for immunity for employers in tort actions based on claims that the employer should have required an applicant or employee to divulge information related to their personal social media accounts.

Littler Mendelson's Workplace Policy Institute (WPI) is devoted to developing and influencing workplace legislative and regulatory developments at the federal and state levels. WPI provides the employer community with advocacy services, including litigation support. In addition, WPI closely monitors important labor, employment, and benefits policy initiatives and provides clients, trade associations, and policymakers with timely and thoughtful analysis of the practical implications of such proposals.If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, Mr. Gordon at pgordon@littler.com, Ms. Spataro at aspataro@littler.com, or Mr. Simmons at jwsimmons@littler.com.