FIU Law Review

Volume 9 | Number 1 Article 31

Fall 2013

The Password Requirement: State Legislation and Social Media Access

Brittany Dancel
Florida International University College of Law

Online ISSN: 2643-7759

Recommended Citation
Brittany Dancel, *The Password Requirement: State Legislation and Social Media Access* , 9 FIU L. Rev. 119 (2013).
DOI: https://dx.doi.org/10.25148/lawrev.9.1.31

The Password Requirement: State Legislation and Social Media Access

Brittany Dancel[*]

I. INTRODUCTION

A certain level of social media[1] exposure is inevitable nowadays, especially in the United States.[2] Over one billion people use Facebook[3] on a monthly basis.[4] Twitter[5] sees over 340 million tweets a day.[6] YouTube[7]

* Florida International University College of Law, J.D. May 2014; Florida State University, B.S. 2011. I thank Professor Howard Wasserman for his assistance and guidance as I wrote this comment; Daniel Tarazona, for his love and encouragement; and my parents, Jose and Lesley Dancel, for their direction and support.

1 Social Media has been defined as "forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)." *Social Media*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/social%20media (last visited Mar. 4, 2013). However, statutes and sources often vary in their definitions of "social media" and "social networking." *See infra* notes 64-67, 93-95.

2 *Facebook Statistics by Country*, SOCIALBAKERS, http://www.socialbakers.com/facebook-statistics/ (last visited Jan. 19, 2013) (finding the United States is the number one country in the world in terms of the number of social media users).

3 Many websites attempt to define "Facebook" in general terms, assuming that individuals know the definition of "social networking site" or "social media." For example, one website defines Facebook as:

> The name of a social networking site (SNS) that connects people with friends and others who work, study and live around them. People use Facebook to keep in touch with friends, post photos, share links and exchange other information. Facebook users can see only the profiles of confirmed friends and the people in their networks.

Facebook, WEBOPEDIA, http://www.webopedia.com/TERM/F/Facebook.html (last visited Nov. 10, 2013). Another website states Facebook is "a social networking service that lets you connect with friends, co-workers, and others who share similar interests or who have common backgrounds." Josh Lowensohn, *Newbie's Guide To Facebook*, CNET.COM (Aug. 1, 2007, 5:17 PM), http://news.cnet.com/newbies-guide-to-facebook. *See also id.* ("Many use [Facebook] as a way to stay in touch after finishing school, or as a way to share their life publicly. What makes Facebook different from other social networks are its extensive privacy controls, its development platform, and its large and quickly growing user base. Facebook has been called the 'thinking person's' social network. Compared to many other social networks, Facebook gets new features and improvements on a regular basis.").

4 Dave Lee, *Facebook Surpasses One Billion Users as It Tempts New Markets*, BBC NEWS (Oct. 5, 2012, 4:54 AM), http://www.bbc.co.uk/news/technology-19816709; Aaron Smith, Laurie Segall & Stacy Cowley, *Facebook Reaches One Billion Users*, CNN MONEY (Oct. 4, 2012, 9:50 AM), http://money.cnn.com/2012/10/04/technology/facebook-billion-users/index.html; Geoffrey A. Fowler, *Facebook: One Billion and Counting*, WALL ST. J. (Oct. 4, 2012), http://online.wsj.com/article/SB10000872396390443635404578036164027386112.html.

5 Twitter is "a free social networking website that allows user[s] to micro-blog . . . a service for friends, family, and co–workers to communicate and stay connected through the exchange of quick, frequent answers . . . ." *See* James Bucki, *Twitter*, ABOUT.COM,

had more than 1 trillion views (around 140 views for every person on Earth) in 2011.[8]

The prominence and growth of social media in recent years has not left the legal industry unaffected. In 2012, six states—California, Delaware, Illinois, Maryland, Michigan, and New Jersey—enacted legislation that prohibits requesting or requiring an employee, student, or applicant to disclose a username or password to a personal social media account.[9] In 2013, eight additional states—Arkansas, Colorado, Nevada, New Mexico, Oregon, Utah, Vermont, and Washington—followed suit and also enacted legislation restricting employer or university access to employee, student, or applicant social media accounts.[10] In all of 2012, fourteen states introduced legislation that would restrict employers or educational institutions from requesting access to social networking usernames and passwords.[11] At the end of 2013, similar legislation was introduced or pending in an impressive 36 states.[12]

Whether social media accounts can be used as part of a hiring or

---

http://operationstech.about.com/od/glossary/g/twitter.htm (last visited Feb. 27, 2013) (internal quotations & citations omitted); *see also About*, TWITTER, https://twitter.com/about (last visited Feb. 27, 2013) ("Twitter is a real-time information network that connects you to the latest stories, ideas, opinions and news about what you find interesting. Simply find the accounts you find most compelling and follow the conversations.").

6 *Twitter Turns Six*, TWITTER BLOG (Mar. 21, 2012, 10:18 AM), http://blog.twitter.com/2012/03/twitter-turns-six.html.

7 YouTube is "a website on which subscribers can post video files." *See YouTube*, DICTIONARY.COM, http://dictionary.reference.com/browse/YouTube (last visited Mar. 4, 2013); *see also About YouTube*, YOUTUBE, http://www.youtube.com/t/about_youtube (last visited Mar. 4, 2013) ("YouTube allows billions of people to discover, watch and share originally-created videos. YouTube provides a forum for people to connect, inform, and inspire others across the globe and acts as a distribution platform for original content creators and advertisers large and small.").

8 *Statistics*, YOUTUBE, http://www.youtube.com/t/press_statistics (last visited Mar. 4, 2013).

9 *See Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, NAT'L CONF. STATE LEGISLATURES (Jan. 17, 2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx (state legislation).

10 *See Employer Access to Social Media Usernames and Passwords, 2013 Legislation*, NAT'L CONF. STATE LEGISLATURES (Oct. 23, 2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx. In 2013, ten states in total enacted new legislation. *Id.* Although already having enacted legislation for the employment setting in 2012, *see* 820 ILL. COMP. STAT. ANN. 55 / 10 (2012), Illinois's legislature took the opportunity in 2013 to pass a law that places restrictions on academic institutions. *See* 105 ILL. COMP. STAT. ANN. 75 / 10 (2014). Similarly, although already placing restrictions on higher education institutions in 2012, *see* N.J. STAT. ANN. § 18A:3-30 (West 2012), New Jersey's lawmakers passed into law restrictions on employers in 2013. *See* N.J. STAT. ANN. § 34:6B-6 (West 2013). In 2013, Illinois also amended its previously enacted Right to Privacy in the Workplace Act, which provides restrictions on employers. *See* S.B. 2306, 98th Gen. Assemb., Reg. Sess. (Ill. 2013), 2013 Ill. Legis. Serv. P.A. 98-501 (West) (amendment).

11 *See Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, *supra* note 9.

12 *See Employer Access to Social Media Usernames and Passwords, 2013 Legislation*, *supra* note 10.

admissions process is a popular issue, especially in employment law.[13] Employers are increasingly using social media sites in order to assess a candidate during recruitment and hiring. In 2011, the Society for Human Resource Management (SHRM) found that 56% of employers had used social media in the recruitment process.[14] Career Builder found similar numbers, reporting that nearly two in every five companies use social networking sites in order to research job candidates.[15] A survey cited by Time Magazine found even higher numbers, stating that an astonishing 92% of employers were using or planned to use social networks for recruiting in 2012.[16]

Employers want to utilize social media to search employees and applicants for a variety of reasons. Some claim to look for whether the candidate fits the company's corporate culture, presents him or herself in a professional manner, or meets certain job qualifications.[17] Social media can also serve as reference to learn about a candidate's work style,[18] to avoid serious legal liabilities,[19] or to protect proprietary information and comply

---

[13] *See* Scott Brutocao, *Symposium: Social Media: Issue Spotting: The Multitude Of Ways Social Media Impacts Employment Law And Litigation*, 60 ADVOC. 8 (2012); Debbie Kaminer, *Can Employers Ask Applicants for Social Media Login Information?*, N.Y.L.J. (July 27, 2012), http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202564023558&slreturn=20130019204800 ("The issue of privacy in social media, and specifically the question of whether an employer can ask an employee or job applicant for his private social media login information, is a developing area of the law.").

[14] *The Rapid Rise of Social Media as a Recruiting Tool*, WORKPLACE VISIONS: ISSUE 2 (2012), http://www.shrm.org/Research/FutureWorkplaceTrends/Documents/12-0331%20Workplace%20Visions%20Issue%202%202012_FNL.pdf. This was a significant increase from 2008, where the organization found that only about 34 percent of employers had used social media sites in the recruitment process. *Id.*

[15] *Thirty-seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey*, CAREERBUILDER.COM (Apr. 18, 2012), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2F18%2F2012&ed=4%2F18%2F2099 [hereinafter *CareerBuilder Survey*]. Also note that 11% of companies did not presently use social media to screen job applicants, but intended to implement such practices for the future. *Id.* As technology advances, these types of practices are only likely to become more prevalent.

[16] Dan Schawbel, *How Recruiters Use Social Networks to Make Hiring Decisions Now*, TIME (July 9, 2012) http://business.time.com/2012/07/09/how-recruiters-use-social-networks-to-make-hiring-decisions-now/. The study retrieved information from over 1,000 companies (mostly United States based companies) in a variety of industries. *Id.*

[17] *Career Builder Survey*, *supra* note 15.

[18] Leslie Kwoh, *Beware: Potential Employers Are Watching You*, WALL ST. J., Oct. 29, 2012, at B8, *available at* http://online.wsj.com/article/SB10000872396390443759504577631410093879278.html.

[19] Alissa Del Riego, Patricia Sánchez Abril & Avner Levin, *Your Password Or Your Paycheck?: A Job Applicant's Murky Right To Social Media Privacy*, 16 No. 3 J. INTERNET L. 1, Sept. 2012, at 18-19 (2012) ("[A] poor hiring decision can subject an employer to a malpractice claim and have serious business repercussions. An employee's poor reputation or questionable behavior can negatively affect his employer's reputation. Recent studies have shown that an individual's OSN [Online Social Networking] profile can provide an accurate window into the individual's personality and character.

with federal regulations.[20]

Students are also affected by the increased prevalence of social media in society. This is no surprise as social networking sites are most popular among younger people,[21] including 83% of people surveyed in an eighteen to twenty-nine age bracket stating they used social networking.[22] In some instances, universities and colleges want to monitor student-athletes' social media sites in order to ensure that the students are following conference and eligibility rules, as well as positively promoting the school's brand.[23]

Even with seemingly legitimate excuses for looking into personal sites, state legislatures have taken action against certain social media practices due to recent news stories of employers requiring applicants to provide their social media usernames and passwords.[24] New state bills have been enacted in order to prohibit employers and/or academic institutions from requiring this login information.[25]

This Comment addresses the provisions of recently enacted legislation restricting employers and academic institutions from requiring certain social media information. Part II (A) covers stories that led to the policy

---

Gaining this additional insight into the moral character of an applicant is instrumental for employers to assess whether contracting this applicant would be in the organization's best interest."). *See generally* Robert Sprague, *Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship*, 50 U. LOUISVILLE L. REV. 1, 7-9 (2011) (an employer can be held liable for failing to perform an adequate background investigation).

20 *See Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, *supra* note 9. *See also* Brutocao, *supra* note 13 ("Some commentators enthusiastically support such laws as necessary protections of employee privacy, while others contend they are simply another example of unnecessary regulation of employers.").

21 Facebook, for example, started as a site for university students and grew to over 800 college networks in under two years of being launched. *Newsroom Timeline*, FACEBOOK, http://newsroom.fb.com/Timeline (last visited Jan. 19, 2013).

22 Somini Sengupta, *Half of America Is Using Social Networks*, N.Y. TIMES BITS BLOG (Aug. 26, 2011, 7:30 PM), http://bits.blogs.nytimes.com/2011/08/26/half-of-america-is-using-social-networks/.

23 Pete Thamel, *Tracking Twitter, Raising Red Flags*, N.Y. TIMES, Mar. 30, 2012, at D1, *available at* http://www.nytimes.com/2012/03/31/sports/universities-track-athletes-online-raising-legal-concerns.html?pagewanted=all; Allie Grasgreen, *Watch What You Tweet*, INSIDE HIGHER ED (Aug. 27, 2012), http://www.insidehighered.com/news/2012/08/27/california-second-state-forbid-colleges-social-media-monitoring-athletes.

24 *See infra* Part II (A).

25 *See Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, *supra* note 9; *Employer Access to Social Media Usernames and Passwords, 2013 Legislation*, *supra* note 10. Comparatively, federal laws have also been considered. *See* Joanna Stern, *SNOPA: Bill to Ban Schools and Employers From Asking for Passwords*, ABC NEWS (May 1, 2012, 3:21 PM), http://abcnews.go.com/blogs/technology/2012/05/snopa-bill-to-ban-schools-and-employers-from-asking-for-passwords/ (discussing the Social Networking Online Protection Act which was introduced at the federal level); Laura Arredondo-Santisteban, *Access Denied: Proposed Federal Legislation Takes Aim at Employers Requesting Employee Social Network Passwords*, N.C. J. L. & TECH. (Sept. 4, 2012), http://ncjolt.org/access-denied-proposed-federal-legislation-takes-aim-at-employers-requesting-employee-social-network-passwords/. *See also infra* note 27 (discussing proposed federal laws).

concerns underlying the legislation. Part II (B) explores the details of the passed legislation and the scope of the currently enacted statutes. Part III explains the issues that accompany the language being chosen by lawmakers, and examines the most effective provisions of each of these laws. Part IV addresses the necessity of the currently enacted employment statutes and the arguments against their enactment.

II. THE HISTORY OF SOCIAL MEDIA PASSWORD PROTECTION LEGISLATION

A. The Media Craze that Prompted Enactment

An array of legislation[26] has been proposed, at both the state and federal levels,[27] which restricts employers' and educational institutions' access to social media login information. Maryland was the first state to enact a law prohibiting employers from asking current and prospective employees for their passwords to personal websites such as Facebook and Twitter.[28] The legislation in Maryland arose from a hiring procedure that occurred within the Maryland Department of Public Safety and

---

[26] *See Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, *supra* note 9; *Employer Access to Social Media Usernames and Passwords, 2013 Legislation*, *supra* note 10.

[27] Multiple federal laws have been proposed in order to prohibit employers and educational institutions from requesting login information to personal accounts. First, the Social Networking Online Protection Act (SNOPA) included protections both for employees and applicants, as well as for students and potential students. H.R. 5050, 112th Cong. (2d Sess. 2012). If the Act passed, it would have made it unlawful for an employer to require an employee or applicant to provide the employer with a username, password, or other information in which the employer could access an email account or a personal social networking account. *Id.* Similar to some of the state legislation, if an employee or applicant declined to provide such information, the federal law would also make it unlawful for an employer to discipline, deny, or discharge such person's employment. *Id.* This bill was re-introduced as H.R. 537 on February 6, 2013. H.R. 537, 113th Cong. (1st Sess. 2013). Second, the Password Protection Act of 2012 ("PPA of 2012") sought to prohibit employers from coercing prospective or current employees to provide access to their personal "protected computer that is not the employer's protected computer" as a condition of employment. H.R. 5684, 112th Cong. (2d Sess. 2012). Interestingly, the bill had a state of mind requirement that the employer act "knowingly and intentionally." *Id.* The PPA of 2012 also included exceptions to provide the employer with rights in governing their own equipment and other employment systems and accounts. *Id.* Introduced on May 21, 2013, the Password Protection Act of 2013 ("PPA of 2013") calls for a law with similar language, with a few revisions, including an exemption if the employer is complying with the requirements of Federal or State law, rules, regulations, or the rules of a self-regulatory organization. H.R. 2077, S. 1426, 113th Cong. (1st Sess. 2013).

[28] *See* MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); Helen A.S. Popkin, *Maryland is First State to Ban Employers from Asking for Facebook Passwords*, NBC NEWS (Apr. 10, 2012, 3:31 PM), http://www.nbcnews.com/technology/technolog/maryland-first-state-ban-employers-asking-facebook-passwords-700452; Kevin Rector, *Maryland Becomes First State to Ban Employers from Asking for Social Media Passwords*, BALTIMORE SUN (Apr. 10, 2012), http://articles.baltimoresun.com/2012-04-10/news/bs-md-privacy-law-20120410_1_facebook-password-social-media-bradley-shear; Allie Bohm, *Maryland Legislature to Employers: Hands Off Facebook Passwords*, ACLU: BLOG OF RIGHTS (Apr. 9, 2012, 4:13 PM), http://www.aclu.org/blog/technology-and-liberty/maryland-legislature-employers-hands-facebook-passwords.

Corrections.[29] Corrections Officer Robert Collins claimed that he was required to undergo a background investigation as part of the hiring process, including exposing whether he used any social media sites.[30] Consequently, the interviewer requested that Collins provide his login and password information so that the Department (according to department policy) could review Collins' Facebook profile and postings.[31] Although the Department of Public Safety and Corrections later suspended its policy,[32] and claimed that it never "demanded" this social media information be provided,[33] Collins' experience caused an exuberant number of stories in the media and, more importantly, raised a red flag at the state capitol.[34]

State lawmakers heard about the Department of Public Safety and Corrections' request for Collins' social media information, and, in reaction, Maryland's legislature passed House Bill No. 964,[35] a law for social media protection in the employment context. The Law prohibits an employer from requesting or requiring an employee or applicant to disclose a user name, password, or any other means of accessing an Internet site.[36]

---

29 Bohm, *supra* note 28; Rector, *supra* note 28.

30 Tim Persinko & Chris Gordon, *Job Applicant Required to Give Facebook Login: ACLU*, NBC WASH. (Feb. 22, 2011, 9:59 PM), http://www.nbcwashington.com/news/tech/DC-Job-Applicant-Required-to-Give-Facebook-Password-ACLU-116655589.html.

31 *Id.* The Department of Public Safety and Corrections claimed that they needed to review Collins' social media account in order to ensure that he was not affiliated with a gang. *Id.*; Sarah Perez, *Facebook Considering Laws, Legal Action Against Employers Asking for Users' Passwords*, FOX BUSINESS (Mar. 23, 2012), http://www.foxbusiness.com/technology/2012/03/23/facebook-considering-laws-legal-action-against-employers-asking-for-users/; Shannon Mcfarland, *Job Seekers Getting Asked for Facebook Passwords*, USA TODAY (Mar. 21, 2012, 10:56 AM), http://usatoday30.usatoday.com/tech/news/story/2012-03-20/job-applicants-facebook/53665606/1.

32 Helen A.S. Popkin, *Gov't Agency Suspends Facebook Password Demands*, NBC NEWS (Feb. 24, 2011, 2:12 PM), http://www.nbcnews.com/technology/technolog/govt-agency-suspends-facebook-password-demands-124883.

33 *ACLU Says Division of Corrections' Revised Social Media Policy Remains Coercive and Violates "Friends" Privacy Rights*, ACLU MD. (Apr. 18, 2011), http://www.aclu-md.org/press_room/30. The Department of Public Safety and Corrections claimed that Collins' decision as to whether to provide his social media information was "voluntary." *Id.*

34 The Maryland legislature drafted its bill following the story about Collins. *See* H.B. 964, Gen. Assemb., 430th Sess. (Md. 2012), 2013 Md. Laws Ch. 234. The story is listed in the bill's Fiscal Policy Note background section, recognizing Collins' story as part of its purpose in enacting the law. *See* DEP'T LEGIS. SERVS., FISCAL & POL'Y NOTE, H.B. 964, Gen. Assemb., 430th Sess. (Md. 2012).

35 H.B. 964, Gen. Assemb., 430th Sess. (Md. 2012), 2013 Md. Laws Ch. 234. *See* MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012) (current statutory code).

36 *Id*. The statute reads:

> FOR the purpose of prohibiting an employer from requesting or requiring that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through certain electronic communications devices; prohibiting an employer from taking, or threatening to take, certain disciplinary actions for an employee's refusal to disclose certain password and related information; prohibiting an employer from failing or refusing to hire an

Maryland lawmakers thought it reasonable to consider social media protection policies in the employment context because Maryland law had already prohibited and otherwise regulated certain employer practices in the areas of recruitment, hiring, and retention.[37]

Media stories also often mention the city of Bozeman, Montana when discussing the need for social media protection in the employment context. In 2009, the city requested that "all job applicants . . . provide log-in information and passwords to social networking profiles . . . ."[38] The city's website did not just request login information and passwords for "social networking," but also for personal and professional sites.[39] However, the city repealed its policy before the issue reached the courts.[40]

Academic institutions have faced their own share of social media privacy concerns.[41] Universities may require that students let officials access their social media, going so far as to require that students install

applicant as a result of the applicant's refusal to disclose certain password and related information; prohibiting an employee from downloading certain unauthorized information or data to certain Web sites or Web–based accounts; providing that an employer, based on the receipt of certain information regarding the use of certain Web sites or certain Web–based accounts, is not prevented from conducting certain investigations for certain purposes; defining certain terms; and generally relating to employment and privacy protection.

37 Some of these regulations provide that employers or prospective employers cannot require employees and applicants to submit to a polygraph examination as a condition of employment. DEP'T LEGIS. SERVS., FISCAL & POL'Y NOTE, H.B. 964, Gen. Assemb., 430th Sess. (Md. 2012). Employers also cannot deny employment to an applicant based on his or her credit report or credit history. *Id.*

38 Timothy J. Long, EMP. L. Y.B., § 12:5 (citing Ki Mae Heusnner, *Montana City Asks Job Applicants for Online Passwords*, ABC NEWS (June 19, 2009), http://abcnews.go.com/Technology/JobClub/story?id=7879939&page=1).

39 *Id.*

40 Martha Neil, *Mont. Town Rescinds Rule Requiring Job Seekers to Reveal Social Web Passwords*, A.B.A. J. (June 23, 2009, 3:01 PM), www.abajournal.com/news/article/mont._town_rescinds_rule_requiring_job_seekers_to_reveal_social_web_passwor/.

41 Some of the restrictions imposed on employers arose from concerns with policies and requirements imposed by academic institutions. *See* DEP'T LEGIS. SERVS., FISCAL POL'Y NOTE, H.B. 964, Gen. Assemb., 430th Sess. (Md. 2012) ("Several companies offer a fee-based service that monitors the Twitter, Facebook, and other social media accounts of individuals by installing monitoring software on electronic devices. Though currently concentrated primarily on student-athletes in collegiate sports, such services could be used to monitor social media activity by employees. More than two dozen institutions, including the University of Louisville, Louisiana State University, and Texas A&M, have signed up with a social media monitoring company to monitor social media activity of their student-athletes."). In fact, university practices of requesting this information arose years ago. *See* Autumn K. Leslie, *Online Social Networks and Restrictions on College Athletes: Student Censorship?*, 5 DEPAUL J. SPORTS L. & CONTEMP. PROBS. 19 (2008) (discussing instances of social media searches being run on student-athletes as early as 2005, including the University of Kentucky administration using incriminating Facebook photos to convict its students of alcohol-related violations; Florida State administrators instructing coaches to randomly run Facebook searches on their student-athletes and requiring athletes to "cleanse their profiles" of certain pictures; and Loyola University Chicago banning its student-athletes from participation in MySpace and Facebook completely).

spying software on their devices.[42] In addition, universities and colleges are turning to social media monitoring software that automates the task of monitoring online activities.[43] Colleges have also required their student-athletes to consent to the monitoring of their Facebook, MySpace, and Twitter accounts by signing a social media policy.[44] In one example, the University of North Carolina's handbook included that "[e]ach team must identify at least one coach or administrator who is responsible for having access to and regularly monitoring the content of team members' social networking sites and postings."[45] In another, at the University of Kentucky, all student athletes are required to sign a form saying they will "friend" on Facebook and open their Twitter accounts to an athletics compliance officer.[46] These instances have led the state legislators to believe that statutory protection is necessary.

B. Statutes Passed in 2012 and 2013

i. Laws Regulating Employers

In 2012, four states—Maryland, Illinois, California, and Michigan—passed laws that restricted employer rights to social media accounts.[47] In 2013, the enactment of this type of legislation increased in speed. Nine more states, including Arkansas, Colorado, Nevada, New Jersey, New Mexico, Oregon, Vermont, Washington, and Utah, enacted employment-related social media password protection laws.[48] The statutes have four basic sections: 1) Prohibitions or Restrictions; 2) Definitions; 3) Exceptions and Exemptions; and 4) Enforcement Mechanisms.

Prohibitions/Restrictions

Generally, the laws enacted to regulate the employment setting restrict

---

42 David L. Hudson Jr., *Site Unseen: Schools, Bosses Barred from Eyeing Students', Workers' Social Media*, A.B.A. J. (Nov. 1, 2012, 2:10 AM), http://www.abajournal.com/magazine/article/site_unseen_schools_bosses_barred_from_eyeing_students_workers_social_media/.

43 *See* Bob Sullivan, *Govt. Agencies, Colleges Demand Applicants' Facebook Passwords*, NBC NEWS (Mar. 6, 2012, 6:13 AM), http://www.nbcnews.com/technology/govt-agencies-colleges-demand-applicants-facebook-passwords-328791; Linda B. Blackford, *What are the Wildcats Tweeting? UK Knows; It Monitors Athletes' Accounts*, KENTUCKYSPORTS.COM (July 26, 2012), http://www.kentucky.com/2012/07/26/2272406/what-are-the-wildcats-tweeting.html.

44 Blackford, *supra* note 43.

45 Sullivan, *supra* note 43.

46 Blackford, *supra* note 43.

47 *See Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, *supra* note 9.

48 *See Employer Access to Social Media Usernames and Passwords, 2013 Legislation*, *supra* note 10.

the employers' ability to request or require that an employee or applicant provide social media access information, like usernames or passwords.[49] The only exceptions to this general restriction are in New Mexico and Vermont. The law in New Mexico only restricts an employer from requiring access information from a *prospective* employee, not *current* employees.[50] Vermont's legislation does not provide for a restriction, but instead designates a committee to examine the laws enacted by other states, and then make recommendations and propose legislation.[51] Additionally, a majority of the states' legislation restricts an employer from taking adverse action against an employee, potential employee, or applicant for refusing to provide access information.[52] These provisions make it unlawful for an

---

[49] *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("An employer shall not require, request, suggest, or cause a current or prospective employee to . . . [d]isclose his or her username and password to the current or prospective employee's social media account . . . ."); CAL. LAB. CODE § 980 (West 2012) ("An employer shall not require or request an employee or applicant for employment to . . . [d]isclose a username or password for the purpose of accessing personal social media . . . ."); COLO. REV. STAT. § 8-2-127 (2013) ("An employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing the employee's or applicant's personal account or service through the employee's or applicant's electronic communications device."); 820 ILL. COMP. STAT. ANN. 55 / 10 (2014) ("[I]t shall be unlawful for any employer to 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 . . . ."); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012) ("[A]n employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device."); MICH. COMP. LAWS § 37.273 (2012) ("An employer shall not . . . [r]equest an employee or an applicant for employment to grant access to . . . or disclose information that allows access to or observation of the employee's or applicant's personal internet account."); NEV. REV. STAT. § 613.135 (2013) ("It is unlawful for any employer in this State to . . . [d]irectly or indirectly, require, request, suggest or cause any employee or prospective employee to disclose the user name, password or any other information that provides access to his or her personal social media account; N.J. STAT. ANN. § 34:6B-6 (West 2013) ("No employer shall require or request a current or prospective employee to provide or disclose any user name or password, or in any way provide the employer access to, a personal account through an electronic communications device."); N.M. STAT. ANN. § 50-4-34 (2013) ("It 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. REV. STAT. § 659A.330 (2013) ("It is an unlawful employment practice for an employer to . . . [r]equire or request an employee or an applicant for employment to disclose or to provide access through the employee's or applicant's user name and password, password or other means of authentication that provides access to a personal social media account . . . ."); UTAH CODE ANN. § 34-48-201 (West 2013) ("An employer may not . . . request 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 . . . ."); WASH. REV. CODE § 49.44.200 (2013) ("An employer may not . . . [r]equest, require, or otherwise coerce an employee or applicant to disclose login information for the employee's or applicant's personal social networking account").

[50] *See* N.M. STAT. ANN. § 50-4-34 (2013) (emphasis added) ("It 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 . . . .").

[51] S. 7, Gen. Assemb., 2013-2014 Leg. Sess. (Vt. 2013), 2013 Vt. Legis. Serv. 47 (West).

[52] *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("An employer shall not . . . [t]ake action

employer to discipline, discharge, or otherwise retaliate against employees who refuse to provide such information.[53] Moreover, employers cannot fail to hire an applicant who refuses to disclose his or her username or password.[54]

Outside of the two restrictions mentioned above, the statutes lack uniformity in terms of what else they prohibit. A few of the statutes prevent employers from requesting employees (or potential employees) to access social media accounts in the presence of that employer[55] (i.e. a restriction

against or threaten to discharge, discipline, or otherwise penalize a current employee for exercising his or her rights . . . or . . . [f]ail or refuse to hire a prospective employee for exercising his or her rights under subsection (b) of this section."); CAL. LAB. CODE § 980 (West 2012) ("An employer shall not discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section."); COLO. REV. STAT. § 8-2-127 (2013) ("An employer shall not . . . [d]ischarge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose any information specified in paragraph (a) of subsection (2) of this section . . ."); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012) ("An employer may not . . . discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose any information specified in subsection (b)(1) of this section; or . . . [f]ail or refuse to hire any applicant as a result of the applicant's refusal to disclose any information specified in subsection (b)(1) of this section."); MICH. COMP. LAWS § 37.273 (2012) ("An employer shall not . . . [d]ischarge, discipline, fail to hire, or otherwise penalize an employee or applicant for employment for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account."); NEV. REV. STAT. § 613.135 (2013) ("It is unlawful for any employer in this State to . . . [d]ischarge, discipline, discriminate against in any manner or deny employment or promotion to, or threaten to take any such action against any employee or prospective employee who refuses, declines or fails to disclose the user name, password or any other information that provides access to his or her personal social media account."); N.J. STAT. ANN. § 34:6B-8 (West 2013) ("No employer shall retaliate or discriminate against an individual because the individual has [refused] or was about to . . . [r]efuse to provide or disclose any user name or password, or in any way provide access to, a personal account through an electronic communications device . . . [,][r]eport an alleged violation of this act to the Commissioner of Labor and Workforce Development . . .[,] [t]estify, assist, or participate in any investigation, proceeding, or action concerning a violation of this act; or . . . [o]therwise oppose a violation of this act."); OR. REV. STAT. § 659A.330 (2013) ("It is an unlawful employment practice for an employer to . . . [t]ake, or threaten to take, any action to discharge, discipline or otherwise penalize an employee for the employee's refusal to disclose, or to provide access through, the employee's user name and password, password or other means of authentication that is associated with a personal social media account . . . or . . . [f]ail or refuse to hire an applicant for employment because the applicant refused to disclose, or to provide access through, the applicant's user name and password, password or other means of authentication that is associated with a personal social media account . . . ."); UTAH CODE ANN. § 34-48-201 (West 2013) ("An employer may not . . . take adverse action, fail to hire, or otherwise penalize an employee or applicant for employment for failure to disclose information described in Subsection (1)."); WASH. REV. CODE § 49.44.200 (2013) ("An employer may not . . . [t]ake adverse action against an employee or applicant because the employee or applicant refuses to disclose his or her login information, access his or her personal social networking account in the employer's presence, add a person to the list of contacts associated with his or her personal social networking account, or alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account..").

53 *See* statutes cited *supra* note 52.

54 *Id.*

55 *See, e.g.*, CAL. LAB. CODE § 980 (West 2012) ("An employer shall not require or request an

that targets "shoulder surfing"[56]). Other statutes protect against an employer's request or requirement that an employee add the employer (or its representative or agents) to its "friends" or list of contacts.[57] Some also prohibit employers from requesting an employee or prospective employee to change privacy settings on his or her social media accounts.[58] And

employee or applicant for employment to . . . [a]ccess personal social media in the presence of the employer"); 820 ILL. COMP. STAT. ANN. 55 / 10 (2014) ("[I]t shall be unlawful for any employer . . . to demand access in any manner to an employee's or prospective employee's account or profile on a social networking website."); MICH. COMP. LAWS § 37.273 (2012) ("An employer shall not . . . [r]equest an employee or applicant for employment to . . . allow observation of . . . the employee's or applicant's personal internet account."); OR. REV. STAT. § 659A.330 (2013) ("It is an unlawful employment practice for an employer to . . . [c]ompel an employee or applicant for employment to access a personal social media account in the presence of the employer and in a manner that enables the employer to view the contents of the personal social media account that are visible only when the personal social media account that are visible only when the personal social media account is accessed by the account holder's user name and password, password or other means of authentication . . ."); WASH. REV. CODE § 49.44.200 (2013) ("An employer may not . . . [r]equest, require, or otherwise coerce an employee or applicant to access his or her personal social networking account in the employer's presence in a manner that enables the employer to observe the contents of the account . . . ").

56 "Shoulder surfing" is defined as "the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information." *Definition of Shoulder Surfing*, OXFORD DICTIONARIES, http://oxforddictionaries.com/us/definition/american_english/shoulder-surfing (last visited Aug. 26, 2013). In this context, shoulder surfing constitutes an employer requesting an employee or potential employee to sign into his or her social media account in the presence of the employer in order to allow the employer to observe the account from the accountholder's point of view. *See* Phillip L. Gordon, Amber M. Spataro & William J. Simmons, *Social Media Password Protection and Privacy—The Patchwork of State Laws and How it Affects Employers*, LITTLER (May 3, 2013), http://www.littler.com/files/press/pdf/WPI-Social-Media-Password-Protection-Privacy-May-2013.pdf (Shoulder surfing is "asking applicants to log into their profiles and click through private messages, photos, wall posts, and other items as the interviewer watches"); Timothy J. Buckley, *Password Protection Now: An Elaboration on the Need for Federal Password Protection Legislation and Suggestions on How to Draft It*, 31 CARDOZO ARTS & ENT. L.J. 875, 887 (2013) ("Shoulder surfing occurs when an interviewer demands that someone access their personal account in the interviewer's presence in order to examine the password-protected features of the account.").

57 *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("An employer shall not require, request, suggest, or cause a current or prospective employee to . . . [a]dd an employee, supervisor, or administrator to the list or contacts associated with his or her social media account . . . ."); COLO. REV. STAT. § 8-2-127 (2013) ("An employer shall not compel an employee or applicant to add anyone, including the employer or his or her agent, to the employee's or applicant's list of contacts associated with a social media account . . . ."); OR. REV. STAT. § 659A.330 (2013) ("It is an unlawful employment practice for an employer to . . . [c]ompel an employee or applicant for employment to add the employer or an employment agency to the employee's or applicant's list of contacts associated with a social media website . . . .").

58 *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("An employer shall not require, request, suggest, or cause a current or prospective employee to . . . [c]hange the privacy settings associated with his or her social media account."); COLO. REV. STAT. § 8-2-127 (2013) ("An employer shall not . . . cause an employee or applicant to change privacy settings associated with a social networking account."); WASH. REV. CODE § 49.44.200 (2013) **(**An employer may not . . . [t]ake adverse action against an employee or applicant because the employee or applicant refuses to . . . alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account.").

finally, other statutes provide broad, generalized restrictions on employers demanding access to any social media information, or in *any* manner, to an employee or prospective employee's account.[59] The lack of uniformity among the statutes may cause difficulty for employers with workers in multiple states.[60]

Definitions

Two definitions are vital to the scope of this legislation. The first is for the term "employer." Many employment statutes define "employer" generally, as a person, individual, or entity engaged in a business, industry, profession, trade, or enterprise in the state of a unit of state or local government.[61] Uniquely, however, both the Colorado and New Jersey legislation specify that "employer" does not include the department of corrections, county corrections departments, or any state or local law enforcement agency.[62] New Mexico excludes similar agencies through an

---

59 *See, e.g.*, CAL. LAB. CODE § 980 (West 2012) (emphasis added) ("An employer shall not require or request an employee or applicant for employment to. . . [d]ivulge *any* personal social media . . . ."); 820 ILL. COMP. STAT. 55 / 10 (2014) (emphasis added) ("[I]t shall be unlawful for any employer . . . to demand access *in any manner* to an employee's or prospective employee's account or profile on a social networking website."); N.M. STAT. ANN. § 50-4-34 (2013) (emphasis added) ("It is unlawful for an employer . . . to demand access in *any* manner to a prospective employee's account or profile on a social networking website.").

60 *See* Gordon, Spataro, & Simmons, *supra* note 56, at 3-4 ("[S]tates have yet to settle on any model legislation with identical, or nearly identical, terms, and none offers a 'perfect' solution. Instead, they create a complex patchwork that makes it virtually impossible for a multi-state employer to establish a uniform policy . . .").

61 *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("'Employer' means a person or entity engaged in business, an industry, a profession, a trade or other enterprise in the state or a unit of state or local government, including without limitation an agent, representative, or designee of the employer . . . "); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012) ("'Employer' means: 1. a person engaged in a business, an industry, a profession, a trade, or other enterprise in the state; or 2. a unit of State or local government"); MICH. COMP. LAWS § 37.272 (2012) ("'Employer' means a person, including a unit or local government, engaged in business, industry, profession, trade, or other enterprise in this state and includes an agent, representative, or designee of the employer."); WASH. REV. CODE § 49.44.200 (2013) ("'Employer' means any person, firm, corporation, partnership, business trust, legal representative, or other business entity which engages in any business, industry, profession, or other activity in this state and employs one or more employees, and includes the state, any state institution, state agency, political subdivisions of the state, and any municipal corporation or quasi-municipal corporation. 'Employer' includes an agent, a representative, or a designee of the employer.").

62 *See, e.g.*, COLO. REV. STAT. § 8-2-127 (2013) ("'Employer' means a person engaged in a business, industry, profession, trade, or other enterprise in the state or a unit of state or local government. 'Employer' includes an agent, a representative, or a designee of the employer. 'Employer' does not include the Department of Corrections, County Corrections Departments, or any state or local law enforcement agency."); N.J. STAT. ANN. § 34:6B-5 (West 2013) ("'Employer' means an employer or employer's agent, representative, or designee. The term 'employer' does not include the Department of Corrections, State Parole Board, county corrections departments, or any State or local law enforcement agency.").

exception.[63]

Also important to the scope of the legislation is the definition of "social media" or "social networking account." How the laws define these terms, and whether a definition is included in the statute, varies based on state. For example, a few of the statutes define "social media" so broadly that they functionally include *any* type of online account.[64] Some state legislatures, such as those in Illinois, New Jersey, and New Mexico, attempted narrower definitions of "social media" or "social networking website" to specify the use of social media accounts today; for instance, these laws describe a list of connections, or friends, and use of "profile."[65] Other legislation does not provide a definition for "social media" or "social networking" at all, but instead provides restrictions on "personal accounts" or "personal internet accounts."[66] Two laws provide a definition for both.[67]

---

63 *See* N.M. STAT. ANN. § 50-4-34 (2013) ("Nothing in this section shall apply to a federal, state or local law enforcement agency. Nothing in this section shall prohibit federal, state or local government agencies or departments from conducting background checks as required by law.").

64 *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) (emphasis added) ("'[S]ocial media account' means a personal account with an electronic medium or service where users may create share or view user-generated content, including without limitation: (i) Videos; (ii) Photographs; (iii) Blogs; (iv) Podcasts; (v) Messages; (vi) Emails; or (vii) Website profile or location"); CAL. LAB. CODE § 980 (West 2012) ("'[S]ocial media' means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."); NEV. REV. STAT. § 613.135 (2013) ("'[S]ocial media account' means any electronic service or account or electronic content, including, without limitation, videos, photographs, blogs, video blogs, podcasts, instant and text messages, electronic mail programs or services, online services or Internet website profiles."); OR. REV. STAT. § 659A.330 (2013) ("'[S]ocial media' means an electronic medium that allows users to create, share and view user-generated content, including, but not limited to, uploading or downloading videos, still photograph, blogs, video blogs, podcasts, instant messages, electronic mail or Internet website profiles or locations.").

65 *See, e.g.*, 820 ILL. COMP. STAT. 55 / 10 (2014) ("'[S]ocial networking website' means an Internet-based service that allows individuals to: (A) construct a public or semi-public profile within a bounded system, created by the service; (B) create a list of other users with whom they share a connection within the system; and (C) view and navigate their list of connections and those made by others within the system. 'Social networking website' shall not include electronic mail."); N.J. STAT. ANN. § 34:6B-5 (West 2013) ("'Social networking website' means an Internet-based service that allows individuals to construct a public or semi-public profile within a bounded system created by the service, create a list of other users with whom they share a connection within the system, and view and navigate their list of connections and those made by others within the system."); N.M. STAT. ANN. § 50-4-34 (2013) ("'[S]ocial networking web site' means 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.").

66 *See, e.g.*, MICH. COMP. LAWS § 37.272 (2012) ("'Personal internet account' means an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data."); UTAH CODE ANN. § 34-48-102 (West 2013) ("'Personal Internet account' means an online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer. . . .

Other statutes provide no definition for social media, social networking, or personal accounts.[68]

Exceptions/Exemptions

Practitioners recognize that "[t]he range of exceptions to the general prohibition is even more dizzying than the range of prohibitions,"[69] because the statutes lack uniformity. Seven of the eleven states—Arkansas, Illinois, Michigan, New Jersey, New Mexico, Oregon, and Utah—currently permit employers to view social media account information that is publicly available.[70] Seven of the eleven states' legislation—Arkansas, Illinois,

'Personal Internet account' does not include an account created, maintained, used, or accessed by an employee or applicant for business related communications or for a business purpose of the employer.").

67 *See, e.g.*, 820 ILL. COMP. STAT. 55 / 10 (2014). Notably, Illinois's Workplace Privacy Act did not initially provide a definition for personal accounts, but was later amended to include the broad definition of "personal account," meaning "an account, service, or profile on a social networking website that is used by a current or prospective employee exclusively for personal communication unrelated to any business purposes of the employer." *See* S.B. 2306, 98th Gen. Assemb., Reg. Sess. (Ill. 2013), 2013 Ill. Legis. Serv. 98-501 (West). *See also* N.J. STAT. ANN. § 34:6B-5 (West 2013) ("'Personal account' means an account, service or profile on a social networking website that is used by a current or prospective employee exclusively for personal communications unrelated to any business purposes of the employer. This definition shall not apply to any account, service or profile created, maintained, used or accessed by a current or prospective employee for business purposes of the employer or to engage in business related communications."). The New Jersey Legislature's definition of "[s]ocial networking website" is "an Internet-based service that allows individuals to construct a public or semi-public profile within a bounded system created by the service, create a list of other users with whom they share a connection within the system, and view and navigate their list of connections and those made by others within the system." N.J. STAT. ANN. § 34:6B-5 (West 2013).

68 *See, e.g.*, COLO. REV. STAT. § 8-2-127 (2013); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012).

69 Philip L. Gordon & Joon Hwang, *Making Sense of the Complex Patchwork Created by Nearly One Dozen New Social Media Password Protection Laws*, LITTLER (July 2, 2013), http://www.littler.com/publication-press/publication/making-sense-complex-patchwork-created-nearly-one-dozen-new-social-med.

70 *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("This section does not prohibit an employer from viewing information about a current or prospective employee that is publicly available on the Internet."); 820 ILL. COMP. STAT. 55 / 10 (2014) ("Nothing in this subsection shall prohibit an employer from obtaining about a prospective employee or an employee information that is in the public domain . . . ."); MICH. COMP. LAWS § 37.275 (2012) ("This act does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain."); N.J. STAT. ANN. § 34:6B-10 (West 2013) ("Nothing in this act shall prevent an employer from viewing, accessing, or utilizing information about a current or prospective employee that can be obtained in the public domain."); N.M. STAT. ANN. § 50-4-34 (2013) ("Nothing in this section shall prohibit an employer from obtaining information about a prospective employee that is in the public domain."); OR. REV. STAT. § 659A.330 (2013) ("Nothing in this section prohibits an employer from accessing information available to the public about the employee or applicant that is accessible through an online account."); UTAH CODE ANN. § 34-48-202(4) (West 2013) ("This chapter does not prohibit or restrict an employer from viewing, accessing, or using information about an employee or applicant . . . that is available in the public domain.").

Michigan, Nevada, New Jersey, Oregon, and Washington—state that the main prohibition does not apply when an employer needs to take action to comply with the requirements of federal, state, or local laws, rules or regulations, or the rules or regulations of self-regulatory organizations.[71] Some laws are narrower than others, such as those of Colorado and Maryland; these provide an exception for employers to conduct investigations to comply with applicable securities or financial law or regulatory requirements.[72]

Seven of the eleven states—Arkansas, California, Michigan, New Jersey, Oregon, Utah, and Washington—provide exceptions for investigations of employee misconduct or employee violation of applicable laws and regulations.[73] The laws enacted in Colorado, Illinois, Maryland,

---

71 *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("Nothing in this section . . . [p]revents an employer from complying with the requirements of federal, state, or local laws, rules, or regulations or the rules or regulations of self-regulatory organizations . . . ."); NEV. REV. STAT. § 613.135 (2013) ("Nothing in this section shall be construed to prevent an employer from complying with any state or federal law or regulation or with any rule of a self-regulatory organization . . ."); N.J. STAT. ANN. § 34:6B-10 (West 2013) ("Nothing in this act shall be construed to prevent an employer from complying with the requirements of State or federal statutes, rules or regulations, case law or rules of self-regulatory organizations."); OR. REV. STAT. § 659A.330 (2013) ("Nothing in this section prevents an employer from . . . [c]omplying with state and federal laws, rules and regulations and the rules of self-regulatory organizations."); WASH. REV. CODE § 49.44.200 (2013) ("This section does not . . . [p]revent an employer from complying with the requirements of state or federal statutes, rules or regulations, case law, or rules of self-regulatory organizations.").

72 *See, e.g.*, COLO. REV. STAT. § 8-2-127 (2013) ("This section does not prevent an employer from . . . [c]onducting an investigation to ensure compliance with applicable securities or financial law or regulatory requirements based on the receipt of information about the use of a personal web site, internet web site, web-based account, or similar account by an employee for business purposes"); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012) ("This section does not prevent an employer . . . based on the receipt of information about the use of a personal Web site, Internet Web site, Web-based account, or similar account by an employee for business purposes, from conducting an investigation for the purpose of ensuring compliance with applicable securities or financial law, or regulatory requirements"). For laws with other narrower, more specific exceptions, *see also* 820 ILL. COMP. STAT. 58/10 (2014) ("Provided that the password, account information, or access sought by the employer relates to a professional account, and not a personal account, nothing in this subsection shall prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications as required under Illinois insurance laws or federal law or by a self-regulatory organization . . ."); MICH. COMP. LAWS § 37.275 (2012) ("This act does not prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under federal law or by a self-regulatory organization, as defined in section 3(a)(26) of the securities and exchange act of 1934, 15 USC 78c(a)(26).").

73 *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) ("Nothing in this section . . . [a]ffects an employer's existing rights or obligations to request an employee to disclose his or her username and password for the purpose of accessing a social media account if the employee's social media account activity is reasonably believed to be relevant to a formal investigation or related proceeding by the employer of allegations of an employee's violation of federal, state, or local laws or regulations or of the employer's written policies."); CAL. LAB. CODE § 980 (West 2012) ("Nothing in this section shall affect an employer's existing rights and obligations to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct . . .");

Michigan, New Jersey, Utah, and Washington provide additional varying exceptions or exemptions benefiting employers; these include provisions that allow employers to request information on accounts or equipment that are provided by the employer, for investigating the employer's internal computer or information systems, and/or for taking action when the employee downloads the employer's proprietary, confidential or financial information.[74]

MICH. COMP. LAWS § 37.275 (2012) ("This act does not prohibit an employer from . . . [c]onducting an investigation or requiring an employee to cooperate in an investigation . . . [i]f there is specific information about activity on the employee's personal internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct."); N.J. STAT. ANN. § 34:6B-10 (West 2013) ("Nothing in this act shall prevent an employer from conducting an investigation: (1) for the purpose of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on a personal account by an employee . . .); OR. REV. STAT. § 659A.330 (2013) ("Nothing in this section prevents an employer from . . . [c]onducting an investigation, without requiring an employee to provide a user name and password, password or other means of authentication that provides access to a personal social media account of the employee, for the purpose of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct based on receipt by the employer of specific information about activity of the employee on a personal online account or service."); UTAH. CODE ANN. § 34-48-202 (West 2013) ("This chapter does not prohibit an employer from . . . conducting an investigation or requiring an employee to cooperate in an investigation . . . for . . . prohibitions against work-related employee misconduct"); WASH. REV. CODE § 49.44.200 (2013) ("This section does not apply to an employer's request or requirement that an employee share content from his or her personal social networking account if the following conditions are met: (a) [t]he employer requests or requires the content to make a factual determination in the course of conducting an investigation; (b) [t]he employer undertakes the investigation in response to receipt of information about the employee's activity on his or her personal social networking account; (c) [t]he purpose of the investigation is to: (i) [e]nsure compliance with . . . prohibitions against work-related employee misconduct; . . . (d) [t]he employer does not request or require the employee to provide his or her login information.").

[74] *See, e.g.*, COLO. REV. STAT. § 8-2-127 (2013) ("This section does not prevent an employer from . . . [i]nvestigating an employee's electronic communications based on the receipt of information about the unauthorized downloading of an employer's proprietary information or financial data to a personal web site, internet web site, web-based account, or similar account by an employee."); 820 ILL. COMP. STAT. ANN. 55 / 10 (2014) ("Nothing in this subsection shall limit an employer's right to . . . monitor usage of the employer's electronic equipment and the employer's electronic mail without requesting or requiring 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."); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012) ("An employer may require an employee to disclose any user name, password, or other means for accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems. . . . This section does not prevent an employer . . . [b]ased on the receipt of information about the unauthorized downloading of an employer's proprietary information or financial data to a personal Web site, Internet Web site, Web–based account, or similar account by an employee, from investigating an employee's actions under subsection (d) of this section."); MICH. COMP. LAWS § 37.25 (2012) ("This act does not prohibit an employer from doing any of the following: (a) Requesting or requiring an employee to disclose access information to the employer to gain access to or operate any of the following: (i) An electronic communications device paid for in whole or in part by the employer; (ii) An account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes. (b) Disciplining or

All of the employment statutes, except for New Mexico's law (because it only applies to job applicants, not current employees), provide an exception that allows employers to request or require that the employees provide access to information to *non-personal* accounts (i.e. accounts that are used for employer's business purposes).[75]

discharging 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. (c) Conducting an investigation or requiring an employee to cooperate in an investigation . . . [i]f the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal internet account."); N.J. STAT. ANN. § 34:6B-10 (West 2013) ("Nothing in this act shall prevent an employer from implementing and enforcing a policy pertaining to the use of an employer issued electronic communications device or any accounts or services provided by the employer or that the employee uses for business purposes . . . Nothing in this act shall prevent an employer from conducting an investigation . . . of an employee's actions based on the receipt of specific information about the unauthorized transfer of an employer's proprietary information, confidential information or financial data to a personal account by an employee"); UTAH CODE ANN. § 34-48-202 (West 2013) ("This chapter does not prohibit an employer from doing any of the following: (a) requesting or requiring an employee to disclose a username or password required only to gain access to the following: (i) an electronic communications device supplied by or paid for in whole or in part by the employer; or (ii) an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, and used for the employer's business purposes; (b) disciplining or discharging 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; (c) conducting an investigation or requiring an employee to cooperate in an investigation in any of the following . . . if the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal Internet account . . .; (e) monitoring, reviewing, accessing, or blocking electronic data stored on an electronic communications device supplied by, or paid for in whole or in part by, the employer, or stored on an employer's network . . ."); WASH. REV. CODE § 49.44.200 (2013) ("This section does not apply to an employer's request or requirement that an employee share content from his or her personal social networking account if the following conditions are met: (a) The employer requests or requires the content to make a factual determination in the course of conducting an investigation; (b) The employer undertakes the investigation in response to receipt of information about the employee's activity on his or her personal social networking account; (c) The purpose of the investigation is to . . . (ii) investigate an allegation of unauthorized transfer of an employer's proprietary information, confidential information, or financial data to the employee's personal social networking account; and (d) The employer does not request or require the employee to provide his or her login information. . . (3) This section does not: (a) Apply to a social network, intranet, or other technology platform that is intended primarily to facilitate work-related information exchange, collaboration, or communication by employees or other workers; (b) Prohibit an employer from requesting or requiring an employee to disclose login information for access to: (i) An account or service provided by virtue of the employee's employment relationship with the employer; or (ii) an electronic communications device or online account paid for or supplied by the employer . . .").

75 *See, e.g.*, statutes cited *supra* note 74. Originally, Illinois's legislation was the one exception to this, *see* Gordon & Hwang, *supra* note 69, but with its amendment in 2013, *see* S.B. 2306, 98th Gen. Assemb., Reg. Sess. (Ill. 2013), 2013 Ill. Legis. Serv. P.A. 98-501 (West), Illinois's legislation now also differentiates between personal and non-personal, or "professional" accounts. *See* 820 ILL. COMP. STAT. ANN. 55 / 10 (2014) (final statute).

Enforcement Mechanisms

The manner in which the social media legislation will be enforced, if an employer violates the statute, is one of the biggest issues surrounding enactment. It is no surprise that the enforcement mechanisms in the laws differ vastly from state to state (including whether the law even has an enforcement provision at all). There are a variety of enforcement mechanisms in the state laws, including administrative remedies, civil actions, and equitable relief. Summarily:

> The remedial schemes for violation of these laws vary even more substantially than the prohibitions and exceptions. In three states — Arkansas, Nevada and New Mexico — the statutes do not include a remedial provision and do not expressly incorporate one by reference. Two states — California and Colorado — provide no private right of action. The remaining states provide a private right of action with varying caps: Utah and Washington ($500); Michigan ($1,000); Illinois and Maryland (no cap); Oregon (unclear). Four states — California, Colorado, Illinois, and Oregon — expressly create administrative remedies; the other states do not.[76]

Additionally, New Jersey's bill, not discussed in the paragraph above, provides for a summary proceeding and assessment of civil penalties (not to exceed $1,000 for the first violation and $2,500 for each subsequent violation).[77]

ii. Laws Regulating Educational Institutions

In 2012, four states—Delaware, California, New Jersey, and Michigan—passed legislation which restricts educational institutions' access to social media accounts.[78] In 2013, five more states—Arkansas, Illinois, New Mexico, Oregon, and Utah—passed legislation restricting an educational institution from requesting a student's or applicant's social media password or username.[79] Similar to the statutes that regulate employers, the educational statutes tend to have four basic sections: 1) Prohibitions/Restrictions; 2) Definitions; 3) Exceptions and Exemptions; and 4) Enforcement Mechanisms.

---

76 Gordon & Hwang, *supra* note 69.

77 N.J. STAT. ANN. § 34:6B-9 (West 2013).

78 *See Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, *supra* note 9.

79 *See Employer Access to Social Media Usernames and Passwords, 2013 Legislation*, *supra* note 10.

Prohibitions/Restrictions

All of the statutes passed for the academic setting provide a restriction on an educational institution's ability to request or require that a student or applicant provide social media access information (i.e. his or her username or password to a social media account).[80] Additionally, a majority of the states' legislation includes a restriction on an educational institution's ability to take adverse action against a student, applicant, or prospective applicant for refusing to provide access information.[81] These provisions

[80] *See, e.g.*, ARK. CODE ANN. § 6-60-104 (2013) ("An institution of higher education shall not require, request, suggest, or cause . . . [a] current or prospective employee or student to disclose his or her username and password to the current or prospective employee or student's social media account . . . ."); CAL. EDUC. CODE § 99121 (West 2012) ("Public and private postsecondary educational institutions, and their employees and representatives, shall not require or request a student, prospective student, or student group to . . . [d]isclose a user name or password for accessing personal social media . . . ."); DEL. CODE ANN. tit. 14, § 8103 (2012) ("An academic institution shall not request or require that a student or applicant disclose any password or other related account information in order to gain access to the student's or applicant's social networking site profile or account by way of an electronic communication device."); 105 ILL. COMP. STAT. ANN. 75 / 10 (2014) ("It is unlawful for a post-secondary school to request or require a student or his or her parent or guardian to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website . . . "); MICH. COMP. LAWS § 37.274 (2012) ("An educational institution shall not . . . [r]equest a student or prospective student to grant access to, allow observation of, or disclose information that allows access to or observation of the student's or prospective student's personal internet account."); N.J. STAT. ANN. § 18A:3-30 (West 2012) ("No public or private institution of higher education in this State shall . . . [r]equire a student or applicant to provide or disclose any user name or password, or in any way provide access to, a personal account or service through an electronic communications device . . ."); N.M. STAT. ANN. § 21-1-46 (2013) ("It is unlawful for a public or private institution of post-secondary education to request or require a student, applicant or potential applicant for admission to provide a password to gain access to the student's, applicant's or potential applicant's account or profile on a social networking web site . . ."); OR. REV. STAT. § 326.551 (2013) ("A public or private educational institution may not . . . [r]equire, request or otherwise compel a student or prospective student to disclose or to provide access to a personal social media account through the student's or prospective student's user name and password, password or other means of authentication that provides access."); UTAH CODE ANN. § 53B-25-201 (West 2013) ("A postsecondary institution may not do any of the following: (1) request a student or prospective student to disclose a username and password, or a password that allows access to the student's or prospective student's personal Internet account . . .").

[81] *See, e.g.*, ARK. CODE ANN. § 6-60-104 (2013) ("An institution of higher education shall not . . . [t]ake action against or threaten to discharge, discipline, prohibit from participating in curricular or extracurricular activities, or otherwise penalize a current student for exercising his or her rights under subsection (b) of this section; or . . . [f]ail or refuse to admit or hire a prospective employee or student for exercising his or her rights under subsection (b) of this section."); CAL. EDUC. CODE § 99121(West 2012) ("A public or private postsecondary educational institution shall not suspend, expel, discipline, threaten to take any of those actions, or otherwise penalize a student, prospective student, or student group in any way for refusing to comply with a request or demand that violates this section."); DEL. CODE ANN. tit. 14, § 8104 (2012) ("An academic institution may not discipline, dismiss or otherwise penalize or threaten to discipline, dismiss or otherwise penalize a student for refusing to disclose any information specified in § 8103(a) or (b) of this title. It shall also be unlawful for a public or nonpublic academic institution to fail or refuse to admit any applicant as a result of the applicant's refusal to disclose any information specified in § 8103(a) or (b) of this title."); MICH. COMP. LAWS § 37.2748

make it unlawful for an educational institution to expel, discipline, fail to admit, or otherwise retaliate against students or applicants who refuse to provide their social media password or username.[82]

Outside of the restrictions on requesting passwords or usernames and taking adverse action, the legislation as a whole lacks uniformity. Many state legislatures included provisions with an especially broad scope. Some laws prohibit an institution of higher education from requiring, requesting, or suggesting a current or prospective student to add an employee of the institution to a list of contacts.[83] Educational institutions may also be prohibited from requesting a student to change the privacy settings associated with his or her account.[84] Importantly, some of the legislation provides a restriction on shoulder surfing,[85] includes broad language

(2012) ("An educational institution shall not . . . [e]xpel, discipline, fail to admit, or otherwise penalize a student or prospective student for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the student's or prospective student's personal internet account."); N.J. STAT. ANN. § 18A:3-30 (West 2012) ("No public or private institution of higher education in this State shall . . . [p]rohibit a student or applicant from participating in activities sanctioned by the institution of higher education, or in any other way discriminate or retaliate against a student or applicant, as a result of the student or applicant refusing to provide or disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device as provided in subsection a. of this section."); N.M. STAT. ANN. § 21-1-46 (2013) ("It is unlawful for public or private institutions of post-secondary education to deny admission to an applicant or potential applicant for admission on the basis of the applicant's or potential applicant's refusal to provide an agent of a public or private institution of post-secondary education access to the applicant's or potential applicant's account or profile on a social media networking site. It is unlawful for a private or public institution of post-secondary education to take any disciplinary action against a student for the student's refusal to grant access to an agent of the private or public institution of post-secondary education to the student's account or profile on a social media networking site."); OR. REV. STAT. § 326.551 (2013) ("A public or private educational institution may not . . .[t]ake, or threaten to take, any action to discipline or to prohibit from participation in curricular or extracurricular activities a student or prospective student for refusal to disclose the information or take actions specified in paragraph (a) or (b) of this subsection . . . [or] [f]ail or refuse to admit a prospective student as a result of the refusal by the prospective student to disclose the information or take actions specified in paragraph (a) or (b) of this subsection."); UTAH CODE ANN. § 53B-25-201 (West 2013) ("A postsecondary institution may not . . . expel, discipline, fail to admit, or otherwise penalize a student or prospective student for failure to disclose information specified in Subsection (1).").

82 *See* statutes cited *supra* note 81.

83 *See, e.g.*, ARK. CODE ANN. § 6-60-104 (2013) ("An institution of higher education shall not require, request, suggest, or cause . . . [a] current or prospective student, as a condition of acceptance in curricular or extracurricular activities, to . . . [a]dd an employee or volunteer of the institution of higher education, including without limitation a coach, professor, or administrator, to the list of contacts associated with his or her social media account . . ."); DEL. CODE ANN. tit. 14, § 8103 (2012) ("An academic institution shall not request or require a student or applicant to add the employer or its representative to their personal social networking site profile or account").

84 *See* ARK. CODE ANN. § 6-60-104 (2013) ("An institution of higher education shall not require, request, suggest, or cause . . . [a] current or prospective student, as a condition of acceptance in curricular or extracurricular activities, to . . . [c]hange the privacy settings associated with his or her social media account.").

85 *See, e.g.*, CAL. EDUC. CODE § 99121 (West 2012) ("Public and private postsecondary

restricting someone from accessing a social media account by way of another,[86] and/or provides broad restrictions against inquiring as to whether a student has a social networking account.[87]

Definitions

The statutes that put restrictions on educational institutions vary in terms of scope, with all covering colleges and universities, but some also covering elementary and secondary schools. Two definitions are at issue in these statutes: 1) the definition of "educational institution"; and 2) the definition of "social media" or "social networking website." All of the legislation regulating academic institutions, except for Michigan's Internet Privacy Protection Act,[88] applies *only* to postsecondary institutions or institutions of higher education. In fact, Oregon's lawmakers specifically excluded kindergarten, elementary, or secondary schools.[89] Alarmingly, Michigan's Internet Privacy Protection Act includes an especially broad definition of educational institution, protecting not only the individuals attending postsecondary institutions, but also those students at elementary or secondary schools and nurseries.[90]

---

educational institutions, and their employees and representatives, shall not require or request a student, prospective student, or student group to . . . [a]ccess personal social media in the presence of the institution's employee or representative."); DEL. CODE ANN. tit. 14, § 8103 (2012) ("An academic institution shall not require or request that a student or applicant log onto a social networking site, mail account, or any other internet site or application by way of an electronic communication device in the presence of an agent of the institution so as to provide the institution access")"); OR. REV. STAT. § 326.551 (2013) ("A public or private educational institution may not . . . [r]equire, request or otherwise compel a student or prospective student to access a personal social media account in the presence of an administrator or other employee of the educational institution in a manner that enables the administrator or employee to observe the contents of the personal social media account."). For a definition of "shoulder surfing," *see supra* note 56.

86 *See, e.g.*, DEL. CODE ANN. tit. 14, § 8103 (2012) ("An academic institution is prohibited from accessing a student's or applicant's social networking site profile or account indirectly through any other person who is a social networking contact of the student or applicant.").

87 *See, e.g.*, N.J. STAT. ANN. § 18A:3-30 (West 2012) (emphasis added) ("No public or private institution of higher education in this State shall . . . [i]n *any* way inquire as to whether a student or applicant has an account or profile on a social networking website.").

88 MICH. COMP. LAWS §§ 37.272, 37.274 (2012).

89 *See, e.g.*, OR. REV. STAT. § 326.551 (2013) ("'Educational institution' means an institution that offers participants, students or trainees an organized course of study or training that is academic, technical, trade-oriented or preparatory for gainful employment in a recognized occupation. 'Educational institution' includes, but is not limited to, community colleges and the public universities . . . but does not include kindergarten, elementary or secondary schools.").

90 *See* MICH. COMP. LAWS § 37.272 (2012) ("'Educational institution' means a public or private educational institution or a separate school or department of a public or private educational institution, and includes an academy; elementary or secondary school; extension course; kindergarten; nursery school; school system; school district; intermediate school district; business, nursing, professional, secretarial, technical, or vocational school; public or private educational testing service or administrator; and an agent of an educational institution. Educational institution shall be construed broadly to include

Comparatively, Illinois's law partially restricts secondary schools' access to social media accounts by including a notice requirement to parents or guardians.[91] Illinois's statute also requires that an educational institution have a reason to review the account based on a published school policy.[92] Although these provisions limit an institution's access, the Illinois law still appropriately provides a way for elementary and secondary schools to request this information.

Also important is the manner in which the statutes define "social media" or "social networking." Similar to the laws that regulate employers, some of the legislation that regulates educational institutions defines "social media" so broadly that it effectively includes any type of online account.[93] Others more appropriately attempt to narrowly describe social media as a "profile" in which individuals make "connections" within a bounded system.[94] Other laws do not define social media or social networking, but

public and private institutions of higher education to the greatest extent consistent with constitutional limitations.").

91 *See* 105 ILL. COMP. STAT. ANN. 75 / 15 (2014) ("An elementary or secondary school must provide notification to the student and his or her parent or guardian that the elementary or secondary school may request or require a student to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website if the elementary or secondary school has reasonable cause to believe that the student's account on a social networking website contains evidence that the student has violated a school disciplinary rule or policy. The notification must be published in the elementary or secondary school's disciplinary rules, policies, or handbook or communicated by similar means.").

92 *Id.*

93 *See, e.g.*, ARK. CODE ANN. § 6-60-104 (2013) ("'Social media account' means a personal account with an electronic medium or service where users may create, share, or view user generated content, including without limitation: (i) Videos; (ii) Photographs; (iii) Blogs; (iv) Podcasts; (v) Messages; (vi) Emails; or (vii) Website profiles or locations . . . 'Social media account' includes without limitation an account established with Facebook, Twitter, LinkdIn, MySpace, or Instagram . . ."); CAL. EDUC. CODE § 99120 (West 2012) ("'[S]ocial media' means an electronic service or account, or electronic content, including, but not limited to, videos or still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."); OR. REV. STAT. § 326.551(2013) ("'Social media' means an electronic medium that allows users to create, share and view user-generated content, including, but not limited to, uploading or downloading videos, still photographs, blogs, video blogs, podcasts, instant messages, electronic mail or Internet website profiles or locations.").

94 *See, e.g.*, DEL. CODE ANN. tit. 14, § 8102 (2012) ("'Social networking site' means an Internet-based, personalized, privacy-protected website or application whether free or commercial that allows users to construct a private or semi-private profile site within a bounded system, create a list of other system users who are granted reciprocal access to the individual's profile site, send and receive email, and share personal content, communications, and contacts."); 105 ILL. COMP. STAT. ANN. 75 / 5 (2014) ("'Social networking website' means an Internet-based service that allows individuals to do the following: (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. 'Social networking website' does not include electronic mail."); N.J. STAT. ANN. § 18A:3-29 (West 2012) ("'Social networking website' means an Internet-based service that allows individuals to construct a public or semi-public profile within a bounded system created by the service, create a list of other users with

instead use the term "personal internet account."[95]

Exceptions/Exemptions

The exceptions in the educational laws are just as "dizzying" as those in the employment laws.[96] Five of the eight states that have enacted password protection bills to regulate educational institutions—Arkansas, Illinois, Michigan, New Mexico, and Utah—provide an exception to allow an academic institution to view information that is publicly available or in the public domain.[97] At the end of 2013, only one educational password protection law provided a generalized exception allowing an educational institution to request access information if it is complying with the requirements of federal or state laws, rules, or regulations.[98] Other exceptions provide for investigations of student misconduct and violations of federal or state law,[99] violations of school disciplinary rules or

whom they share a connection within the system, and view and navigate their list of connections and those made by others within the system."); N.M. STAT. ANN. § 21-1-46 (2013) ("'[S]ocial networking web site' means 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.").

95 *See, e.g.*, MICH. COMP. LAWS § 37.272 (2012) ("'Personal internet account' means an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data."); UTAH CODE ANN. § 53B-25-102 (West 2013) ("'Personal Internet account' means an online account that is used by a student or prospective student exclusively for personal communications unrelated to any purpose of the postsecondary institution . . . 'Personal Internet account' does not include an account created, maintained, used, or accessed by a student or prospective student for education related communications or for an educational purpose of the postsecondary institution.").

96 *See generally supra* Part II (B)(i); Gordon & Hwang, *supra* note 69..

97 *See, e.g.*, ARK. CODE ANN. § 6-60-104 (2013) ("This section does not prohibit an institution of higher education from viewing information about a current or prospective employee or student that is publicly available on the Internet."); 105 ILL. COMP. STAT. ANN. 75 / 10 (2014) ("Nothing in this Section prohibits a post-secondary school from obtaining information about a student that is in the public domain or that is otherwise obtained in compliance with this Act."); MICH. COMP. LAWS § 37.276 (2012) ("This act does not prohibit or restrict an educational institution from viewing, accessing, or utilizing information about a student or applicant that can be obtained without any required access information or that is available in the public domain."); N.M. STAT. ANN. § 21-1-46 (2013) ("Nothing in this section prohibits a public or private institution of post-secondary education from obtaining information about a student, applicant or potential applicant for admission that is in the public domain."); UTAH CODE ANN. § 53B-25-202 (West 2013) ("This chapter does not prohibit or restrict a postsecondary institution from viewing, accessing, or using information about a student or prospective student . . . that is available in the public domain.").

98 *See* ARK. CODE ANN. § 6-60-104 (2013) ("Nothing in this section prevents an institution of higher education from complying with the requirements of federal or state laws, rules, or regulations.").

99 *See, e.g.*, CAL. EDUC. CODE § 99121(c)(1) (West 2012) ("This section shall not . . . [a]ffect a public or private postsecondary educational institution's existing rights and obligations to protect against and investigate alleged student misconduct or violations of applicable laws and regulations."); DEL.

policies,[100] or monitoring of accounts or equipment provided by the university.[101]

Enforcement Mechanisms

The social media protection laws that apply to educational institutions also have varying statutory enforcement mechanisms. The enacted bills in Arkansas and New Mexico provide no enforcement mechanism.[102] The laws in Michigan, New Jersey, Oregon, and Utah provide for civil actions.[103] Michigan's law caps damages at $1,000;[104] New Jersey's statute

CODE ANN. tit. 14, § 8105 (2012) ("This chapter shall not apply to investigations conducted by an academic institution's public safety department or police agency who have a reasonable articulable suspicion of criminal activity, or to an investigation, inquiry or determination conducted pursuant to an academic institution's threat assessment policy or protocol."); OR. REV. STAT. § 326.551 (2013) ("Nothing in this section prohibits an educational institution from: (a) Conducting an investigation, for the purpose of ensuring compliance with applicable law, regulatory requirements or prohibitions against student misconduct, that is based on the receipt of specific information about activity associated with a personal social media account; (b) Conducting an investigation authorized under paragraph (a) of this subsection that requires the student to share specific content on a social media account with the educational institution in order for the educational institution to make a factual determination about that content.").

100 *See, e.g.*, 105 ILL. COMP. STAT. ANN. 75 / 10 (2014) ("This Section does not apply when a post-secondary school has reasonable cause to believe that a student's account on a social networking website contains evidence that the student has violated a school disciplinary rule or policy.").

101 *See, e.g., id.* ("Nothing in this Section limits a post-secondary school's right to . . . monitor usage of the post-secondary school's electronic equipment and the post-secondary school's electronic mail without requesting or requiring a student to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website."); MICH. COMP. LAWS § 37.276(1) (2012) ("This act does not prohibit an educational institution from requesting or requiring a student to disclose access information to the educational institution to gain access to or operate any of the following: (a) An electronic communications device paid for in whole or in part by the educational institution. (b) An account or service provided by the educational institution that is either obtained by virtue of the student's admission to the educational institution or used by the student for educational purposes."); OR. REV. STAT. § 326.551 (2013) ("Nothing in this section applies to social media accounts intended for use solely for educational purposes at an educational institution or to social media accounts that are created by the educational institution and provided to the student if the student has been provided advance notice that the account may be monitored at any time by the educational institution."); UTAH CODE ANN. § 53B-25-202 (West 2013) ("This chapter does not prohibit a postsecondary institution from requesting or requiring a student to disclose a username or password to gain access to or operate the following: (a) an electronic communications device supplied by or paid for in whole or in part by the postsecondary institution; or (b) an account or service provided by the postsecondary institution that is either obtained by virtue of the student's admission to the postsecondary institution or used by the student for educational purposes.").

102 *See* ARK. CODE ANN. § 6-60-104 (2013); N.M. STAT. ANN. § 21-1-46 (2013).

103 MICH. COMP. LAWS § 37.278(1)-(2) (2012) ("An individual who is the subject of a violation of this act may bring a civil action to enjoin a violation of section 3 or 4 and may recover not more than $1,000.00 in damages plus reasonable attorney fees and court costs. Not later than 60 days before filing a civil action for damages or 60 days before adding a claim for damages to an action seeking injunctive relief, the individual shall make a written demand of the alleged violator for not more than $1,000.00. The written demand shall include reasonable documentation of the violation. The written demand and documentation shall either be served in the manner provided by law for service of process in civil

provides for compensatory and consequential damages with no cap;[105] Oregon's legislation provides for damages of $200 or actual damages, whichever is greater;[106] and Utah's bill provides that an aggrieved person shall not receive more than $500.[107] Delaware's legislation amends pre-existing legislation, but a separate, unique enforcement mechanism was not drafted into the bill.[108] Lastly, Illinois's law and Michigan's law provide for criminal offenses. Illinois's law punishes the post-secondary school or an agent of the post-secondary school with a petty offense.[109] Michigan's law makes violating the statute a misdemeanor.[110]

III. CONSIDERATIONS FOR STATE LEGISLATURES

There are two situations for which states have enacted bills to regulate social media access: 1) the employer-employee relationship; and 2) the student-university relationship. In light of the rapid increase in the use of internet technology and the rampant use of social media sites, these statutes attempt to provide some protection to online accounts. However, because of their numerous exceptions and broad reaching restrictions, the statutes have major issues. Legislatures with pending bills need to slow down and take more time to truly consider the effects of every provision included in a bill. Otherwise, similar to the laws already enacted, there will be unintended consequences. While a statute may prohibit an employer or academic institution from asking an employee, student, or applicant for his or her social media password, broad protection for situations in which the

actions or mailed by certified mail with sufficient postage affixed and addressed to the alleged violator at his or her residence, principal office, or place of business. An action under this subsection may be brought in the district court for the county where the alleged violation occurred or for the county where the person against whom the civil complaint is filed resides or has his or her principal place of business.") (footnote omitted); N.J. STAT. ANN. § 18A:3-32 (West 2013) ("In response to the action, the court may, as it deems appropriate, order or award . . . compensatory and consequential damages incurred. . ."); OR. REV. STAT. § 326.554 (2013) ("Any person claiming to be aggrieved by a violation of section 1 of this 2013 Act may file a civil action in circuit court for equitable relief or, subject to the terms and conditions of ORS 30.265 to 30.300, damages, or both. The court may order such other relief as may be appropriate. Damages shall be $200 or actual damages, whichever is greater."); UTAH CODE ANN. § 34-48-301 (West 2013) ("(1) A person aggrieved by a violation of this chapter may bring a civil cause of action against a postsecondary institution in a court of competent jurisdiction. (2) In an action brought under Subsection (1), if the court finds a violation of this chapter, the court shall award the aggrieved person not more than $500.").

104 MICH. COMP. LAWS § 37.278 (2012).

105 N.J. STAT. ANN. § 18A:3-32 (West 2012).

106 OR. REV. STAT. § 326.554 (2013).

107 UTAH CODE ANN. § 53B-25-201 (West 2013).

108 *See* DEL. CODE ANN. tit. 14, § 8101 (2012).

109 105 ILL. COMP. STAT. ANN. 75 / 20 (2014) ("A post-secondary school or an agent of a post-secondary school who violates this Act is guilty of a petty offense.").

110 MICH. COMP. LAWS § 37.278 (2012).

bill was not intended may also be included in the language of the statute. In other instances, the bills may also fail to protect a student or employee in a situation that the legislators likely wanted to protect.

In fact, as recently as August 2013, lawmakers approved amendments.[111] For example, Illinois recently passed Senate Bill 2306,[112] which amends Illinois's Right to Privacy in the Workplace Act, to provide that the restriction on requesting information applies only to an employee's "personal account[s]." [113] It also adds exceptions for employers to comply with the rules of self-regulatory organizations, and newly defines the term "personal account."[114]

Comparatively, Vermont's legislature revised Senate Bill 7 drastically before enactment; it does not provide an actual prohibition on employers, as introduced, but instead establishes a committee to "study the issue of prohibiting employers from requiring employees or applicants for employment to disclose a means to accessing the employee's or applicant's social network account."[115] This committee will be made up of two representatives for employers, two representatives from labor organizations, the Attorney General, the Commission of Labor, the Commission of Financial Regulation, the Commission of Human Resources, the Commissioner of Public Safety, the Executive Director of the Human Rights Commission, and a representative from the American Liberties Union of Vermont.[116] Ultimately, the Committee will make recommendations and even propose legislation.[117]

Other legislatures should consider this approach prior to enacting their own state bill in order to ensure that the bill is not only necessary, but that the scope of the bill is controlled and specific. First, Vermont's statute appropriately describes every individual that should be on the committee; the committee has representatives of different areas and specializations,

---

111 *See, e.g.*, S.B. 2306, 98th Gen. Assemb., Reg. Sess. (Ill. 2013), 2013 Ill. Legis. Serv. P.A. 98-501 (West) (amending Right to Privacy in the Workplace Act, 820 ILL. COMP. STAT. 55 / 10 (2012)).

112 S.B. 2306, 98th Gen. Assemb., Reg. Sess. (Ill. 2013), 2013 Ill. Legis. Serv. P.A. 98-501 (West).

113 820 ILL. COMP. STAT. 55 / 10 (2014).

114 *Id.*

115 S. 7, Gen. Assemb., 2013-2014 Leg. Sess. (Vt. 2013), 2013 Vt. Legis. Serv. 47 (West). The committee is to specifically examine the following: "(1) existing social networking privacy laws and proposed legislation in other states; (2) the interplay between state law and existing or proposed federal law on the subject of social networking privacy and employment; and (3) any other issues relevant to social networking privacy or employment." *Id.*

116 *Id.* The Attorney General, the Commission of Labor, the Commission of Financial Regulation, the Commissions of Human Resources, the Commissioner of Public Safety, and the Executive Director of the Human Rights Commission may have a designee for the committee. *Id.*

117 *Id.* The Committee is to report its findings and recommendations no later than January 15, 2014. *Id.* After it does so, the Committee will cease to function. *Id.*

which ensures that the law will not be biased in favor of certain parties.[118] Second, the law prescribes a specific time period for these findings, so there should be no delay by the committee, and also positively lays out the specific findings the legislature seeks to know.[119]

Although Vermont's approach has positive aspects, its requirement for the Committee to report findings and recommendations on or before January 15, 2014 is problematic. The application of these laws is still unclear. Therefore, the Committee was likely not given enough time to fully comprehend the repercussions of these laws before recommending new legislation.

Below, this comment will address provisions that legislators should consider when enacting legislation if they are going to continue to propose laws in this area.

A. Prohibitions/Restrictions

All of these bills must include the general restriction on requesting or requiring social media usernames or passwords, which all (but Vermont's) do.[120] However, all of the statutes should also include a retaliatory action provision to prohibit employers or academic institutions from taking adverse action against an individual for refusing to comply.[121] These two provisions would most directly address situations similar to Collins' interview and the City requests in Bozeman, Montana, on which the media focuses so frequently.[122]

Outside of the two main prohibitions, legislators should consider including a provision against shoulder surfing and against third-party review.[123] Third-party review restrictions are important because the restrictions against requesting social media information, and against taking adverse action, are alone not adequate to keep an employer from accessing the information they want. For example, some of the laws that regulate employers do not prohibit an employer from looking at the social media account of an individual who may be connected to the employee, applicant, or prospective employee for whom the employer seeks information. Therefore, the employer could easily use a third party, without requesting access from the employee, applicant or prospective employee, and gain the desired information. Because the employer could easily work around the

118 *Id.*

119 *Id.*

120 *See supra* notes 49, 80.

121 *See supra* notes 52-54, 81-82.

122 *See supra* Part II (A).

123 *See generally supra* notes 55-56, 85.

main restrictions by asking another a third party for assistance, without this provision, the law would be of no effect.

Further, if the state is experiencing situations where employees must sign-in and allow the employer to review the content of the account, a shoulder surfing provision would be an appropriate addition to the legislation. This provision would prevent employers and academic institutions from "working around" the restrictions and gaining the information by shoulder surfing instead.

That considered, other practitioners are concerned with shoulder surfing or third party access restrictions in these laws. For example, consider the scenario below:

> An employee reports to his employer that a coworker posted on his Facebook page that he intends to cause his supervisor harm. The employer has not only a right but also a legal duty to prevent workplace violence and would be legally obligated to take steps to prevent the coworker from carrying out the threat . . . . First, you'd have to investigate the employee's claim. Most often, that's done by asking the reporting employee to pull up his own Facebook page for the purpose of showing the coworker's allegedly threatening post, but the proposed law would prohibit you from doing that. Alternatively, you could ask the coworker whether he posted the threat, but if he denies it, you have no recourse and must take him at his word. Why? Because under the new law, you would be prohibited from "requiring or requesting" that he log into his account to clear up the allegation.[124]

Because of the clear negatives that could accompany additional restrictions, exceptions are necessary in the bill in order to mitigate the risks and harm placed on the employer.[125]

Comparatively, legislators should be cautious in including provisions that provide broad, generalized, and unspecific restrictions. For example, provisions stating that an individual cannot "divulge *any* personal social media,"[126] or that an educational institution cannot "[i]n *any way* inquire as to whether a student or applicant has an account or profile on a social networking website,"[127] restricts employers' or institutions' ability to request legitimate information.

First, this type of generalized provision goes against the common

---

124 Molly M. DiBianca, *Delaware Proposes Facebook Privacy Law*, DEL. EMP. L. BLOG (May 2013), http://www.delawareemploymentlawblog.com/2012/05/delaware-proposes-facebook-privacy-law.html.

125 *See infra* Part III (C).

126 CAL. EDUC. CODE § 99121 (West 2012) (emphasis added).

127 N.J. STAT. ANN. § 18A:3-30(b) (West 2012) (emphasis added).

understanding that anything in public domain may be reviewed.[128] Second, these provisions are unclear in terms of what they are aiming to restrict. For example, does merely asking an applicant whether he or she has a social media account violate the restriction in California's law about "*divulg[ing]* any social media"? And what if an employee "friends"[129] a supervisor on social media—does this also "*divulge*" social media unlawfully? Although the answers to these questions should surely be "no," the broad language may allow an individual to slip in these claims. Consider also the following hypothetical: a California employer requests that an applicant provide his or her email address in order to communicate after an interview. E-mail is included in California's social media definition,[130] so the employer likely violated the statute by "requesting" that the potential employee "divulge social media," merely by asking the individual to provide an email address.

Restrictions on adding employers or academic institutions to "friends" or a list of contacts are also too broad. First, these restrictions leave open the question of what happens if an employer is already a contact with an employee. Would the employer have to unfriend or delete that employee from their list of contacts? Also, in family businesses, what if a supervisor, who also happens to be a family member, asks an employee to add him or her to the social media account? These cases may run afoul of the newly enacted laws, although these issues were not necessarily the focus when drafting the restrictions. Moreover, imagine a teenager who begins working at his or her parent's place of employment. The parent is technically now a supervisor, and therefore, the parent may not be able to request that the teenager provide information related to his or her social media account—even if it is in a personal setting.[131]

Further, the application of these broad restrictions in regards to "professional" networking sites, such as "LinkedIn," is unclear. For example, assume that an employee's supervisor requested to "connect" to the employee's profile. Even though LinkedIn's purpose is to connect with

---

128 *See supra* notes 70, 97 (these provisions allow an employer to review any information that is on public domain); *see also* Gordon & Hwang, *supra* note 69 ("[T]here does not appear to be any viable basis for an applicant or employee to complain about an employer's access to publicly available social media content.").

129 The term "friend" can be used as a verb to mean "to add a person to one's list of contacts on a social-networking Web site." Greg Miller, *Redefining the word 'Friend' in the Social Media Age*, DIGITAL PIVOT, http://www.talentzoo.com/digital-pivot/blog_news.php?articleID=13060 (last visited Jan. 12, 2013); *see also* Bradley Shear, *The Legal Definition of a Facebook Friend*, SHEAR SOC. MEDIA L. (Jan. 8, 2010), http://www.shearsocialmedia.com/2010/01/legal-definition-of-facebook-friend.html.

130 CAL. LABOR CODE § 980(a) (West 2012).

131 *See generally* Margaret DiBianca *Why Delaware's Proposed Workplace Privacy Act Is All Wrong*, LEXISNEXIS COMMUNITIES: LABOR & EMP'T L. BLOG (May 15, 2012, 02:00 PM), http://www.lexisnexis.com/community/labor-employment-law/blogs/labor-employment-commentary/archive/2012/05/15/why-delaware-s-proposed-workplace-privacy-act-is-all-wrong.aspx.

such career-related contacts, and the employee would probably like to "connect," a supervisor may be acting unlawfully simply by making the request.

Lastly, the prohibition on requiring an individual to be added to a list of contacts is much more relevant in the university context, specifically as applied to student-athletes, not employees. Remember that the restriction against "friending" was initially proposed in order to combat monitoring programs and to stop coaches and professors from monitoring athletes' accounts.[132] However, this prohibition has consequences that are much broader. First, it precludes professors from asking students to use social media for discussion boards, or requesting students to post to blogs or other forums. This actually slows the progression of integrating social media use into academic situations. Second, it may also raise concerns between colleagues. Students may simultaneously *work* for an institution, maybe as a research assistant or teaching assistant, *and* attend classes at the institution as a *student*. However, because the student may be considered an *employee*, these individuals must now be careful in interacting with other students on social media.

B. Definitions

When drafting these laws, legislators must be specific, and need to appropriately develop terminology in order to target the purpose for which the legislation was drafted.[133] Legislators are advised to define "social media" or "social networking" as narrowly as possible. The first major definitional problem regarding the laws, in both the academic and employment contexts, arises when lawmakers attempt to define the word "social media" or "social networking." For example, California's definition of "social media" essentially covers *all* electronic activity, including, but not limited to, email, videos, photographs, blogs, podcasts, instant and text messages, online services or accounts, and Internet Web site profiles.[134] While the intent of the law was to prohibit access to certain types of social web sites, the California law is much broader. Legislators should avoid these broad range definitions because seemingly harmless questions, such as asking an attorney whether they have a legal *blog*, or asking a manager whether they have an *email* account to send documents to, could potentially cause a violation of the law.

---

132 *See supra* note 41; *see supra* Part II (A).

133 *See generally* Buckley, *supra* note 56, at 885 (proposing that in order to pass a federal protection bill, "Congress must also develop a coherent set of terminology so that the law is properly inclusive and can achieve its desired outcome. Perhaps one of the reasons that the PPA failed to become law is that the bill did not precisely define what content would be protected.").

134 CAL. LABOR CODE § 980(a) (West 2012).

Additionally, legislators have failed to consider that how social media or social networking sites work is constantly changing. For clarity and interpretation purposes, it may be helpful for statutes to include specific references to sites such as Facebook, Twitter, and MySpace in their definitions. Alarmingly, as of now, most definitions include protection for more than just social sites such as Facebook and Twitter, specifically including text messages or email.[135]

The second major definitional problem arises when the statutes exclude state and local law enforcement agencies, and other state agencies, from its definition of "employer." Because some laws exclude the Department of Corrections, County Corrections Departments, or any state or local law enforcement agency from the definition of "employers,"[136] enforcement in the very situations for which the bills were enacted is precluded. If the Colorado statute,[137] for example, was enacted to protect people like Collins,[138] the Law would fail to do so because Collins was applying for an *enforcement agency*, an agency not defined as an "employer" under the law.

The definition of "educational institution" or "academic institution" is also important for the scope of the legislation. Social media protection laws should apply *only* to postsecondary educational institutions or institutions of higher education. Michigan's Internet Privacy Protection Act is alarming because it construes "Educational institution" broadly, including not just institutions of higher education, but also kindergarten, nursery school, elementary and secondary schools.[139] Initially, Delaware also wanted its bill to protect students in kindergarten through the twelfth grade; however, there was a concern that the bill would protect bullies, and the provision was removed.[140]

Ultimately, a bill that protects secondary educational institutions rips institutional actors of power to monitor student safety. Consider a hypothetical where elementary-aged Student X tells Student Y something via a social media account that could harm the class. The teacher, nor institution, is allowed to request Student X or Student Y to show them his or her social media because it would likely be considered an unlawful request, improper access, or maybe even result in "shoulder surfing" or unlawful third-party access under some of the other prohibitions.[141]

---

135 *See, e.g.*, statutes cited *supra* notes 64, 93.

136 *See, e.g.*, *supra* notes 61-63.

137 COLO. REV. STAT. § 8-2-127 (2013).

138 *See supra* Part II (A).

139 MICH. COMP. LAWS § 37.272 (2012).

140 Hudson, *supra* note 42.

141 If a bill restricts access in secondary schools and nurseries, the bill should at least provide

C. Exceptions/Exemptions

Legislators must also more carefully consider exceptions prior to enacting a new law. First, future legislation should allow employers to comply with the requirements of federal, state, or local laws, rules or regulations, or the rules or regulations of self-regulatory organizations.[142] This will protect employers from opening themselves up to additional liability, and having to potentially choose between what law they want to follow, if the laws are in conflict. Arguments in opposition to the bills have claimed that they "conflict[] with the duty of securities firms to supervise, record, and maintain business-related communications as required by the Financial Industry Regulatory Authority (FINRA),"[143] and that "firms will be in the untenable position of having to violate either state law or their FINRA obligations."[144] By providing exceptions for compliance with state or federal laws or regulations, the opposition's arguments carry less weight.

However, the manner in which this exception is drafted can still cause concern. For example, Illinois's law states:

> Provided that the password, account information, or access sought by the employer *relates to a professional account*, and not a personal account, nothing in this subsection shall prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications as required under Illinois insurance laws or federal law or by a self-regulatory organization . . . .[145]

This provision is deceitfully narrow. By narrowing this exception to "professional accounts," unlike other statutes, it is not completely negating the restriction on asking for access information to allow compliance with other laws and obligations; instead, its limiting the exception to be similar to those which allow employers to access "professional accounts," or those accounts which were created or owned by the employer.

Secondly, legislators should consider an exception to allow employers to monitor accounts that they provide to the employee, as well as equipment

exceptions to allow authority figures to conduct investigations for safety purposes. *See also* Molly DiBianca, *How Delaware's Password-Privacy Bill Would Impact Teachers*, DEL. EMP. L. BLOG (May 25, 2012), http://www.delawareemploymentlawblog.com/2012/05/how-delawares-password-privacy-bill-would-impact-teachers.html (expressing concerns with Delaware's Workplace Privacy Act, H.B. 308, by posing a hypothetical; if a teacher was accused of inappropriate conduct with a student, and a bill restricts access to information by secondary schools and nurseries, the secondary school or nursery authority would be unable to question the teacher about the conduct to prove her innocence).

142 *See supra* note 73.

143 SEN. RULES COMMITTEE, THIRD READING, CAL. LAB. CODE § 980 (West 2012).

144 *Id.*

145 820 ILL. COMP. STAT. ANN. 55 / 10 (2014).

which is employer owned.[146] That being said, the bills with these exceptions must be more specific. The currently enacted legislation has "a lack of detail as to the degree in which employers can 'monitor' such [equipment and accounts]."[147] For example, the bills are unclear as to whether the allowed monitoring is limited to the amount of time spent on social media during work hours or whether that allowed monitoring can be extended to the content of employees' posts.[148] If the restriction is that employers cannot monitor the amount of time spent on social media, employees and applicants still have no protection over the content of their posts, which was arguably the purpose of the statutes to begin with.

Further, the laws must be broad enough to allow employers to protect the workplace from unlawful or unsafe behaviors. For example, Michigan's law states that an employer may investigate whether there is information about activity on the employee's personal account for the purpose of guaranteeing compliance with restrictions on work-related employee misconduct.[149] This exception will allow an employer to ask employees for login information regarding general misconduct, including inappropriate, derogatory, or discriminatory postings.[150] The exception must also be broad enough to allow employers to use personal social media in a way to assess and correct illegal or inappropriate workplace conduct.[151] These exceptions have been criticized because in what seems to be an effort to restrict general investigations, the statute requires "an employer to have 'specific information about activity on the employee's personal internet account' that may violate laws, regulatory requirements or constitute work-related misconduct, in order to conduct an investigation."[152] Ultimately, "these provisions may needlessly restrict an employer's ability to provide an environment free from unlawful or unsafe behavior."[153]

---

146 *See* statutes cited *supra* note 74.

147 Tina A. Syring-Petrocchi, *Texas Legislature Will Consider Employers' Ability to Access Social Media Passwords*, NAT'L L. REV. (Jan. 9, 2013), http://www.natlawreview.com/article/texas-legislature-will-consider-employers-ability-to-access-social-media-passwords.

148 *Id.*

149 MICH. COMP. LAWS § 37.275 (2012).

150 *See id.*; *see also* William Balke & Philip Gordon, *Michigan's New "Internet Privacy Protection Act" Sets Limitations for Employers and Employees*, LITTLER (Jan. 4, 2013), http://www.littler.com/publication-press/publication/michigans-new-internet-privacy-protection-act-sets-limitations-employe ("This exception would, for example, permit an employer to ask an employee for login credentials where a coworker reports a social media post that threatens workplace violence or contains racially derogatory comments about the coworker.").

151 Cynthia G. Burnside & Lindsay Dennis Swiger, *The ABC's of Social Media for Corporate Counsel*, *in* A.B.A. CORP. COUNSEL CLE SEMINAR (2013), *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2013_corporate_counsel_cleseminar/11_1_the_abcs_of_social_media.authcheckdam.pdf.

152 *Id.*

153 *Id.*

In addition, lawmakers have failed to consider the rapid increase of Bring Your Own Device ("BYOD")[154] practices among businesses. For example, the exceptions do not provide for what happens when an employee's *personal* device would be searchable by an employer because the employee's *personal* device uses the *employer's network* during business hours to connect or access personal social media. Alternatively, it is unclear what happens when an employee takes home an *employer-owned* electronic device after hours, but uses such device to check their *personal* networking sites or to connect to their *personal* network.

Legislators should not exempt law enforcement agencies or correctional agencies from the provisions of these laws.[155] Similar to excluding these types of agencies from the term "employer,"[156] exempting these agencies from the restrictions under the legislation, such as that in New Mexico's legislation,[157] would exclude protection in Collins' situation, the very situation in which these bills were intended to protect.

Finally, although some of the bills specifically provide an exception on whether an employer or educational institution can search for information about an individual's social media account that is in the public domain,[158] others do not. While there is nothing to suggest that an employer or academic institution could not use public information,[159] whether a practitioner should advise an employer or academic institution from prohibiting all searches is unclear. This is an exception that legislators should include for clarity purposes.

D. Enforcement

One of the biggest issues regarding the social media password protection legislation includes the varying enforcement mechanisms if the statute is violated. Legislators must include an enforcement mechanism in the legislation in order for it to be effective.

Civil actions as the only enforcement mechanism may be troublesome if the bill does not also provide for attorney's fees. Because some of the bills cap recovery, with none of the caps being more than $1,000,[160] a

154 Nadeem Unuth, *Bring Your Own Device – At Work or For a VoIP Service*, ABOUT.COM, http://voip.about.com/od/hardware/a/What-Is-BYOD.htm (last visited Jan. 10, 2013) ("BOYD is another acronym that is likely to stand as a word in itself shortly. It stands for Bring Your Own Device and it means exactly that – bring your own piece of hardware when you come to our network or premises.").

155 *See* COLO. REV. STAT. § 8-2-127 (2013); N.M. STAT. ANN. § 50-4-34 (2013).

156 *See* COLO. REV. STAT. § 8-2-127 (2013).

157 N.M. STAT. ANN. § 50-4-34 (2013).

158 *See* statutes cited *supra* notes 70, 97.

159 *See* Gordon & Hwang, *supra* note 69.

160 *See, e.g.*, MICH. COMP. LAWS § 37.278 (2012) (capping recovery at $1000); UTAH CODE ANN. § 34-48-301 (West 2013) (capping recovery at $500). *Cf.* WASH. REV. CODE § 49.44.205 (West

plaintiff may spend more on representation than he or she could recover in bringing suit.[161] This may cause deterrence to individuals who would bring these types of actions. Moreover, large employers, such as multi-billion dollar companies, may not want to take the risk or take on the costs of such litigation unnecessarily, even if they had a valid defense under one of the many exceptions to the legislation. Instead, they may just pay the $1,000 fee. While the $1,000 is a slight deterrence, it does not do nearly enough to actually provide any protection to an applicant or employee.

The Michigan law's misdemeanor provision is also worth discussing. It states, "[a] person who violates section 3 or 4 is guilty of a misdemeanor punishable by a fine of not more than $1,000.00."[162] The statute leaves open the question of whether the fine will be placed on the specific individual that requests the information (in an individual capacity) or whether it will be placed on the employer.[163]

Lastly, administrative remedies are likely the best enforcement mechanism for these types of laws. Administrative remedies will provide an individual redress, if necessary, without all of the litigation expenses and time that usually accompany civil private rights of action. This is important considering the relatively small range of damages[164] that are likely to occur under the new legislation. Drafting specific administrative procedures in the laws will provide the clearest instructions for attorneys when approaching this new, and confusing,[165] legislation.

IV. LEGISLATION FOR A PROBLEM THAT DOES NOT EXIST

Finally, before deciding what provisions to include in the legislation,

2013) (allows a court to award actual damages and a penalty in the amount of five hundred dollars).

161 *See generally How, and How Much, Do Lawyers Charge?*, LAWYERS.COM, http://research.lawyers.com/how-and-how-much-do-lawyers-charge.html (last visited Jan. 25, 2014) ("In rural areas and small towns, lawyers tend to charge less, and fees in the range of $100 to $200 an hour for an experienced attorney are probably the norm. In major metropolitan areas, the norm is probably closer to $200 to $400 an hour. Lawyers with expertise in specialized areas may charge much more. In addition, you can expect to be charged at an hourly rate for paralegals and other support staff. A good paralegal's time, for example, may be billed out at $50 to a $100 an hour or perhaps more. It would not be unusual for a legal secretary's time on things like document production to be billed out at perhaps $25 to $50 an hour. What About Expenses and Court Costs? Little things add up. Carefully discuss with your lawyer anticipated miscellaneous costs so that you can estimate those costs up front and avoid any unpleasant surprises. Be prepared to scrutinize court costs, filing fees, secretarial time, and delivery charges.").

162 MICH. COMP. LAWS § 37.278 (2012).

163 *Id.*

164 *See supra* note 160 for statutes with recovery caps of no more than $1000. *See also* OR. REV. STAT. § 326.554 (2013) (allowing damages of at least $200 or actual damages, whichever is greater).

165 *See* Gordon, Spataro, & Simmons, *supra* note 56 (calling the new legislation a "patchwork" of laws and recognizing that the differing provisions in each laws make it difficult for multi-state employers to develop general and uniform strategy).

lawmakers should make a true determination of whether these bills are necessary. Arguments exist that they are not.[166]

Although the ACLU, other media sources, and social media sites called for urgent action in order to protect employees, students, or applicants from these aggressive hiring and admission practices,[167] in actuality, these types of requests from employers or colleges are few and far between.[168] Frankly, the media successfully unsettled lawmakers about a situation that rarely occurs. For example, in the "media frenzy of spring 2012"[169] that covered the stories of employers requesting access information, *no* article established that it is routine for private employers to ask for login credentials.[170]

An analysis of the language and history of the legislation demonstrates how rarely a situation occurs where an individual is requested to provide his or her social media password or username. Certain state legislatures fail to recognize a single instance in committee reports or legislative history that details a situation that occurred in their own state. For example, the California law's legislative history details Maryland's dilemma between Collins' and the Department of Public Safety and Corrections as a reason for enacting its own legislation.[171] While Maryland lawmakers should, and did, use this situation as an argument to rapidly enact a social media protection bill,[172] California's law does not, on its face or in its legislative history, describe a single instance where California's *own* agencies are

166 *Id.*; Philip Gordon & Lauren Woon, *Re-Thinking and Rejecting Social Media "Password Protection" Legislation*, 12 Social Media L. & Pol'y Rep. (BNA) No. 1, at 1 (July 3, 2012), http://www.bna.com/uploadedFiles/Content/Press/ReThinking_and_Rejecting_Social_Media_SMLR.pdf.

167 *See, e.g.*, Ategah Khaki, *Status Update: Employers Asking For Your Facebook Password Violates Your Privacy and the Privacy of All Your Friends, Too*, ACLU: BLOG OF RIGHTS (Mar. 22, 2012, 2:49 PM), https://www.aclu.org/blog/technology-and-liberty/status-update-employers-asking-your-facebook-password-violates-your; *Your Facebook Password Should Be None of Your Boss' Business*, ACLU: BLOG OF RIGHTS (Mar. 20, 2012), https://www.aclu.org/blog/technology-and-liberty/your-facebook-password-should-be-none-your-boss-business; Doug Gross, *Facebook speaks out against employers asking for passwords*, CNN (Mar. 23, 2012, 10:25 AM), http://www.cnn.com/2012/03/23/tech/social-media/facebook-employers/.

168 Gordon & Woon, *supra* note 166. *See also* Steven Palazzolo, *What A Way to End the Year!*, MICH. EMP. L. (Dec. 30, 2012), http://zomichiganemploymentlaw.wnj.com/?cat=14 ("I read somewhere, I can't remember where, that this bill was a solution looking for a problem. I'm inclined to agree. I represent all kinds of clients all over this state, big and small, and I don't know of a single one ever requiring that an employee or a candidate for employment turn over his or her Facebook password to get or keep a job.").

169 Gordon & Woon, *supra* note 166.

170 *Id.* Furthermore, 99% of C-suite executives, corporate counsel, and human resource professionals from corporations throughout the United States answered in the negative when asked whether their organization requested social media login information as part of the hiring process. *Id.*

171 *See* SEN. RULES COMMITTEE, THIRD READING, *supra* note 143.

172 *See* MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012).

requiring this type of information, or that California's *own* employees are experiencing the same type of requests.

From both a legal and social perspective, adequate forces are also already in place to prevent employers from requesting social media access information. Addressing social boundaries first, generally, qualified and talented prospective employees would likely not be interested in working for an employer that requires this type of information. Those same employees likely have a variety of employment choices and would probably choose a company that does not attempt such risky hiring practices, or practices that arguably infringe on their privacy. As demonstrated by the events in Montana and Maryland,[173] public outcry and attention was adequate pressure to force the employers in both instances to modify or completely terminate the hiring practice.[174]

Additionally, employers may face legal ramifications and risks if they require social media access information. Under the Stored Communications Act, the courts have held that accessing unauthorized sites as an unintended user could result in punitive damages against an employer.[175] The National Labor Relations Board has also afforded protection to employees under the National Labor Relations Act, finding that employees participating in discussions through social networks constituted protected activity.[176]

Furthermore, practitioners specifically recommend to their employer-clients not to require social media login information because doing so only exposes the employer to potential liability and risks.[177] Specifically, claims against the employer for discrimination under Title VII may arise if an employer uses certain information in a hiring decision, such as an individual's race, religion, or gender, after finding that information on social media sites.[178] Not only should employers be cautious due to existing legal doctrines and negative social stigmas, but these types of requests from

---

173 *See supra* Part II (A).

174 *Id; supra* notes 32, 40.

175 Pietrylo v. Hillstone Rest. Grp., No. CIV.06-5754(FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

176 *See Am. Med. Response of Conn., Inc.*, 2010 N.L.R.B. GCM LEXIS 63 (2010).

177 Lisa Quast, *Social Media, Passwords, and the Hiring Process: Privacy and Other Legal Rights*, FORBES (May 28, 2012, 8:56 AM), http://www.forbes.com/sites/lisaquast/2012/05/28/social-media-passwords-and-the-hiring-process-privacy-and-other-legal-rights/. *See also* Buckley, *supra* note 56, at 883 ("Employers who access password-protected social media run the risk of violating Title VII because social media are replete with information relating to employees' and applicants' membership in protected classes. Privately configured messages can reveal protected characteristics that are not immediately apparent to employers, and they can also reveal characteristics that employers are prohibited from inquiring about, such as religion and national origin. Allowing employers unfettered access to applicants' social media substantially increases the risk that they will illegally consider impermissible criteria while making employment decisions.").

178 Quast, *supra* note 177. These members are of a protected group.

employers are also forbidden by websites' privacy policies.[179]

States are also enacting protection over *employers* even though some of the concern has been due to recent developments in the *student-university* relationship. For example, Maryland's law recognizes that part of the lawmakers' decision to enact was due to the possibility that companies that currently monitor collegiate student-athletes could begin monitoring employees' social media activity.[180] However, nothing indicates that Maryland companies intend to begin monitoring employees' sites using these software packages. In addition, although Maryland lawmakers are seemingly concerned with the way that these companies monitor *students*, the state has not yet enacted a law that applies in an *educational* setting.

Further, most stories involving education institutions were concerned about students in extracurricular activities, specifically coaches requiring student athletes to allow a coach to monitor an athlete's social media accounts or by using monitoring software.[181] However, not all of the educational bills, including the laws from California[182] and Michigan,[183] provide prohibitions against monitoring or tracking software.

Moreover, some educational institutions have recognized that they do not engage in the activities prohibited by the bills.[184] For example, according to the public postsecondary educational institutions in California, they do not currently engage in the activities prohibited by California's legislation.[185] While other private postsecondary education institutions may request that "athlete students provide information on their social media accounts," a lack of clarity exists in terms of what type of information is actually being requested.[186]

Finally, in terms of the laws that restrict educational institutions, legislators should consider that generally these statutes prohibit what may be useful and valid practices. Delaware's statute, for example, restricts an academic institution from monitoring or tracking personal electronic

---

179 For example, it goes against Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password. *See Protecting Your Passwords and Your Privacy*, FACEBOOK (Mar. 23, 2012, 5:32 AM), http://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057. *See also* Gross, *supra* note 167.

180 MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2013).

181 *See supra* Part II (A).

182 CAL. EDUC. CODE §§ 99120-22 (West 2013).

183 MICH. COMP. LAWS §§ 37.271-278 (2012).

184 *See* SEN. RULES COMMITTEE, UNFINISHED BUSINESS, S.B. 1349, 2011-2012 Reg. Sess. (Aug. 17, 2012) (Yee).

185 *Id.*

186 *See id.*

communication devices.[187] Academic institutions are also restricted from adding the employer or its representatives to their personal social networking accounts or accessing a student's or applicant's site indirectly through another person who is connected to that site.[188] However, students have found these practices to be for their own benefit. For example, in asking students at the University of Pennsylvania about their opinions on it being mandatory to "friend" their coach, the students responded that they did not feel it was an invasion of privacy, nor were they offended by the use of the practice.[189] Instead, the students felt that prohibiting a coach from monitoring social media would be "detrimental" to the reputation of the program and could place burdens on other students.[190] Therefore, general opinion may call for legislators to re-think this legislation.

V. CONCLUSION

The increased prevalence of social media in society and the widespread use of Internet technology has brought new considerations to state legislatures. At the end of 2013, social media password protection legislation had been introduced or was pending in at least thirty six states. Although the laws were likely drafted with good intentions, the enacted bills have instead created further confusion. The statutes not only provide for different protections, enforcement, and damages, but the bills also create an open question of necessity. Further, the legislation's language is flawed in a number of ways, including a lack of clarity in terminology, a failure to include a workable enforcement mechanism, and exemptions for agencies that were surrounding the password controversy to begin with.

Moving forward, lawmakers must carefully consider each provision included in a bill, in order to ensure that the law will do exactly what it is intended to do, without unintended consequences. Moreover, lawmakers must more carefully assess the types of provisions and restrictions that they

187 DEL. CODE ANN. tit. 14, § 8103(c) (2012).

188 *Id.*

189 Molly DiBianca, *Delaware Law Protects Privacy of Student Facebook Posts*, DEL. EMP. L. BLOG (July 24, 2012), http://www.delawareemploymentlawblog.com/2012/07/delaware-law-protects-privacy-of-student-facebook-posts.html.

190 *Id.* The students provided the following hypothetical:

> Student X, a member of the track team, sells anabolic steroids and "advertises" his conduct via Facebook. If the student-player is required to be Facebook friends with the team's coach, such conduct could be quickly detected and turned over to law enforcement. Without the watchful eyes of a school authority, it would be up to fellow students and team members to turn over the student to police or school authorities. Although it's nice to think that this would happen, I think it's fair to say that there's hardly any guarantee.If, however, the student is arrested and a public scandal ensues, the team loses credibility and support from the university community, fellow students, and from donors. The loss of donor support can result in decreased funding to the program, which can, in turn, translate into less scholarship money. Which harms—not helps—student athletes.

want to include, why they are protecting circumstances such as the employment relationship, the student-university relationship, or other relationships that may arise in the future. Lawmakers must also consider how certain exemptions or exceptions may affect the protection that is projected by such a statute.