THE LEGISLATIVE RESPONSE TO EMPLOYERS’ REQUESTS FOR PASSWORD DISCLOSURE

By Jordan M. Blanke*

Introduction

As often happens when a new societal problem emerges, there has been a quick legislative response. A dozen states have already passed legislation prohibiting an employer from requesting or requiring an employee or a prospective employee from disclosing password information that would provide access to one’s personal social media account. This article will explore the incidents that led to this response and will compare the various approaches taken by these twelve states and by bills proposed in twenty-seven other states and the federal government.

Background

In 2010, Robert Collins was reapplying for a job as a security guard at the Maryland Department of Public Safety and Correctional Services.1 As part of the recertification process, there was “a request – or to me, rather, a demand . . . for my Facebook e-mail and login information,” said Collins.2 The Department had initiated the practice of asking prospective employees to voluntarily provide user names and passwords to social media sites in order to perform background checks and to investigate possible gang affiliations.3 “I understood the investigator to be saying that I had . . . to hand over my Facebook log-in and password,” said Collins.4 He was stunned but complied with the request: “I needed my job to feed my family.”5

---

* Professor of Computer Information Systems and Law, Stetson School of Business and Economics.
Mercer University, Atlanta, GA

1 See Meredith Curtis, Want a Job? Password, Please!, ACLU (Feb. 18, 2011), archived at www.perma.cc/0XHR45NkASc (providing the background information for a complaint sent to the Maryland Public Safety Secretary).
2 See id. (explaining requirement for current employees undergoing recertification to supply social media network usernames and passwords for background checks).
3 See Aaron C. Davis, Md. Corrections Department Suspends Facebook Policy for Prospective Hires, THE WASHINGTON POST (Feb. 22, 2011), archived at www.perma.cc/0n28sWTU8GK (explaining Maryland corrections system screening of employees to combat gang violence).
4 Id.

Copyright © 2014 Journal of High Technology Law and Jordan Blanke. All Rights Reserved. ISSN 1536-7983.
This incident publicized a growing practice among some employers to ask prospective employees for access to their social media accounts. In March 2012, Facebook itself addressed the problem in a post by its Chief Privacy Officer:

The most alarming of these practices is the reported incidents of employers asking prospective or actual employees to reveal their passwords. If you are a Facebook user, you should never have to share your password, let anyone access your account, or do anything that might jeopardize the security of your account or violate the privacy of your friends. We have worked really hard at Facebook to give you the tools to control who sees your information.

As a user, you shouldn’t be forced to share your private information and communications just to get a job. And as the friend of a user, you shouldn’t have to worry that your private information or communications will be revealed to someone you don’t know and didn’t intend to share with just because that user is looking for a job. That’s why we’ve made it a violation of Facebook’s Statement of Rights and Responsibilities to share or solicit a Facebook password.

We don’t think employers should be asking prospective employees to provide their passwords because we don’t think it’s the right thing to do.

State Senator Ronald N. Young, one of the sponsors of the bill that was enacted in Maryland, stated “he thought the problem was ‘starting to be widespread’ and that he’s ‘hearing of more and more cases.’” Similarly, Assemblywoman Nora Campos, one of the sponsors of the bill, expressed concern over the trend of employers requesting passwords from prospective employees. She noted that this practice is not only unethical but also potentially illegal under Maryland law.

---


7 See id. (stating that employers should not be asking future employees for social media passwords).

8 See Charles Cooper, Fork Over Your Facebook Log-on or You Don’t Get Hired. What?, CNET NEWS (Mar. 24, 2012), archived at www.perma.cc/ozNLm8DPB3F (quoting Senator Ronald N. Young on increased frequency of employers soliciting private social network information).
sponsors of the California bill that became law, stated that it would be a “preemptive measure” that would offer guidelines to... [protect] private information behind... [our] ‘social media wall.’”9 She stated, “Our social-media accounts offer views into our personal lives and expose information that would be inappropriate to discuss during a job interview.”10 Campos’ office indicated that more than 100 cases currently before the National Labor Relations Board involve employer workplace policies regarding social media.11

Two U.S. Senators, Charles Schumer and Richard Blumenthal, asked the Department of Justice and the Equal Employment Opportunity Commission to determine whether this type of practice violates existing federal law.12 This question was addressed to some extent a couple of times in cases involving current employees, rather than perspective employees.13 In Konop v. Hawaiian Airlines, Inc.,14

---


10 See Katz, supra note 9 (quoting Assemblymember Campos on exposure of personal lives due to access of social-media account information).

11 See Dara Kerr, Calif. Law Passed to Halt Employer Snooping on Social Media, CNET NEWS (Sept. 27, 2012), archived at www.perma.cc/P43X-YNBA (reporting Governor Brown’s support of the bill).

12 See Anita Ramasastry, Can Employers Legally Ask You for Your Facebook Password When You Apply for a Job? Why Congress and the States Should Prohibit This Practice, VERDICT (Mar. 27, 2012), archived at www.perma.cc/8CR-8TS2 (reporting on the Congressional response to the problems created by such employer requests).


14 See 302 F.3d 868, 878-79 (9th Cir. 2002) (holding third party access to electronically stored communications does violate the SCA).
and Pietrylo v. Hillstone Restaurant Group, courts wrestled with the question of whether “coerced” access to restricted web sites violated the federal Stored Communications Act (SCA). In decisions that are probably limited to their unique factual situations, both courts held that the employers’ access to employees’ websites were unauthorized under the SCA. It is questionable, however, whether the SCA would be of much use to employees or prospective employees who, presumably, would be giving permission to access their social media sites, and would have to argue that their permission was coerced or that the access was unauthorized.

The Legislative Response

In an effort to nip this growing practice in the bud, four states in particular have proposed a variety of bills, some of which passed by 2012; of these four, Illinois was the first to propose a bill on May 18, 2011, followed by Maryland on February 2, 2012, California on February 22, 2012, and Michigan on March 29, 2012. These bills became law on August 1, 2012, May 2, 2012, September 27, 2012, and December 28, 2012, respectively. The Maryland law

15 See No. 06-5754, 2009 WL 3128420, at *10-11 (D. N.J. Sept. 25, 2009) (finding that managers’ use of password was unauthorized by employee and thus potentially in violation of the SCA).
16 See 18 U.S.C. §§ 2701-2712(c) (2012) (stating the exceptions to unlawful access to stored communications); Konop, 302 F.3d at 884 (explaining triable issues obtaining information to assist and coerce Konop); Pietrylo, 2009 U.S. Dist. LEXIS 88702, at *8-9 (questioning whether coerced access to restricted web sites violated the SCA).
17 See Konop, 302 F.3d at 880 (reversing district court’s decision to conclude that Hawaiian Air did violate SCA); Pietrylo, 2009 WL 3128420, at *10-11 (denying employer’s motions for dismissal and for judgment as a matter of law).
18 See 18 U.S.C. §§ 2701-2712(c) (2012) (applying only to individuals who have not given their consent).
23 See Ill. H.B. 3782 (displaying a bill that came into law on August 1, 2012); Md. S.B. 443 (displaying a bill that came into law on May 2, 2012); Cal. A.B. 1844
became effective on October 1, 2012, the Michigan law on December 28, 2012, and the Illinois and California laws on January 1, 2013. An additional nine states (Arkansas, Colorado, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and Washington) enacted legislation in 2013. Twenty-seven other states and Congress have considered or are considering similar bills. This paper will compare and discuss the various ap-

2013) (barring employers from requesting or requiring an employee or applicant to disclose personal account information); S.B. 53, Reg Sess., archived at www.perma.cc/0SrLtS8s68F (Kan. 2013) (prohibiting employers from requesting passwords of employees or applicants for employment); H.B. 314, 2013 Leg., Reg. Sess., archived at www.perma.cc/T2KQ-5M53 (La. 2013) (protecting employees’ privacy with respect to social media account information); H.P. 838, 126th Leg., 1st Reg. Sess., archived at www.perma.cc/0truEnGGwAGF (Me. 2013) (protecting social media privacy in school and the work place); H.B. 1707, 188th Gen. Ct., Reg. Sess., archived at www.perma.cc/0LRComNQ9Ng (Mass. 2013) (proposing that employees cannot be compelled to provide access to personal social media accounts or services to employers); S.B. 852, 188th Gen. Ct., archived at www.perma.cc/0HJjAqw8DMA (Mass. 2013) (denying employers access to employees’ personal social media accounts); S.B. 872, 188th Gen. Ct., archived at www.perma.cc/058FTskjoJe (Mass. 2013) (forbidding employers from requesting or require an employee to disclose any means for viewing or accessing information contained on a personal electronic account or service); H.F. 293, 88th Reg. Sess., archived at www.perma.cc/0pVfo7xB2Zn (Minn. 2013) (prohibiting employers from requiring prospective employees from providing social network passwords as a condition of employment); H.F. 611, 88th Reg. Sess., archived at www.perma.cc/L268-QD3N (Minn. 2013) preventing disclosure of social network passwords as a condition of employment); S.F. 596, 88th Reg. Sess., archived at www.perma.cc/0w2URcwWk7J (Minn. 2013) (proposing an amendment to Minnesota statute to protect employees’ social networking privacy); H.B. 165, 128th Leg.Reg. Sess., archived at www.perma.cc/0DTTrBS5jFre (Miss. 2013) (penalizing employers who demand access to employees’ social networking sites); H.B. 115, 97th Gen. Assemb., 1st Reg. Sess., archived at www.perma.cc/0tWntj4vrUT (Mo. 2013) (amending state regulation as it pertains to the disclosure of private information to employers); H.B. 286, 97th Gen. Assemb., 1st Reg. Sess., archived at www.perma.cc/0RcpM2Emrwx (Mo. 2013) (amending state regulation as it pertains to an employer’s request for account information from a social networking website); H.B. 706, 97th Gen. Assemb., 1st Reg. Sess., archived at www.perma.cc/0Gn5JXfDg81 (Mo. 2013) (changing the existing regulations to protect employee’s passwords); H.B. 1020, 97th Gen. Assemb., 1st Reg. Sess., archived at www.perma.cc/0xFq5aT65jH (Mo. 2013) (limiting requests by employer’s for social networking website account information from employee’s); S.B. 164, 97th Gen. Assemb., 1st Reg. Sess., archived at www.perma.cc/0r3tN4DDVN5 (Mo. 2013) (adopting employee password protection legislation); S.B. 195, 63d Leg., Reg. Sess., archived at www.perma.cc/0fA2fl1FDaC (Neb. 2013) (protecting employee rights as they pertain to social networking sites, electronic communication, and passwords); H.B. 379, 2013 Gen. Ct., Reg. Sess., archived at www.perma.cc/08n5JDPNkT (N.H. 2013) (prohibiting requested disclosures of social media account passwords); A.B. 443, Reg. Sess., archived at www.perma.cc/0qyEpCm3zpQ (N.Y. 2013) (discontinuing the practice of requiring applicants or employees of educational institutions to disclose personal account
To Whom do the Prohibitions Apply?

All of the laws and bills restrict an “employer” from acting in a certain manner. About half of the states that have enacted legisla-

information); S.B. 2434, Reg. Sess., archived at www.perma.cc/0BbBCm9rWgo (N.Y. 2013) (prohibiting educational institutions from demanding personal account access information from perspective applicants and employee’s); H.B. 846, 2013 Gen. Assemb., Reg. Sess., archived at www.perma.cc/0A9RifwmRbf (N.C. 2013) (preventing colleges from requiring access information to individuals social media and personal electronic mail accounts); H.B. 1455, 63d Leg. Assemb., Reg. Sess., archived at www.perma.cc/0GUE4nMuX3v (N.D. 2013) (establishing workplace privacy regulations for social media and internet accounts); S.B. 45, 130th Gen. Assemb., Reg. Sess., archived at www.perma.cc/0Huv6HSk8Ze (Ohio 2013) (denying mandated access to private electronic accounts of employees by employers); H.B. 1130, 2013 Gen. Assemb., Reg. Sess., archived at www.perma.cc/0jRVpzXjfa4 (Pa. 2013) (enacting the protection of private or personal account information of employee’s from their employers); H.B. 5255, Gen. Assemb., archived at www.perma.cc/0kwq9mr5YB (R.I. 2013) (refusing to allow social media account access to employers’); S.B. 0493, Gen. Assemb., (R.I. 2013) (reiterating the purpose of H.B. 5255, as both bills are identical); H.B. 5105, 119th Leg. Sess., archived at www.perma.cc/0NpuH9nJwHY (S.C. 2011-12) (denying employer access to employee’s social networking accounts); H.B. 318, 83d Reg. Sess. (Tex. 2013) (establishing as an unlawful employment practice the requesting of personal account access information); H.B. 451, 83d Reg. Sess. (Tex. 2013) (restricting access to certain personal online accounts through electronic communication devices); S.B. 118, 83d Reg. Sess. (Tex. 2013) (requiring or requesting personal account information is prohibited); S.B. 416, 83d Reg. Sess. (Tex. 2013) (recognizing as unlawful employment practice the requesting or requiring of employees to divulge personal account information); H.B. 2966, 81st Leg., 1st Sess., archived at www.perma.cc/0lRgXkY5LRR (W. Va. 2013) (explaining the prohibited actions of employers as it relates to access to employee account information); A.B. 218, Leg. Sess., archived at www.perma.cc/0ucBVf5zTY8 (Wis. 2013-14) (requesting access to an employee’s personal internet account is prohibited); S.B. 223, Leg. Sess. (Wis. 2013-14) (reiterating the purpose of A.B. 218, as both bills are identical); H.R. 5050, 112th Cong., 2d Sess. (2012) (establishing the Social Networking Online Protection Act, also known as SNOPA). Similar legislation restricting certain actions by colleges and universities with regard to students has been passed by Arkansas, California, Delaware, Michigan, New Mexico, New Jersey, Oregon and Utah, and proposed by several other states, but is beyond the scope of this article.
tion specifically define the term “employer” within the statute. Maryland defines an employer as “a person engaged in a business, an industry, a profession, a trade, or other enterprise in the state” or “a unit of state or local government.” It provides that employer “includes an agent, representative, and a designee of the employer.”

Arkansas, Colorado, Michigan, and New Jersey use basically the same language, with Colorado specifically excluding “the department of corrections, county corrections departments, or any state or local law enforcement agency” and New Jersey specifically excluding the “Department of Corrections, State Parole Board, county corrections departments, or any State or local law enforcement agency.”

Utah defines an “employer” as “a person, including the state or a political subdivision of the state, that has one or more workers or operators employed in the same business, or in or about the same establishment, under any contract of hire, express or implied, oral or written.” Washington has an even more detailed definition:

"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.

---

38 MD. CODE ANN. at § 3-712(a)(4)(i)(1).
39 Id. at § 3-712(a)(4)(i)(2).
40 Id. at § 3-712(a)(4)(ii).
41 See ARK. CODE ANN. at § 11-2-124(a)(2) (providing that “employer” includes an agent, representative, or designee of the employer).
42 See COLO. REV. STAT. at § 8-2-127(c) (providing that “employer” includes his or her agent, representative, or designee).
43 See Mich. Pub. Acts 478 at § 2(c) (providing that “employer” includes an agent, representative, or designee).
44 See N.J. STAT. ANN. § 34:6B-5 (West 2013) (providing that “employer” includes an agent, representative, or designee)
45 COLO. REV. STAT. at § 8-2-127(c).
47 UTAH CODE ANN. at § 34-48-102(2).
48 WASH. REV. CODE ANN. at § 49.12.005.
Some of the bills propose a broader scope for the actor, such as Minnesota, which would prohibit any “person, whether acting directly or through an agent,” and Ohio, which would prohibit any “employer, employment agency, personnel placement service, or labor organization.” The definition proposed by Congress in the Social Networking Online Protection Act (SNOPA) would include “any person acting directly or indirectly in the interest of an employer in relation to an employee or an applicant for employment.”

Who Is Protected?

The actions prohibited by the “employer” (generally) pertain to “employees” and to “prospective employees.” Also, Colorado and Washington define an “applicant” as an “applicant for employment.” Interestingly, New Mexico’s law protects only a prospective employee, not a current employee. Other than this last distinction, there appears to be little significance in the choices of terms used.

What is Prohibited?

Although there are multiple variations of law implemented or proposed, very generally speaking, an employer is prohibited from requesting or requiring from an employee or an applicant the disclosure of a user name or password in order to gain access to a personal account or social networking site.

49 Minn. S.F. 596; S.F. 484, 88th Leg., 1st Reg. Sess. (Minn. 2013); Minn. H.F. 611; Minn. H.F. 293.
50 Ohio S.B. 45.
52 See, e.g. ARK. CODE. ANN. at § 11-2-124 (stating that prohibited actions pertain to current and prospective employees alike); Neb. L.B. 58 (defining “applicant” as “a prospective employee applying for employment” in Nebraska).
53 See COLO. REV. STAT. at § 8-2-127; WASH. REV. CODE ANN. at § 49.44.0003.
54 See N.M. STAT. ANN. at § 50-4-34 (stating that only “prospective employees” are protected under New Mexico law).
55 See ARK. CODE. ANN. at § 11-2-124; Neb. L.B. 58; COLO. REV. STAT. at § 8-2-127; WASH. REV. CODE ANN. at § 49.44.0003. But see N.M. STAT. ANN. at § 50-4-34 (providing protection only for prospective employees).
56 See ARK. CODE ANN. at § 11-2-124; CAL. LAB. CODE at § 980; COLO. REV. STAT. at § 8-2-127; ILL. COMP. STAT. ANN. 55/10; MD. CODE ANN. at § 3-712; N.M.
“Request or Require”

The laws in eleven of the thirteen states provide that an employer may not “request or require” the specified information from the employee or applicant, while Michigan and Utah use only the term “request.” In addition to “request or require,” the language in Arkansas and Colorado includes “suggest” and “cause [to disclose].” Nevada goes a step further, making it unlawful for an employer to “[d]irectly or indirectly, require, request, suggest or cause [to disclose].” Washington provides that an employer may not “request, require, or otherwise coerce” disclosure. In Illinois and New Mexico, there is a separate restriction that makes it unlawful for an employer to “demand access” to ones account or profile.

---

57 See ARK. CODE ANN. at § 11-2-124(b)(1); CAL. LAB. CODE at § 980(b); COLO. REV. STAT. at § 8-2-127(2)(a); ILL. COMP. STAT. ANN. 55/10 at § 10(b)(1); MD. CODE ANN. at § 3-712(b)(1); N.M. STAT. ANN. at § 50-4-34(A); WASH. REV. CODE ANN. at § 49.12.003; Nev. A.B. 181; Oh. S.B. 45; 2013 Vt. Legis. Serv. 47 (providing examples of language used in different state statutes).

58 See Mich. Pub. Acts 478 at § 3(a) (stipulating that an employer is prohibited from requesting information relevant to personal internet accounts); UTAH CODE ANN. at § 34-48-201(1) (mirroring Michigan’s prohibition).

59 See ARK. CODE ANN. at § 11-2-124(b)(1) (outlining prohibited employer conduct); COLO. REV. STAT. at § 8-2-127(2)(a) (reflecting language of prohibited employer conduct relative to personal internet accounts, similar to Utah).

60 See NEV. REV. STAT. 613-135 (1)(a) (2013); Nev. A.B. 181 at § 2(1)(a) (restricting an employer’s ability to obtain information about an employee’s social media account).

61 WASH. REV. CODE ANN. at § 49.44.003(1)(a) (broadening the prohibited conduct to include coercion).

62 See ILL. COMP. STAT. ANN. 55/10 at § 10(b)(1) (specifying that employer demands for personal account information are prohibited); N.M. STAT. ANN. at §
Although the prohibited action is simply to “ask” in South Carolina and to “ask or require” in Ohio, most of the bills in other states use similar language. In Minnesota, the prohibited action is to “require as a condition precedent to employment.” There is little significance in these variations.

“Disclose”

The laws in ten of the thirteen states prohibit a request to “disclose” username or password information, while Illinois and

50-4-34(A) (requiring employers not demand access from employees to enter personal accounts).


64 Ohio S.B. 45. Ohio is the only state that has language requiring that all of the proscribed acts be done “recklessly.” See id. at § 4112.02(K)(1). The Supreme Court of Ohio held that reckless conduct is characterized by the conscious disregard of or indifference to a known or obvious risk of harm to another which is unreasonable under the circumstances and substantially greater than negligent conduct. See Anderson v. City of Massillon, 951 N.E.2d 1063, 1068 (Ohio Ct. App. 2011) (defining the meaning of the term reckless).

It also stated, given the cross-application of these terms in our case law, it is not surprising that Ohio appellate courts have reached the conclusion that the “wanton or reckless misconduct” and “willful or wanton misconduct…are functionally equivalent.” See id. In its criminal code section entitled “Culpable mental states,” Ohio provides that a “person acts recklessly when, with heedless indifference to the consequence, he perversely disregards a known risk that his conduct is likely to cause a certain result or is likely to be of a certain nature. A person is reckless with respect to circumstances when, with heedless indifference to the consequences, he perversely disregards a known risk that such circumstances are likely to exist.” OHIO REV. CODE ANN. at § 2901.22(C). While it is unlikely that Ohio would apply the criminal standard, even the civil standard would seem to greatly diminish the effectiveness of the proposed legislation. See Anderson, 951 N.E. 2d. at 1069 (contrasting the criminal and civil standards and the impact it would have on legislation). If the civil standard, as enunciated by the Ohio Supreme Court is to be applied, the word “recklessly” would have to be removed from the bill in order for the legislation to be of any practical use. See id. at 1070 (holding no statutory immunity applied based on the totality of the circumstances in assessing the defendant’s reckless conduct).

65 See discussion infra p. 12-13 (describing the language of similar state statutes pertaining to password disclosure to employers).

66 Minn. H.F. 293; Minn. H. F. 611; Minn. S.F. 484; Minn S.F. 596 at § 181.53(b).

67 See ARK. CODE ANN. at § 11-2-124 (using the term “disclose”); CAL. LAB. CODE at § 980 (stating prohibited employer actions) COLO. REV. STAT. at § 8-2-127
New Mexico prohibit a request to “provide” the information and New Jersey prohibits a request to “provide or disclose” the information. Most states choose one word or the other, although the bill in Nebraska borrows New Jersey’s approach. Again, there is not much significance in these variations.

“Username and Password”

Maryland prohibits a request for the disclosure of “any user name, password, or other means for accessing a personal account or service,” while California prohibits a request for the disclosure of “a username or password for the purpose of accessing personal social media.” Illinois prohibits a request 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.” Michigan provides the definition of a term called “Access Information” to mean “user name, password, login in-
formation, or other security information that protects access to a personal internet account.\textsuperscript{74}

Some of the other states that have already enacted laws have followed these approaches,\textsuperscript{75} while others have tried new variations. New Mexico restricts only a “password,”\textsuperscript{76} while other states have multiple combinations using that word: Oregon prohibits the disclosure of a “username and password, password or other means of authentication that provides access,”\textsuperscript{77} Utah restricts the disclosure of “a username and password, or a password that allows access,”\textsuperscript{78} and Washington defines the term “login information” as “a username and password, a password, or other means of authentication that protects access.”\textsuperscript{79}

While for the most part these variations seem inconsequential, one can envision two situations that might become problematic. First, if a state restricts disclosure of a “username and password” and only a password is disclosed, an argument could be made that the requirements of the statute would not be satisfied.\textsuperscript{80} Secondly, if an account is accessible by means other than disclosure of a password specifically, the broader language employed by some states would be

\textsuperscript{75} See Ark. Code Ann. at § 11-2-124(b)(1)(A) (stating employer shall not request user name or password from prospective employee or change privacy settings on prospective employee’s social media account); see also Colo. Rev. Stat. at § 8-2-127(2)(a) (delineating prohibitions on employer access to employee personal accounts through user name and password); Vt. Stat. Ann. at § 495jj(b)(1) (deeming unlawful practice of employer requesting employee user name or password); Nev. Rev. Stat. at § 613-135(1)(a) (prohibiting an employer from requiring, requesting, suggesting, or causing an employee or prospective employee to disclose his or her personal social media account’s user name or password).
\textsuperscript{76} See N.M. Stat. Ann. at § 50-4-34(1)(A) (announcing that it is unlawful for an employer to request or require a prospective employee to provide a password to gain access to their account or profile on a social networking web site).
\textsuperscript{78} See Utah Code Ann. at § 34-48-201(1) (declaring that an employer may not request disclosure of information related to personal Internet account).
\textsuperscript{80} N.M. Stat. Ann. at § 50-4-34(1)(A) (specifying only that it is unlawful for an employer to request or require a prospective employee to provide a password to gain access to their account or profile on a social networking web site, but not specifying the same for usernames).
easier to apply. Generally speaking, however, the variations in the language are not particularly significant.

“*To Gain Access to*”

There are many variations of connective language used to tie together the prohibited requests for information from the prohibited accounts. California, Colorado, Maryland and Vermont use the word “accessing,” Illinois, New Mexico and Vermont use “to gain access to,” Nevada and Oregon use “provides access to,” Utah

---

81 See N.M. STAT. ANN. at § 50-4-34(1)(C) (providing example of statute in which means of access other than by password are not specifically addressed).

82 See ARK. CODE ANN. at § 11-2-124 (describing the social media accounts of current and prospective employees); CAL. LAB. CODE at § 980 (stating prohibited employer actions) COLO. REV. STAT. at § 8-2-127 (prohibiting of employers requiring access to personal electronic communication devices); MD. CODE ANN. at § 3-712 (describing the username and password protection and exclusions); Mich. Pub. Acts 478 at § 3(a) (stating the restrictions of an employer); NEV. REV. STAT. at § 613-135(1)(a) (stating it is unlawful for any employer to directly or indirectly require any employee, or prospective employee, to disclose information regarding their social media account); Or. H.B. 2654 (enacted) (stating it is an unlawful employment practice for employers to request an employee to disclose social media passwords); UTAH CODE ANN. at § 34-48-201 (describing that an employer may not request disclosure of information related to a personal internet account); Vt. S.B. 7 (enacted) (describing a social network privacy protection study committee); WASH. REV. CODE ANN. at § 49.44.0003 (describing employers access to social networking accounts and profiles of employees). See also ILL. COMP. STAT. ANN. 55/10 at § 10(b)(1) (prohibiting employers from requiring or request any employee to provide social network passwords); N.M. STAT. ANN. at § 50-4-34(1)(A) (stating it is prohibited for an employer to request access to social networking accounts of employees).

83 See supra notes 88-92 (explaining the various terms applied to the process of gaining prohibited access).

84 See CAL. LAB. CODE at § 980(b)(1) (prohibiting employers from demanding that employees “disclose a username or password for the purpose of accessing personal social media.”) (emphasis added); COLO. REV. STAT. at § 8-2-127(2)(a) (prohibiting an employer from requesting an employee to disclose any username and password for “accessing” the employee’s personal account); MD. CODE ANN. at § 3-712(b)(1) (prohibiting an employer from requesting or requiring an employee or applicant to disclose a user name, password, or other means for “accessing” a personal account); VT. STAT. ANN. at § 495j(b)(1) (prohibiting an employer from requesting or requiring an employee or applicant to disclose a user name, password, or other means of “accessing” a personal account).

85 See supra notes 88-92 (explaining the various terms applied to the process of gaining prohibited access).
uses “allows access to”87 and Michigan uses both “grant access to” and “allows access to.”88 While these variations are insignificant, a few states have added some more important restrictions.89

In addition to California prohibiting an employer from requiring or requesting an employee or applicant to “[d]isclose a username or password for the purpose of accessing personal social media,”90 it also prohibits the requirement or request to “[a]ccess personal social media in the presence of the employer”91 or to “[d]ivulge any personal social media” except as specifically required for purposes of investigating alleged employee misconduct.92 Oregon and Washington adopted similar approaches.93 Michigan prohibits an employer from requesting information that would “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.”94 Under the Illinois law, the employer cannot “demand access in any manner to an

86 See Nev. A.B. 181 (explaining an employer’s available access to personal accounts in Nevada); see also Or. H.B. 2654 (asserting employers legal access to employees personal accounts).
87 See UTAH CODE ANN. at § 34-48-201(1) (describing an employer’s ability to access personal accounts in Utah).
88 See MICH. COMP. LAWS ANN. at § 37.273 (limiting an employer’s means of access to employee personal accounts).
89 See Stephen Joyce, FINRA, Regulators Push Back on Bills Limiting Employer Social Media Access, 18 ELEC. COM. & L. REP. 917, 917 (2013) (summarizing states that are proposing legislation regarding restriction of employer access to employee’s personal information).
90 CAL. LAB. CODE at § 980(b)(1) (indicating restrictions placed on employer’s access to employee personal accounts in California).
91 Id. at § 980(b)(2) (prohibiting employers from requiring employees to access personal accounts in their presence).
92 Id. at § 980(b)(3) (limiting purpose for which an employee can be made to divulge social media information).
93 See Or. H.B. 2654 (discussing unlawful employment practices requiring employees to disclose username and passwords to social media accounts); see also WASH. REV. CODE ANN. at § 49.44.0003 (1)(a) (restricting employer access to employee social networking accounts).
employee’s or prospective employee’s account or profile on a social networking website.”

A second wave of states also introduced some further restrictions, like Arkansas, which protects a current or prospective employee from having to “[a]dd an employee, supervisor, or administrator to the list of contacts associated with his or her social media account.” Colorado, Oregon and Washington also have this restriction. Arkansas also protects a current or prospective employee from having to “[c]hange the privacy settings associated with his or her social media account.” Colorado uses almost identical language, while Washington prevents an employee or applicant from having 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.” Arkansas, Oregon and Washington also have provisions stating that if an employer “inadvertently receives” password or login information they will not be liable for having the information, but they cannot use it to access the employee’s social media account. In what may be the broadest language adopted, Vermont prohibits an employer from requesting or requiring the employee or applicant to “take an action that permits the employer to gain access to the employee’s or applicant’s account or profile on a social networking service if that information is not available to the general public.”

95 820 ILL. COMP. STAT. ANN. 5/10. See also N.M. STAT. ANN. at § 50-4-34 (following a similar approach).
96 ARK. CODE ANN. at § 11-2-124.
97 See COLO. REV. STAT. at § 8-2-127 (protecting current and prospective employees from being required to connect with employers through social media accounts); see also Or. H.B. 2654 (following the same approach); WASH. REV. CODE ANN. at § 49.44.0003 (containing the same restriction).
98 ARK. CODE ANN. at § 11-2-124.
99 See COLO. REV. STAT. at § 8-2-127 (prohibiting employers from requiring employees to change privacy settings associated with social media accounts).
100 WASH. REV. CODE ANN. at § 49.44.0003(1)(d).
101 See ARK. CODE ANN. at § 11-2-124; Or. H.B. 2654 at § 2(6); WASH. REV. CODE ANN. at § 49.44.0003(4) (indicating Arkansas, Oregon and Washington will not hold employers liable if they inadvertently receive employee login information, as long as employers do not use this information to access an employee’s social media account).
102 Vt. S.B. 7.
Delaware would prohibit an employer from “accessing an employee’s or applicant’s social networking site profile or account indirectly through any other person who is a social networking contact of the employee or applicant.”\(^{103}\) Nebraska borrows this language in its bill.\(^{104}\)

Obviously significant are the restrictions that prohibit the accessing of accounts in the presence of employers, the addition of names to a contact list, the changing of privacy settings, and the indirect access through a third party. Also significant is the broad language adopted by Michigan and New Mexico as to the prohibitions against demanding access in any manner.\(^{105}\) But probably the strongest language is that adopted by Vermont in prohibiting an employer to take any action that gives it access to information that is not available to the general public.\(^{106}\)

**What is Protected?**

“Electronic Communications Device”

A number of states take different approaches to protect their citizens from disclosure; for example, Maryland prohibits the request for the disclosure “for accessing a personal account or service through an electronic communications device.”\(^{107}\) An “[e]lectronic communications device” is any “device that uses electronic signals to create, transmit, and receive information.”\(^{108}\) It specifically “includes computers, telephones, personal digital assistants, and other similar devices.”\(^{109}\) The laws in Colorado,\(^{110}\) New Jersey,\(^{111}\) Vermont\(^{112}\) and

---

\(^{103}\) Del. H.B. 308 at § 710(c)(3).

\(^{104}\) See Neb. L.B. 58 (prohibiting an employer from indirectly accessing an employee’s social networking site profile account through a third party).


\(^{106}\) See Vt. S.B. 7 (forbidding an employer from taking “any action” that yields employee social media information that is not available to the general public).

\(^{107}\) Md. Code Ann. at § 3-712(b)(1).

\(^{108}\) Id. at § 3-712(a)(3)(I).

\(^{109}\) Id. at § 3-712(a)(3)(II).


\(^{112}\) See Vt. S.B. 7.
Washington,113 and bills in Georgia,114 Iowa,115 Missouri,116 New York,117 Texas,118 and West Virginia119 borrow this definition almost verbatim, while Delaware,120 Nebraska,121 North Carolina122 and North Dakota123 use similar language: “'[e]lectronic communication device’ means a cell telephone, personal digital assistant, electronic device with mobile data access, laptop computer, pager, broadband personal communication device, 2-way messaging device, electronic game, or portable computing device.”

"Social Networking Website"

Illinois prohibits the request for the disclosure to gain access to or to demand access to an “account or profile on a social networking website.”124

[A] “social 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.125

113 See WASH. REV. CODE ANN. at § 49.44.0003(5)(c).
114 See Ga. H.B. 149.
115 See Iowa H.F. 172 § 1(1).
116 See Mo H.B. 115 at § 285.600(2); Mo. H.B. 706 at § 285.045(2); Mo. S.B. 164 § 285.045(2).
117 See N.Y. S.B. 2434 at § 1(B).
120 See Del. H.B. 308 at § 710(b)(2).
121 See Neb. L.B. 58 at § 2(2).
123 See N.D. H.B. 1455 at § 1(2).
124 ILL. COMP. STAT. ANN. 55/10 at § 10(b)(1).
125 See id. at § 10(b)(4).
New Jersey and New Mexico adopted this language in their laws, but eliminated the exclusion of e-mail. Bills in Kansas, Minnesota, Mississippi, Missouri, and South Carolina use Illinois’s definition, complete with exclusion of e-mail. Ohio uses the same definition for “social media internet web site” (without the electronic mail exclusion), but incorporates it into a broader definition: a “‘[p]rivate electronic account’ means a collection of electronically stored private information regarding an individual, including such collections stored on social media internet web sites, in electronic mail, and on electronic devices.”

Two issues arise here: first, Illinois (and all of the states that use its definition, complete with exclusion of e-mail) does not include a specific provision protecting e-mail accounts. It does, however, acknowledge the presence of e-mail by reserving to employers the right to monitor it. New Jersey, while not specifically referring to e-mail, enacted very broad language that prohibits requiring the disclosure of a password to provide access to “a personal account or service through an electronic communications device,” which is broad enough to include e-mail systems.

The second issue involves Ohio’s use of the word “private” in the language that contains the Illinois definition

126 See N.J. STAT. ANN. § 34:6B-5 (West 2013); N.M. STAT. ANN. at § 50-4-34(E) (refusing to distinguish between access to social media profiles and email accounts).
127 See Kan. H.B. 2092 at § 1(d)(4); Kan. S.B. 53 § 1(d)(4) (defining social networking website pursuant to employees’ privacy rights).
128 See Minn. H.F. 293 at § 181.53(b); Minn. H.F. 611 at § 181.53(b); Minn. S.F. 484 at § 181.53(b); Minn. S.F. 596 at § 181.53(b).
129 See Miss. H.B. 165 at § 1(4).
130 See Mo. H.B. 286 at § 285.605(2)(1); Mo. H.B. 1020 at § 285.603(2).
131 See S.C. H.B. 5105 at § 41-1-187(B).
132 Ohio S.B. 45 at § 4112.02(K)(3)(b).
133 See ILL. COMP. STAT. ANN. 55/10 (allowing employers to monitor employee electronic mail accounts without requesting access).
134 See id. at § 10(2)(B).
135 See N.J. STAT. ANN. § 34:6B-6 (West 2013). (prohibiting employer to require a current or prospective employee to disclose any user name or password or provide the employer access to “a personal account,” seemingly indicating legislative intent to include email).
of “social networking site.” 136 One of elements of the Illinois
definition is a service that permits users to “construct a public
or semi-public profile.” 137 Presumably, this would include
services like Facebook, which permit users to limit, to some
extent at least, just how public their profiles will be. 138 Within
its definition of a “social networking site,” Ohio has de-
efined a “private electronic account” as “a collection of
electronically stored private information regarding an individual,
including such collections stored on social media internet sites
[and] in electronic mail.” 139 A question that arises is: what if
a service is entirely private? Would the Illinois statute apply?
It would seem that the Ohio language better reflects the notion
that there is private information involved, albeit in a public or
semi-public environment. 140 Delaware uses the Illinois law as
a model, but proposes some changes that seem to be directed
at this concern:

“Social networking site” means an internet-based, personal-
ized, privacy-protected website or application whether free or commercial that allows users to con-
struct 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. 141

136 See Ohio S.B. 45 (defining private electronic account as a “collection of
electronically stored private information regarding an individual, including such
collections stored on social media internet web sites, in electronic mail, and on
electronic devices”).
137 ILL. COMP. STAT. ANN. 55/10 (defining “social networking website” to include
Internet-based services that allow individuals to construct public profiles).
138 See Sharing and finding you on Facebook, Facebook.com (Dec. 11, 2012) ar-
chived at www.perma.cc/5J2S-BY7U (explaining privacy settings for personal Fa-
cebook accounts).
139 Ohio S.B. 45 at (K)(3)(a).
140 See id. (creating no requirement that an account be available to the public in any
sense).
141 Del. H.B. 308 (emphasis added). North Carolina borrows this definition. See
N.C. H.B. 846 (defining “social networking site” under North Carolina bill). Ne-
braska also borrows this definition, but includes an Illinois-like exclusion of elec-
tronic mail. See Neb. L.B. 58 (defining “social networking site” not to include
email). Similarly, North Dakota borrows the definition, but goes even further with
an exclusion: “[t]he term does not include electronic mail or any account created,
There are some good things addressed in this definition: first, it introduces the notion of a “personalized, privacy-protected website.” These are probably two of the most important attributes of the type of system or site intended to be protected by this legislation. Second, it specifically mentions “application,” which, given the direction of computing, seems like a good addition. Third, it specifically includes both free and commercial products. While it is probably unnecessary to make this distinction - certainly if “commercial” is interpreted to mean non-free - it does not burden the definition (other than making it slightly longer). Finally, it describes the profile site as “private or semi-private,” rather than as “public or semi-public.” While this may present semantic issues similar to those involved in choosing whether to refer to “spam” or “anti-spam” laws, or to “dilution” or “anti-dilution” laws, it would seem to better reflect the intent of this type of legislation, that is, to protect private or semi-private information.

The Delaware definition also has some potential problems. First, because the requirements of the definition are anded together, one could argue that a site would not be a “social networking site” unless it had all of the specified attribute requirements, or attributes. For example, if the site did not permit users to send and receive email, it would not qualify as a “social networking site.” Furthermore, some of the individual requirements may similarly prove problematic because they are anded together as well. For example, if the system does not permit a user to create a list of other users maintained, used, or accessed by an employee or applicant for business-related communications or for a business purpose of the employer.” See N.D. H.B. 1455. See Del. H.B. 308 at (b)(4).

See id. (providing clear indication of legislative intent).

See id. (incorporating both terms).

See id. (stating the individual requirements that must be “anded” together).
who are granted reciprocal access, or if the system does not permit
users to grant reciprocal access, or if the system permits the sharing
of only two of “personal content, communications, and contacts,” it
may similarly fail to satisfy the definitional requirements.

“Social Media”

California law takes a different approach. It prohibits an em-
ployer from requiring or requesting an employee or applicant to 1)
“[d]isclose a username or password for the purpose of accessing per-
sonal social media,”150 2) “[a]ccess personal social media in the pres-
ence of the employer,”151 or 3) “[d]ivulge any personal social media,
except as provided by way of specific exceptions.”152 “Social media”
is very broadly defined as “an electronic service or account, or elec-
tronic 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.”153
This is probably the broadest of all the definitions and would, argua-
ibly, include every type of electronic data, service or site now in use.

Bills in Georgia use California’s definition exactly,154 while a
bill in Montana changes the term to “personal social media” and in-
serts the phrase “password-protected” at the beginning of California’s
definition.155 The Nevada law defines “social media account,” using
most of California’s language, but excludes “locations” from the def-
definition.156 A bill in Pennsylvania defines “social media” as including
“social networking Internet websites and any other forms of media

150 CAL. LAB. CODE § 980 at § 980(b)(1).
151 Id. at § 980(b)(2).
152 Id. at § 980(b)(2).
153 Id. at § 980(a).
154 See Ga. H.B. 117 (borrowing California’s language); Ga. H.B. 149 (utilizing
California’s definition of social media).
155 See Mont S.B. 195 at § 1(5) (defining “personal social media” as “a password-
protected electronic service or account or electronic content, including but not
limited to videos, still photographs, blogs, video blogs, podcasts, instant and text
messages, e-mail, online services or accounts, or internet website profiles or
locations”).
156 See NEV. REV. STAT. at § 613-135(4) (defining “social media account” as “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”).
that involve any means of creating, sharing and viewing user-generated information through an account, service or Internet website.”

The law in Oregon defines “social media” as “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.” Bills in Massachusetts use an almost identical definition, while bills in New Hampshire use a very similar definition, but exclude the word “share” and, more significantly, “electronic email or Internet websites or locations.”

The Arkansas law defines “social media account” as a “personal account with an electronic medium or service where users may create, share or view user-generated content, including without limitation” a list of items very similar to California’s and Oregon’s: videos, photographs, blogs, podcasts, messages, e-mails, or website profiles or locations. The Arkansas definition specifically excludes an account:

(i) Opened by an employee at the request of an employer;
(ii) Provided to an employee by an employer such as a company email account or other software program owned or operated exclusively by an employer;
(iii) Setup by an employee on behalf of an employer; or

---

159 See Mass. H.B. 1707 (defining “social media” as “an electronic medium [which allows] users to create, share, and view user-generated content, including, but not limited to, uploading or downloading videos or still photographs, blogs, video blogs, podcasts, messages, e-mails, or Internet Web site profiles or locations”); see also Mass. S.B. 852 at § 1 (offering same definition for “social media”).
160 See N.H. H.B. 379 (defining “social media” as “an electronic medium where users may create and view user-generated content, including uploading or downloading videos or still photographs, blogs, video blogs, podcasts, or instant messages).
161 ARK. CODE ANN. at § 11-2-124(a)(3)(A) (defining social media as including electronic mediums and services).
(iv) Setup by an employee to impersonate an employer through the use of the employer’s name, logos, or trademarks.\textsuperscript{162}

The Arkansas definition specifically includes accounts “established with Facebook, Twitter, LinkedIn, MySpace, or Instagram.”\textsuperscript{163} Bills in Maine and Rhode Island similarly define “social media account” like Arkansas, but without the prefatory “personal” in the definition and using California’s list of items exactly.\textsuperscript{164} The bills specifically exclude an account “opened at an employer’s behest, or provided by an employer, and intended to be used primarily on behalf of the employer.”\textsuperscript{165}

“Personal Internet Account”

Michigan uses an approach similar to California’s but with entirely different language.\textsuperscript{166} It prohibits a request of an employee or applicant that would “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.”\textsuperscript{167} “Personal internet account” is defined as “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.”\textsuperscript{168} This definition is fine for now because most of the requirements are joined in the alternative.\textsuperscript{169} However, the phrase “bounded system established by an internet based service” may someday become outdated as technology advances.

\textsuperscript{162} Id. at § 11-2-124(a)(3)(B) (allowing for employer access to accounts created in or for the course of employment).

\textsuperscript{163} Id. at § 11-2-124(a)(3)(C) (detailing the specific social media company networks).

\textsuperscript{164} See Me. H.P. 838 at § 876(5) (clarifying distinction between state regulations); see also R.I. H.B. 5255, at § 16-100-1(1) (outlining various components of social media definition); see also R.I. S.B. 493 at § 28-55-2 (identifying prohibitive access to social media passwords).

\textsuperscript{165} See Me. H.P. 838 at § 876(4).


\textsuperscript{168} Id.

\textsuperscript{169} \textit{See id.} (taking disjunctive approach).
One of the recent trends in this legislation has been a focus on the personal nature of the account. In fact, Illinois has already amended its law, distinguishing between a “professional account” and a “personal account.” A “professional account” is defined as “an account, service, or profile created, maintained, used, or accessed by a current or prospective employee for business purposes of the employer,” whereas a “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.” New Jersey has similar language for its definition of “personal account.”

Similarly, under Utah law, a “personal Internet account” is “an online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer.” It 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.”

States have proposed a variety of terms: “personal Internet account” in Michigan, Utah and Wisconsin; “personal on-line account” in Connecticut; “personal social media” in Louisiana; and others.

---

170 See, e.g., Me. H.P. 838 at § 876(5) (tailoring the law to recognize personal internet accounts as distinct from work accounts); see also R.I. H.B. 5255 at §16-100-1(1) (defining social media for purposes of the statute); see also R.I. S.B. 493 at § 28-55-2 (identifying prohibitive access to social media passwords).
171 See ILL. COMP. STAT. ANN. 55/10 (West 2013) (providing that employer access to professional accounts is not prohibited).
172 See id. (distinguishing between personal and professional accounts as defined by the bills).
174 UTAH CODE ANN. at § 34-48-102(4)(a) (emphasis added) (defining personal internet account).
175 See id. at § 34-48-102(4)(b).
“personal electronic account” in North Carolina;179 “personal account” in New Hampshire;180 “personal online service” in Missouri;181 and “personal account or service” in Kansas.182 Regardless of the term used, many of the bills follow Utah’s approach, requiring that a personal account be both used exclusively for personal purposes and unrelated to any business purpose of the employer.183

North Carolina proposes a definition of “personal electronic account” that is virtually identical to the definition that Oregon adopted for “social media,” but that specifically excludes any account opened on behalf of or owned by an employer.184 Wisconsin’s proposed definition of “personal Internet account” is exactly like Michigan’s except it replaces the first few words of Michigan’s definition—“an account created via a bounded system” with “an account created and used exclusively for personal purposes within a bounded system.”185

It is interesting to note that Washington, while adopting Maryland’s definition of “electronic communications device,” repeatedly refers to an employee’s “personal social networking account” without ever defining the term.186 Apparently, Washington is comfortable with accepting the “plain meaning” of that phrase.

While the approaches taken by the first four states to enact legislation are very different, the information protected is largely the

181 Mo. H.B. 706; see also Mo. S.B. 164.
183 See Conn. S.B. 159; Mo. H.B. 706; see also Mo. S.B. 164; N.J. A.B. 2878 (distinguishing between employees’ personal electronic accounts and accounts used for business related matters). The bill in New Hampshire requires that the account be used *primarily* for personal purposes. See N.H. H.B. 414. The bill in Louisiana requires that it be used *primarily or exclusively* for personal purposes. See La. H.B. 314. The bill in Kansas requires that the account be used for personal communications. See Kan. H.B. 2092; Kan. S.B. 53.
186 See WASH. REV. CODE ANN. at § 49.44.0003(1)(a); see also MD. CODE ANN. at § 3-712(a)(3)(i).
same. Because of the speed at which technology develops, broad language, like California’s, will probably work the best, or at least, last the longest without the need for revision. One major difference that does exist among the legislation is the presence or absence of protection for personal e-mail accounts.

Further Restrictions

Under Maryland law, an employer may not “discharge, discipline or otherwise penalize, or threaten to discharge, discipline, or otherwise penalize” an employee who refuses to disclose the requested user name or password information, nor may the employer “fail or refuse to hire any applicant” as a result of such refusal to disclose such information. California provides that an employer “shall not discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant” who does not comply with a prohibited request or demand. Michigan does not permit an employer to “[d]ischarge, discipline, fail to hire, or otherwise penalize an employee or applicant . . . for failure to grant access to, allow observation of, or disclose information that allows access to or observation of” the requested account. Illinois has no such restriction.

Most of the second wave of states adopting legislation took approaches similar to those of the first four states. Colorado basi-
Legislatively borrows Maryland’s language. Arkansas adds “take action against” to Maryland’s language and Oregon adds, “take, or threaten to take any action.” Utah and Washington adopted definitions for “adverse action,” which basically include the activities specified in the Maryland law. Likewise, Vermont adopted a definition for “retaliatory action,” which includes “discharge, threat, suspension, demotion, denial of promotion, discrimination, or other adverse employment action.” Nevada used language similar to that proposed in SNOPA, making it unlawful for an employer to “discharge, discipline, discriminate against in any manner, or deny employment or promotion to, or threaten to take any action against” an employee or applicant who refuses to disclose the requested information. New Mexico’s approach is the same as Illinois – no specific additional restrictions against the employer.

New Jersey prohibits retaliation or discrimination for a) refusing to provide or disclose password information or to provide access to a personal account, b) reporting an alleged violation, c) testifying, assisting or participating in any investigation, proceeding or action pertaining to its statute, or d) otherwise opposing a violation of its statute. New Jersey also prohibits employers from requiring an individual to waive or limit any protection under the act as a condition of applying for or receiving an offer of employment – any such agreement is void and unenforceable.

195 Compare COLO. REV. STAT. at § 8-2-127 (3)(a) with MD. CODE ANN. at § 3-712(c)(1) (restricting an employer’s ability to “discharge, discipline, or otherwise penalize… an employee”).
196 ARK. CODE ANN. at § 11-2-124; Or. H.B. 2654.
197 See UTAH CODE ANN. at § 34-48-102 (replacing “…discharge, discipline, or otherwise penalize…” with “adverse action”); see also WASH. REV. CODE ANN. at § 49.44.0003 (using “adverse action” terminology for prohibited employer actions).
199 Nev. A.B. 181 (indicating limitations on employers in regards to employees and personal social media information).
200 See N.M. STAT. ANN. at § 50-4-34; ILL. COMP. STAT. ANN. 55/10 (indicating no further restrictions).
201 See N.J. STAT. ANN. § 34:6B-8 (West 2013) (enumerating potential bases for retaliation claims).
202 See id. at § 3 (providing an employer cannot require prospective employees to waive protection from proposed act).
The North Carolina bill also contains a unique provision: It would prohibit employers from monitoring or tracking “an employee’s or applicant’s personal electronic communication device by installation of software upon the device or by remotely tracking the device by using intercept technology.”

What Employers May Do

There is also great variety in what the different laws specifically permit or would permit employers to do. Maryland provides that employers “may require an employee to disclose any user name, password, or other means for accessing non-personal accounts or services that provide access to the employer’s internal computer or information systems.” Vermont borrows this language exactly, while Nevada models it closely. California specifically provides that nothing in the law “precludes an employer from requiring or requesting an employee to disclose a username, password, or other method for the purpose of accessing an employer-issued electronic device.” Michigan goes even further, specifically permitting employers to request or require access to information that would allow the employer to gain access to or operate: “i) an electronic communications device 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 employee, or used for the employer’s business purposes.” Both Utah and Washington adopted language very similar to Michigan’s, and Oregon used

204 MD. CODE ANN. at § 3-712(b)(2).
205 See VT. S.B. 7 (highlighting employers right to require employee disclosure of non-personal account information).
206 See Nev. A.B. 181 (stating “it is not unlawful for an employer in this State to require an employee to disclose the user name, password or any other information to an account or a service, other than a personal social media account, for the purpose of accessing the employer’s own internal computer or information system”).
207 CAL. LAB. CODE § 980 at § 980(d).
209 See UTAH CODE ANN. at § 34-48-202(1) (stating “[t]his chapter does not prohibit an employer from…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
Michigan’s second prong, permitting access to an account “provided by, or on behalf of, the employer or to be used on behalf of the employer.”

The California law states that it will not “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 or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding.” Arkansas, Nevada, Oregon, and Washington have provisions stating that employers are not prevented from complying with state and federal laws or regulations or the rules of self-regulatory organizations.

Maryland specifically prohibits employees from downloading “unauthorized employer proprietary information or financial data to an employee’s personal web site, an Internet web site, a web-based account, or a similar account” and permits an employer, “based on the receipt of information about the unauthorized downloading” of such proprietary information or financial data to investigate the employee’s actions. The laws in Colorado and Washington would permit similar investigations upon “receipt of information” and in Michigan and Utah as long as there is “specific information.”
Maryland also permits 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” to conduct “an investigation for the purpose of compliance with applicable securities or financial law, or regulatory requirements.”\textsuperscript{216} Again, Colorado and Washington have similar provisions.\textsuperscript{217} The Delaware bill would also permit employers in the financial services industry to conduct internal investigations into employee wrongdoing and other compliance issues.\textsuperscript{218}

The Michigan law provides great detail about what an employer is not prohibited from doing.\textsuperscript{219} An employer can discipline or discharge 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.”\textsuperscript{220} It can also conduct an investigation or require an employee to cooperate in an investigation if i) “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,”\textsuperscript{221} or ii) “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.”\textsuperscript{222}

Additionally, Michigan provides that employers can restrict or prohibit “an employee’s access to certain websites while using an electronic communications device paid for in whole or in part by the

\textsuperscript{216} MD. CODE ANN. at § 3-712(e)(1).
\textsuperscript{217} See COLO. REV. STAT. at § 8-2-127(4)(a) (describing employer’s right to regulate employees’ online business related activities); see also WASH. REV. CODE ANN. at § 49.44.0003(2)(b)-(c) (authorizing employers to monitor employees’ online usage to ensure compliance with regulations).
\textsuperscript{218} See Del. H.B. 308 (providing specific language for employers in the financial industry).
\textsuperscript{219} See Mich. Pub. Acts 478 at § 5 (authorizing employer access to employees’ business related online accounts).
\textsuperscript{220} Id.
\textsuperscript{221} Id.
\textsuperscript{222} Id.
employer or while using an employer’s network" and can monitor, review or access “electronic data stored on an electronic communications device paid for in whole or in part by the employer, or travelling through or stored on an employer’s network, in accordance with state and federal law." These provisions were added to the bill in the Michigan Senate after the bill had been approved by the House without them. They would seem to preserve for employers whatever rights exist to control and monitor both employees and data to whatever extent is permitted by law. Utah borrowed this language from Michigan in its law.

Illinois law provides that the statute does not limit an employer’s right to “promulgate and maintain lawful workplace policies governing the use of the employer’s electronic equipment, including policies regarding Internet use, social networking site use, and electronic mail use” and that an employer may “monitor usage of the employer’s electronic equipment and the employer’s electronic mail” as long as it does not request or require password or related account information in order to gain access to accounts or profiles on a social networking site. New Mexico adopted both of these provisions. Colorado and Washington laws state that employers are not prohibited from “enforcing existing personnel policies that do not conflict with” the other provisions of this law.

---

223 Id.
224 Id.
228 ILL. COMP. STAT. ANN. 55/10 at § 10(b)(2)(A).
229 Id. at § 10(b)(2)(B).
230 See N.M. STAT. ANN. at § 50-4-34(B)(2) (detailing an employer’s right to monitor and regulate workplace internet activity).
231 See COLO. REV. STAT. at § 8-2-127(6); WASH. REV. CODE ANN. at § 49.44.0003(1)(3)(c).
have similar provisions regarding the public domain. Michigan, New Mexico and Utah have similar provisions regarding the public domain, while Oregon permits access to “information available to the public.”

Bills in Massachusetts, Mississippi, Nebraska, Pennsylvania, South Carolina, and Texas largely borrow the Illinois language regarding promulgating and maintaining workplace policies, and obtaining information from the public domain. North Carolina would define “publicly accessible communication” as information “that may be obtained without required access information or that is available in the public domain.” Texas would permit employers to maintain lawful workplace policies regarding employee access to personal accounts on employer-provided electronic communication devices and regarding employee usage of personal electronic communication devices during working hours. Ohio would let employers monitor the electronic accounts of employees and applicants on the employers’ electronic mail and Internet systems. Washington introduced a unique exception in its law, stating that it does not apply to “a social network intranet, or other technology platform that is intended primarily to facilitate work-related in-

232 ILL. COMP. STAT. ANN. 55/10 at § 10(b)(3).
233 See Mich. Pub. Acts 478; N.M. STAT. ANN. at § 50-4-34(C); UTAH CODE ANN. at § 34-48-202(4) (according employer’s access to information that is available in the public domain).
234 Or. H.B. 2654.
235 See Mass. H.B. 1707 (providing that employers have access to information about employees in the public domain).
236 See Miss. H.B. 165.
238 See Pa. H.B. 1130.
239 See S.C. H.B. 5105.
241 N.C. H.B. 846 (defining publicly accessible communication).
242 See Tex. H.B. 451 (permitting employers to have policies regarding employee access to personal accounts on employer owned devices).
243 See Tex. S.B. 416 (permitting employers to have policies regarding use of personal communication devices during working hours).
244 See Ohio S.B. 45 (allowing employer monitoring of employee electronic accounts and Internet systems).
formation exchange, collaboration, or communication by employees or other workers.”

**Enforcement**

The Maryland and California laws do not provide for any specific penalties; general enforcement is left to the Commissioner of Labor and Industry and the Labor Commissioner, respectively.\(^{246}\) The Illinois law has a separate section about administration and enforcement.\(^{247}\) The Director of Labor is authorized to administer and enforce the law.\(^{248}\) An employee or applicant who alleges a violation of the law can file a complaint with the Director of Labor or commence a civil action individually.\(^{249}\) For willful and knowing violations, a court may award $200 plus costs, reasonable attorney’s fees, and actual damages.\(^{250}\) Violators can also be found guilty of a petty offense.\(^{251}\) Michigan provides that violators of the law are “guilty of a misdemeanor punishable by a fine of not more than $1,000.”\(^{252}\) In addition, individuals can bring a civil action, seeking injunctive relief and damages of not more than $1,000 plus reasonable attorney fees and court costs.\(^{253}\) In Michigan, there is an affirmative defense in any action brought under this law for the employer to show that it acted in order to comply with the requirements of a federal or state law.\(^{254}\)

\(^{245}\) WASH. REV. CODE ANN. at § 49.44.250(1)(a).

\(^{246}\) See MD. CODE ANN. at § 3-712(f) (describing commissioner’s steps after section violation); see also CAL. LAB. CODE § 980 (noting lack of action required by Labor Commission upon violation of act). Interestingly, the California law specifically states that the Labor Commissioner “is not required to investigate or determine any violation of this act.” Id.

\(^{247}\) See 820 ILL. COMP. STAT. ANN. 55/15 (West 2013) (stating Director of Labor’s requirement to administer and enforce provisions of act).

\(^{248}\) See id. at § 15(a) (stating Director of Labor may issue rules and regulations necessary to administer and enforce the Act).

\(^{249}\) See id. at § 15(b)-(c) (explaining actions employee or applicant can take upon violation of Act).

\(^{250}\) See id. at § 15(d)(2) (describing penalties for violation of Act).

\(^{251}\) See id. at § 15(e) (providing that an employer, prospective employer, or agent of either, who violates the Act is guilty of a petty offense).


\(^{253}\) See id. § 8(2) (prescribing means of seeking damages and injunctive relief for subjects of violations under the Act).

\(^{254}\) See id. § 8(3) (describing affirmative defense for violation).
Colorado provides that an injured person may file a complaint with the Department of Labor and that penalties may include a fine of up to $1000 for a first offense and up to $5,000 for each subsequent offense.\textsuperscript{255} New Jersey provides for a civil penalty not to exceed $1,000 for the first violation and $2,500 for each subsequent violation.\textsuperscript{256} Utah permits a civil suit to be brought against the employer with a potential award of not more than $500.\textsuperscript{257} Washington law also authorizes a civil suit, which can seek “injunctive or other equitable relief, actual damages, a penalty in the amount of five hundred dollars, and reasonable attorneys’ fees and costs.”\textsuperscript{258} The law also authorizes an award for the prevailing defendant of “reasonable expenses and attorneys’ fees upon final judgment and written findings by the trial judge that the action was frivolous and advanced without reasonable cause.”\textsuperscript{259}

Some of the proposed bills include specific provisions for private civil actions; a civil action would be able to be brought by employees or prospective employees under bills proposed in Georgia,\textsuperscript{260} Iowa,\textsuperscript{261} Maine,\textsuperscript{262} Mississippi,\textsuperscript{263} Nebraska,\textsuperscript{264} North Carolina,\textsuperscript{265} North Dakota,\textsuperscript{266} Ohio,\textsuperscript{267} Rhode Island,\textsuperscript{268} and Wisconsin.\textsuperscript{269}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{255} See COLO. REV. STAT. at § 8-2-127(5) (describing scope of penalties for violation of Act).
\item \textsuperscript{256} See N.J. STAT. ANN. § 34:6B-9 (West 2013).
\item \textsuperscript{257} See UTAH CODE ANN. at § 34-48-301 (stating $500 damages limitation for civil action brought under Act).
\item \textsuperscript{258} Wash. S.B. 5211 at § (2)(1).
\item \textsuperscript{259} Id. at § (2)(2).
\item \textsuperscript{260} See Ga. H.B. 149 (indicating an employee’s right to seek a private civil action against an employer).
\item \textsuperscript{261} See Iowa H.F. 127 (indicating an employee’s right to seek a private civil action against an employer).
\item \textsuperscript{262} See Me. H.P. 838 (indicating an employee’s right to seek a private civil action against an employer).
\item \textsuperscript{263} See Miss. H.B. 165 (indicating an employee’s right to seek a private civil action against an employer).
\item \textsuperscript{264} See Neb. L.B. 58 (indicating an employee’s right to seek a private civil action against an employer).
\item \textsuperscript{265} See N.C. H.B. 846 (indicating the action may be brought by the attorney general to seek a private civil action against an employer).
\item \textsuperscript{266} See N.D. H.B. 1455 (indicating an employee’s right to seek a private civil action against an employer).
\end{itemize}
\end{footnotesize}
Claims could be brought for actual damages, attorney’s fees and costs in Georgia, Maine, Nebraska, North Dakota, and Rhode Island. Maine would provide for damages in the amount of three times lost wages plus reinstatement with full benefits of an employee’s position; Ohio would allow for “damages, injunctive relief, or any other appropriate relief;” and Rhode Island would permit both injunctive relief and punitive damages.

Some of the proposed bills include specific provisions for penalties. Violators of the laws would be subject to a civil penalty of up to $10,000 plus equitable relief in Connecticut, a civil penalty of not less than $200 nor more than $400 in one bill in Georgia and of $1,000 in another bill in Georgia, a civil penalty of not more than $1,000 in Iowa, a civil penalty not to exceed $1,000 and

---

267 See Ohio S.B. 45 (indicating an employee’s right to seek a private civil action against an employer).
268 See R.I. H.B. 5255; R.I. S.B. 493 (indicating an employee’s right to seek a private civil action against an employer).
269 See Wis. A.B. 218; Wis. S.B. 223 (indicating an employee may file a complaint with the department of workplace development).
270 See Ga. H.B. 149 (indicating a court may award reasonable attorney’s fees and costs, in addition to an award of actual damages).
271 See Me. H.P. 838 (indicating a court may award reasonable attorney’s fees and costs, in addition to an award of actual damages).
272 See Neb. L.B. 58 (indicating a court may award reasonable attorney’s fees and costs, in addition to an award of actual damages).
273 See N.D. H.B. 1455 (indicating a court may award reasonable attorney’s fees and costs, in addition to an award of actual damages).
274 See R.I. H.B. 5255; R.I. S.B. 493 (indicating a court may award reasonable attorney’s fees and costs, in addition to an award of actual damages).
275 See Me. H.P. 838 (indicating specific damages employee is entitled to).
276 See Ohio S.B. 45 (indicating specific damages employee is entitled to).
277 See R.I. H.B. 5255; R.I. S.B. 493 (indicating specific damages employee is entitled to).
278 See Conn. S.B. 159 at § 1(4) (authorizing the superior court to assess a penalty not to exceed $10,000 as well as to order other equitable relief as it deems appropriate).
279 See Ga. H.B. 117 (specifying the range of civil penalties to be assessed against any employer, employer’s agent, representative, or designee in violation of any of the subject code section’s provisions).
280 See Ga. H.B. 149 (specifying that violators be assessed a civil penalty of $1,000 per violation).
281 See Iowa H.F. 127 (requiring any penalty recovered to be deposited in the general fund of the state).
of $2,000 for a subsequent offense in Maine, a civil fine of up to $5,000 in Mississippi, a civil penalty to be imposed by the labor commissioner in New Hampshire, a civil penalty in New Jersey of up to $1,000 for the first violation and $2,500 for each subsequent violation, a civil penalty of $300 for the first violation and $500 for each subsequent violation in New York, a civil penalty of up to $1,000 for the first violation and up to $2,000 for each subsequent violation in Ohio, a civil penalty of up to $5,000 in Pennsylvania, a forfeiture of not more than $1289 and under SNOPA a civil penalty of up to $10,000, along with appropriate injunctive or equitable relief.

A Different Approach

The Password Protection Act of 2012 (the “PPA”) was introduced in the Senate by Senator Richard Blumenthal and in the House by Representative Martin Heinrich. The PPA takes a different approach than the legislation discussed above; rather than focusing on the acts of employers, it focuses on where the information is

282 See Me. H.P. 838 (imposing additional liability on employers who “harass” employees or applicants by requiring or repeatedly attempting to require the employees or applicants to disclose the information).
283 See Miss. H.B. 165 (specifying violators be subject to up to $5,000 civil fine).
284 See N.H. H.B. 414 (requiring civil penalty be imposed on violators, in accordance with state labor commissioner’s procedures).
285 See N.J. A.B. 2878 (providing that the applicable penalties be collectible by the Commissioner of Labor and Workforce Development).
287 See Ohio S.B. 45 (imposing a fine of up to $1,000 for a first violation, and up to $2,000 for any subsequent violation, in addition to other damages that may be available).
288 Pa. H.B. 1130 (imposing civil penalty of up to $5,000, in addition to attorney fees, for violations).
289 See Wis. A.B. 218 (confirming the state enforcement amount of not more than $1,000).
290 See H.R. Res. 5050 (explaining the civil penalties and enforcement policies under SNOPA).
stored.\textsuperscript{292} Also, rather than introducing brand new, standalone legislation, the PPA would amend the existing Computer Fraud and Abuse Act.\textsuperscript{293}

The PPA would prohibit an employer from compelling or coercing any person “to authorize access, such as by providing a password or similar information . . . to a protected computer that is not the employer’s protected computer, and thereby obtains information from such protected computer.”\textsuperscript{294} It would also prohibit an employer from discharging, disciplining, or discriminating against any person for failing to provide access to such protected computer, or for retaliating against a person who has instituted a proceeding or has testified or will testify in any related proceeding.\textsuperscript{295} The PPA uses the existing definition for “protected computer.”\textsuperscript{296}

The thrust of this bill is technology-neutral because it does not speak in narrow terms like social media, social networking site, electronic mail, etc.\textsuperscript{297} Reference to specific terms would prevent access to any site or service not maintained on an employer’s protected computer, even if an employee used an employer’s protected computer to access such site or service.\textsuperscript{298} This approach would generally be much broader than those discussed above.

The PPA would provide exceptions for employers if “there are reasonable grounds to believe that the information sought to be obtained is relevant . . . to protecting the intellectual property, a trade

\textsuperscript{292} See id. (emphasizing the protection lies with the computer where information is stored).
\textsuperscript{293} See id. (proposing the PPA as an amendment to Section 1030(c) of Title 18, United States Code, known as the Computer Fraud and Abuse Act).
\textsuperscript{294} Id.
\textsuperscript{295} See id. (prohibiting specific activities by employers).
\textsuperscript{296} See 18 U.S.C. § 1030(e)(2) (2012) (defining “protected computer” as “a computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in or affecting interstate or foreign commerce or communication of the United States”)); S. Res. 3074 (showing no change to the “protected computer” definition given at 18 U.S.C. § 1030(e)(2)i).
\textsuperscript{298} See id. (indicating the resulting impact of the bill’s narrow language).
secret, or confidential information" of the employer, 299 or if "the employer discharges or disciplines a person for good cause and is not motivated by an activity protected by this section." 300 Violations of the law would be punishable by fines. 301

**Conclusion**

As is often the case when states seek to draft legislation addressing a new societal or technical issue, we are afforded an opportunity to watch, in the clever words often uttered by the Supreme Court, our "laboratory of the states." 302 Thirteen states have already passed legislation in this area with more states sure to follow. As is also often the case, many states will model their proposed legislation after other states’ laws or bills. That is certainly evident here. While the four early actors - California, Illinois, Maryland and Michigan - have some very different approaches to the problem, many of the next wave of states to enact and propose legislation borrowed language directly from these earlier models.

---

300 See id. at § 2 (d)(2)(B)(i). There are also exceptions for employees who work with individuals under the age of 13 and for executive branch and military personnel who come into possession of classified information. See § 2 (d)(2)(B)(i); see also

…the prohibition in such subsection shall not apply to an employer’s actions if….a State enacts a law that specifically waives subsection (a)(8) with respect to employees who work with individuals under 13 years of age, and the employer’s action relates to an employee in such class; or an Executive agency…. a military department…. or any other entity within the executive branch that comes into possession of classified information. § 2 (d)(2)(B)(iii)

301 See id. at § 2 (b)(2)(5) (stating “a fine under this title, in the case of an offense under subsection (a)(8) or an attempt to commit an offense punishable under this paragraph”).
One of the more interesting examples of this is the bill proposed by Nebraska.\textsuperscript{303} It borrows its title and almost all of its definition section from Delaware.\textsuperscript{304} Its definition of “social networking site,” excludes electronic mail, just like Illinois.\textsuperscript{305} Its prohibitions against requiring disclosure of password information, requiring access in the presence of an employer, and accessing a site or account indirectly through another person also come from Delaware,\textsuperscript{306} except the phrase “provide or disclose,” which comes from New Jersey.\textsuperscript{307} Its prohibitions against requiring an employee to waive the protections against retaliation or discrimination are also borrowed from New Jersey.\textsuperscript{308} Its prohibition against employees downloading proprietary or financial data is taken from Maryland.\textsuperscript{309} Its provision permitting employers to promulgate policies concerning the use of employer’s equipment is borrowed from Illinois.\textsuperscript{310} The provision permitting an employer to require disclosure of account information when the equipment is owned by the employer comes from Michi-
gan.\textsuperscript{311} Conducting an investigation based upon receipt of information about illegal downloading of proprietary information or financial data is borrowed from Maryland.\textsuperscript{312} And the provision permitting use of information available in the public domain probably comes from either Illinois or Michigan.\textsuperscript{313} Nebraska has certainly done a very good job of comparing other states’ legislation and choosing what it believes are the best provisions to include.

\textsuperscript{311} Compare Neb. L.B. 58 at § 7(2) (permitting employers to require access information to employer-provided devices and services), with Mich. Pub. Acts 478 at § 5(1)(a) (providing same permissions).

\textsuperscript{312} Compare Neb. L.B. 58 at § 7(4) (permitting employers to investigate an appropriate use of websites by employees), with MD. CODE ANN. at § 3-712 (e)(2) (providing same allowances.).

\textsuperscript{313} Compare Neb. L.B. 58 at § 7(3) (permitting employers to view employee information that is in public domain), with III. COMP. STAT. ANN. 55/10 at § 10(b)(3) (providing same permissions as L.B. 58 § 7(3)), and Mich. Pub. Acts 478 at § 5(3) (providing same permissions).