Phishing on Facebook: Do You Ask Job Applicants

There are only a handful of reported instances where employers have requested that applicants or employees turn over their social media passwords. Nevertheless, this practice has generated scathing headlines in several media outlets. This article examines business and legal implications that arise when employers request applicants' and employees' login information.

BY LILY M. STRUMWASSER

for Their Social Media Passwords?

While reviewing applicants for an available position at your company, one candidate's resume sparks your interest. You enter his name into Google, which leads to his LinkedIn, Twitter, MySpace, and Facebook profiles. The profiles reveal little, as the applicant has blocked his profiles from public view. Nevertheless, he is well qualified for the position, so you invite him in for an interview. You begin by asking questions about his experience and references. Then, you ask him to provide you with his Facebook username and password so you can view his restricted profile. You believe that getting a glimpse of the applicant's private life will help you evaluate if he is a good fit with the company.

"Social Media Creates Huge New Portals for the Mass Disclosure of Private Information"[1]

In 2012, an interviewer asked Justin Bassett the same question when he interviewed for a statistician position. Outraged by the interviewer's invasive question, Bassett withdrew his application. The Associated Press reported Bassett's story, and it went viral. The blogosphere lit up with discussion regarding employers asking potential employees for social media login information.

Facebook's chief privacy officer responded with a statement condemning the practice. Later that week, Sens. Richard Blumenthal (D-Conn.) and Charles Schumer (D-N.Y.) wrote to the U.S. Department of Justice (DOJ) and the Equal Employment Opportunity Commission (EEOC) emphasizing their concern that employers who obtain social media login information from applicants could access private information "under the guise of a background check [that] may simply be a pretext for discrimination."[2] The senators asked the DOJ and EEOC to investigate whether asking for Facebook passwords during job interviews violates federal law.

Other federal legislators rushed to introduce laws that prohibit employers from requiring applicants and employees to provide access to their social media accounts. On April 27, 2012, Rep. Eliot Engel (D-N.Y.) introduced the Social Networking Online Protection Act (SNOPA), which calls for a nationwide ban on the practice of requesting access to employees' and applicants' personal accounts. Twelve days later, the Password Protection Act (PPA) of 2012 was introduced in the Senate and a parallel bill was introduced in the House. If passed, the PPA will "prohibit employers from taking adverse actions against employees for refusing to disclose such passwords and [make] employees ... eligible to receive compensatory damages and injunctive relief" in case of violations.[3]

With this federal law pending, 12 states—Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Mexico, Oregon, Utah, Vermont, and Washington—have enacted laws that prohibit employers from requesting employees or job applicants to provide login information for social media accounts. These bills attracted broad, bipartisan support. Thirty-six additional states have introduced similar legislation or have legislation pending. Although unique to each state, in general, each law prohibits employers from requesting passwords to employees' or applicants' personal social media accounts such as Facebook, LinkedIn, Twitter, and MySpace.

If you, as an employer, ask applicants or employees to provide their social media passwords, this article pertains to you. If your company is located in a state shaded green in the map

below, this practice is illegal. If your company is located in a state shaded blue in the map below, legislation is pending that may make asking for private login information illegal.

Even if you are not located in a "protected password" state, are you aware of the negative media attention and lawsuits that may result from asking employees or job applicants for their login information? If you are an attorney representing employers, are your clients up to date on this issue? Do your clients have written policies regarding requesting applicants' and employees' social media passwords?

This article examines business and legal implications that arise when employers request applicants' and employees' login information, discussing everything from the negative press associated with such practices, legal pitfalls, and recommendations to employers.

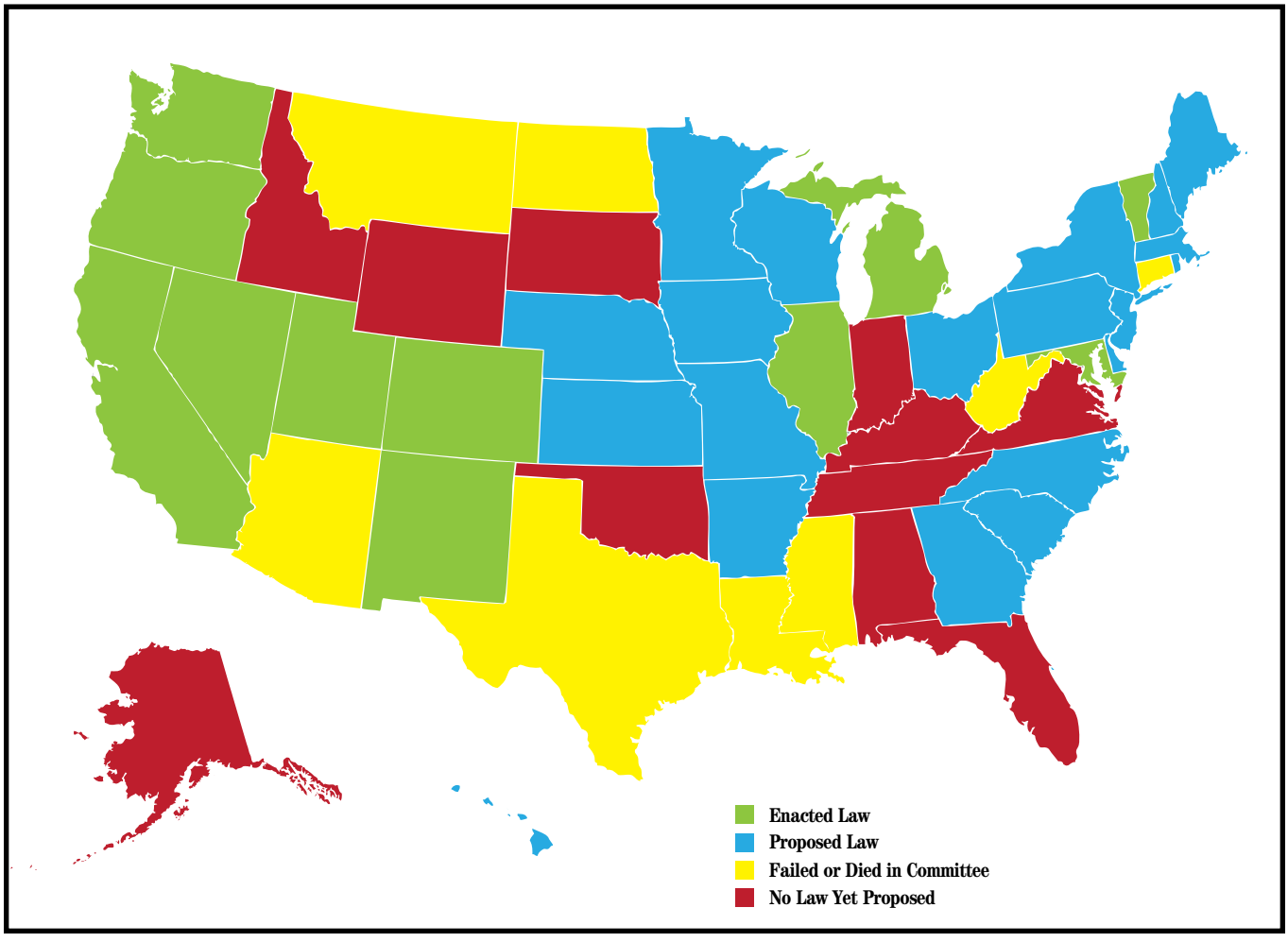
"Information That You Can't Ask for in a Job Interview—Go on the Web, It's All There"[4]

Historically, pre-employment screening techniques consisted of written applications, questionnaires, interviews, and reference checks. Advancements in technology spurred the development of additional forms of screening, such as criminal and credit history checks. Facebook and other social media outlets also created a new avenue for performing this due diligence. People display their digital identities for friends, family, and even strangers to view. More than 1 billion people worldwide have registered accounts with Facebook, and their profiles can reveal their name, country, zip code, gender, date of birth, religion, education, sexual preference, marital status, political preferences, interests, and activities. In addition, many Facebook users have posted or are tagged in pictures or videos.

Despite recent legal turmoil, many employers use Facebook and other social media outlets as a screening tool for job applicants. A recent study commissioned by Microsoft Corporation found that nearly 80 percent of individuals hiring and recruiting use the Internet to investigate candidates.[5] Another report by NBC News indicated that more than 77 percent of employers find information about candidates online, and 35 percent have dismissed candidates based on these findings.[6] As pointed out by one employment litigation attorney, "[i]t's unlikely that a job applicant would ever attach provocative photos, detailed descriptions of sexual escapades, or a list of hobbies that includes funneling beer and recreational drug use on [a] resume. But with just a few clicks of the mouse, you can find out all sorts of revealing information about potential candidates."[7]

Many employers want to know that their hires possess sound judgment and discretion because new employees often gain access to sensitive materials and information. Employers also look for employees who will "fit" well with the organization. One survey revealed that employers ranked an applicant's attitude as the most important factor when conducting interviews.[8] Additionally, employers want to ensure they do not hire someone whose actions can render the employer liable under a negligent hiring theory.

Thus, many employers use social media to obtain a realistic view



of the applicant. But, when applicants block their profile from the public's view, it inhibits employers' research.

Requesting Social Media Passwords—It's Bad for Business

There are only a handful of reported instances where employers have requested that applicants or employees turn over their social media passwords. To date, no court has issued a decision on this issue. Nevertheless, this practice has grabbed headlines in *Forbes*, Fox News, CNN, and many other media outlets and blogs. The public has launched salvos of complaints against the few employers who ask—or even require—applicants or employees to provide their personal login information. The media attention has triggered responses from employers, lawyers, and legislators across the nation. The pitfalls of this practice are apparent: bad press is bad for business. The discussion that follows provides a brief overview of syndicated news outlets that have reported stories about employers requesting private passwords from employees and job applicants.

In 2006, Fox News reported that the Sheriff's Office in McLean County, Ill., asked applicants to sign into their social media accounts during interviews so it could screen private websites. The interviewer defended his practice and explained that the office used the information obtained from the social media pages to "weed out those who have posted inappropriate pictures, had inappropriate relationships with people who are underage, or engaged in other illegal behavior."[9]

In 2009, ABC News reported that the City of Bozeman, Mont., required all applicants to provide login information to social networking sites of which they were members, including Internet-based chat rooms, social clubs, or forums, which included Facebook, Google, Yahoo, YouTube.com, or MySpace. The city's assistant manager explained that the process was a component of a thorough background check.

In 2010, National Public Radio aired an interview with Robert Collins, a prior Maryland Department of Public Safety and Correctional Services employee who was asked to hand over his login information upon returning from leave. The interviewer told Collins that the agency needed his Facebook password so it could verify that he was not affiliated with any gangs. Collins complied with the request and later explained that he did so because he needed the job to feed his family; he felt like he "had no choice" but to agree with the demand.[10]

In 2011, NBC News reported that the superintendent of a Michigan school district asked Kimberly Hester, a teacher's aide, for her Facebook password because Hester's Facebook page reportedly contained a photo of a co-worker with her pants around her ankles. When Hester refused to turn over her Facebook password, the school suspended her employment.

After the media scrutinized these incidents, many of the above-mentioned employers discontinued their practice of requesting personal login information from employees and applicants. Nevertheless, the legal implications of these employment practices are looming large.

High-Tech Discrimination

Even in the absence of statutory authority, there are several legal risks associated with employers requesting applicants' and employees' login information. The practice opens a "whole Pandora's box of issues."[11] The following discussion provides employers with an overview of the types of lawsuits they may face under existing laws if they ask for private login information.

Liability Under Antidiscrimination Laws

Requesting social media passwords from applicants and employees opens the door to potential claims under Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act (ADA), the Age Discrimination in Employment Act (ADEA), and various state laws. Title VII forbids discrimination against applicants and employees based on race, color, religion, sex, or national origin. Rather, employment decisions must be grounded in legitimate, non-discriminatory motives. The EEOC's Guide to Pre-Employment Inquiries states that employment questions concerning the protected status of an applicant violate Title VII "unless the information is needed to judge an applicant's competence or qualification for the job in question."[12]

The ADA prohibits discrimination against qualified individuals "who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires."[13] It goes a step further than Title VII by prohibiting employers from asking applicants about the existence, nature, or severity of a disability. According to the EEOC, this "helps ensure that an applicant's possible hidden disability (including a prior history of a disability) is not considered before the employer evaluates an applicant's non-medical qualifications."[14]

The ADEA forbids discrimination against individuals age 40 or older. Like Title VII and the ADA, the ADEA contains an exception to the prohibition of age-based discrimination, which allows an employer to consider an applicants' or employees' age if it is a *bona fide* occupational qualification (BFOQ) that is reasonably necessary for the normal operation of the business. Additionally, several state and local laws prohibit employers from making employment decisions based on sexual orientation, marital status, pregnancy, political affiliation, genetic affiliation, and gender identity.

It is easy to see how applicants or employees could post pictures or information describing their race, color, religion, sex, national origin, disability, age, sexual preference, or genetics on their social media accounts. For example, a woman may post pictures of her seven children on her Facebook page. Someone else could post pictures celebrating a 50th birthday. Another applicant may have photos of excessive drinking. These pictures could raise issues of sex, age, and disability discrimination.

Against this backdrop, the risk of viewing applicants' and employees' social media profiles is clear. Even if employers who solicit login information do not make hiring decisions based on the online content, they may still face discrimination lawsuits. The applicant could easily point to the employer's practice of viewing social media pages to prove constructive knowledge of the applicant's protected status and the employer's discriminatory intent. At the very least, this presumption could create liability if a lawsuit is filed. Plaintiffs can also use evidence of discriminatory intent to extract large settlements or awards if their case is taken to trial.

Privacy Rights

Employers who request applicants' and employees' login information may also be in violation of the Electronic Communications Privacy Act of 1986 (ECPA) and the Stored Communications Act

(SCA). Title I of the ECPA, commonly referred to as the Wiretap Act, prohibits the unauthorized interception of wire, oral, and electronic communications. Title II prohibits unlawful access to a person's electronic communications without that person's authorization.

In *Pietrylo v. Hillstone Restaurant Group*, Brian Pietrylo and Doreen Marino created a MySpace group[15] where they posted negative and offensive remarks regarding restaurant management. The privacy settings on the MySpace group blocked upper management from viewing the content. One manager later learned of the MySpace group when an employee, Karen St. Jean, showed him a posting from it. This manager, in turn, told another manager about the MySpace group. St. Jean later provided her login information to both managers, granting them access to the MySpace group and its offensive content. Based on the MySpace postings, management fired Pietrylo and Marino.

Pietrylo and Marino responded by filing suit in the U.S. District Court for the Northern District of New Jersey. They alleged, among other things, that the employer violated the SCA and the parallel New Jersey Wiretapping Act by obtaining unauthorized access to private employee communications. The plaintiffs relied on St. Jean's testimony that, "she felt she had to give her password" to the managers because she worked for them.

The jury dismissed several of the claims, but found that the employer violated the SCA, and offered modest compensatory damages. The jury's verdict hinged on its finding that the managers were not authorized to enter the MySpace group.

Like the employees in *Pietrylo v. Hillstone Restaurant Group*, employees and applicants who provide employers with their social media login information may have a viable argument under the SCA that requesting the information was unauthorized and therefore unlawful. Employers defending similar cases can attempt to distinguish *Pietrylo* by relying on the fact that the court found that the employer violated the SCA based on one subjective statement by an employee-witness. Notably, "a different court might well apply an objective test and reach a different result."[16]

Another Employer Minefield—Social Networks' Terms of Service

Employers who request that applicants and employees turn over their social media passwords must sidestep another minefield: social media websites' terms of service. For example, section 4.8 of Facebook's statement of rights and responsibilities states that users "cannot share your password . . . let anyone else access your account, or do anything else that might jeopardize the security of your account."[17] To date, Facebook has not brought a lawsuit against an employer who requested login information, and the grounds for such a lawsuit remain unclear. Nevertheless, Facebook's chief privacy officer warned employers that Facebook will "take action to protect the privacy and security of our users, whether by engaging policymakers, or where appropriate, by initiating legal action."[18]

Suggestions for Employers

This section proposes four straightforward suggestions for employers to avoid lawsuits and improve hiring practices. First, employers should adopt or update social media policies. Second, employers should be prepared to defend their hiring practices in court. Third, employers should train employees about relevant social media laws. Fourth, employers should understand the varying extent of different states' laws.

Update Social Media and Password Policies

It is suggested that employers create formal written policies clearly stating that managers, supervisors, and human resource staff *cannot* request applicants' or employees' social media passwords. This blanket "don't ask" policy will protect employers from the assortment of laws addressing access to applicants' and employees' social media accounts. Remember though, looking at content available to the public domain is fair game. The impact of social media in the workplace is a constant evolution of federal and state laws. So, play it safe. Protect your company by implementing a policy; have it reviewed by your lawyer; consistently enforce it; and include it in the company handbook.

If You Must Ask, Prepare Yourself to Defend Your Practice in Court

Some employers may have a legitimate business reason for viewing applicants' and employees' private websites. In that instance, if employers request private login information, they should be prepared to defend the practice as a business necessity. For example, the Financial Industry Regulatory Agency (FINRA) and the Securities and Exchange Commission (SEC) have made it clear that they need to monitor employees' social media accounts to maintain security in the finance industry. While some of the states' social media laws carve out exceptions for employers subject to FINRA's compliance regulations, other states' laws do not. No court has addressed the conflicts between state statutes and federal securities laws. This issue is just beginning to develop, so employers should stay tuned.

Keep Employees Informed Through Training Sessions

Next, employers should reinforce these policies with training. Employees will more likely follow the company policy if they understand the potential legal risk. Employers can deliver training through formal meetings or through e-mails notifying employees of the updated policy and the reasoning behind it. Requiring employees to acknowledge receipt of this policy in writing may help ensure that they have reviewed the new policy. Employers should also remind employees periodically about the company policy. Furthermore, it is suggested that employers consistently enforce the policy.

Understand Local Laws

In general, states that have enacted social media legislation restrict employers from requesting usernames and passwords for social networking sites such as Facebook, LinkedIn, Twitter, and MySpace from applicants and employees. However, there are subtle inconsistencies among the states' laws. Differences in states' laws typically turn on the types of social media it covers, the nature of the prohibited conduct, and the exceptions to the prohibitions.[19] Companies that conduct business in more than one state should be aware of the differences between different states' laws to "avoid inadvertently running afoul of them."[20]

Conclusion

Phishing social media websites can likewise lead to bad press, litigation, and possibly liability. Thus, while the benefits of using social media are clear, requesting applicants' and employees' social media login information is not recommended. When in doubt, contact your attorney. ⊙

Lily Strumwasser graduated from The John Marshall Law School in May 2013. She held a judicial externship with Hon. Charles Kocoras of the U.S. District Court for the Northern District of Illinois. Strumwasser also served as the executive student articles editor of The John Marshall Law Review *and is a member of the school's Board of Trustees Student Advisory Committee. Strumwasser will join the Chicago office of Seyfarth Shaw LLP in the area of labor and employment law. She can be reached at lstrumwasser@seyfarth.com. The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

Endnotes

[1]Nathan J. Ebnet, *It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, 97 Minn. Law Rev. 306, 318 (2012).

[2]On Mar. 25, 2012, Rep. Blumenthal issued a press release, which stated that "a ban on this practice is necessary to stop unreasonable and unacceptable invasions of privacy. An investigation by the [DOJ] and [EEOC] will help remedy ongoing intrusions and coercive practices, while we draft new statutory protections to clarify and strengthen the law. With few exceptions, employers do not have the need or the right to demand access to applicants' private, password-protected information." Richard Blumenthal, *Blumenthal, Schumer: Employer Demands for Facebook and E-mail Passwords as Precondition for Job Interviews May Be a Violation of Federal Law; Senators Ask Feds to Investigate* (Mar. 25, 2012), 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.

[3]Lawmakers Rush to Ban Employers from Demanding Facebook Passwords, Morrison and Foerster Social Media Newsletter, Vol. 3, Issue 3 at 3 (June 2012), www.mofo.com/files/Uploads/Images/120605-Socially-Aware.pdf. If passed, the PPA will amend the Computer Fraud and Abuse Act. *Id.*

[4]Pam Belluck, *Young People's Web Postings Worry Summer Camp Directors*, N.Y. Times, June 11, 2006 at 1. "When Facebook first launched, it was only available to Harvard students, but quickly expanded to Stanford, Columbia, and Yale. Today, Facebook is open to anyone around the world." *Id.*

[5]Cross-table, Online Reputation in a Connected World 6 (Jan. 2010), www.gomicrostoft.com/?link-id=9709510; What Your Employer Wants with Your Facebook Password, Shutterstock, March 20, 2012.

[6]*College Students Using New Web Site Could Have Their Personal Information Read by Prospective Employers* (NBC television broadcast May 13, 2006) (transcript available at 2006 WLNR 8296767).

[7]*What You Won't See on a Resume*, 18 No. 12 Ga. Emp. L. Letter (Ford, Harrison LLP), July 2006, at 5.

8Benjamin Belcher *et al.*, *Regulation of Information in the Labor Market: What Employers May Learn About Prospective Employees*, 21 Comp. Lab. L. & Pol'y J. 787, 787 (2000).

[9]Chris Leh, *Though Not Yet Banned, Requiring Social Media Information Is a Bad Idea*, Littler Mendelson P.C. (Mar. 27, 2012), www.littler.com/publication-press/publication/though-not-yet-banned-requiring-social-media-information-bad-idea.

[10]Nick Madigan, *Officer Forced to Reveal Facebook Page*, The Baltimore Sun (Feb. 23, 2011), articles.baltimoresun.com/2011-02-23/news/bs-md-ci-officer-facebook-password-20110223_1_facebook-page-facebook-password-privacy-protections (explaining that he "felt like if I didn't comply completely with the process I wouldn't get my job back, that I would no longer be considered for reinstatement to my position ... I felt like I was being treated like a person who had committed a crime, and that my whole life was being scrutinized under a microscope.").

[11]Allison Grande, *Facebook Wants Employers Out Of Workers' Profiles*, Law 360 (Mar. 23, 2012), www.law360.com/articles/322513/facebook-wants-employers-out-of-workers-profiles.

[12]Sarah Crawford, *Lawyers Committee for Civil Rights Under Law: Employer Use of Credit History as a Screening Tool*, U.S. Equal Employment Opportunity Commission (Oct. 20, 2010), www.eeoc.gov/eeoc/meetings/10-20-10/crawford.cfm.

[13]42 U.S.C. § 12111 (1994).

[14]*Equal Employment Opportunity Comm'n*, Notice No. 915.002, ADA Enforcement Guidance: Pre-Employment Disability-Related Questions and Medical Examinations 1 (1995).

[15]2009 U.S. Dist. LEXIS 88702 at *2. The employees called the MySpace page the "Spec-Tator," and it could only be accessed by a user with a password to the account. *Id.* The employee who gave the manager the MySpace password said that she "felt that [she] probably would have gotten in trouble" if she did not turn over the password. *Id.*

[16]Chris Leh, *Though Not Yet Banned, Requiring Social Media Information Is a Bad Idea*, Littler Mendelson P.C. Publications (Mar. 27, 2012), www.littler.com/publication-press/publication/though-not-yet-banned-requiring-social-media-information-bad-idea.

[17]*Id.*

[18]Staff Writer, *Facebook Privacy vs. Employers*, Business Insurance, www.businessinsurance.org/facebook-privacy-vs-employers.

[19]For a more detailed discussion regarding the differences between states' laws, see David Glockner, *Protecting Social Media Privacy in the Workplace Is Not as Simple as It Looks,* Bloomberg Law, about.bloomberglaw.com/practitioner-contributions/protecting-social-media-privacy-in-the-workplace-is-not-as-simple-as-it-looks.

[20]Abigail Rubenstein, *Varied Facebook Password Laws Could Plague Employers*, Law 360 (citing Carol A. Poplawski of Ogletree Deakins Nash Smoak & Stewart P.C.), available at www.jdsupra.com/legalnews/jdsupra-49534. Companies doing business in more than one state have to tailor their practices and policies to abide by state specific social media laws.