NO SURFING ALLOWED: A REVIEW & ANALYSIS OF LEGISLATION PROHIBITING EMPLOYERS FROM DEMANDING ACCESS TO EMPLOYEES' & JOB APPLICANTS' SOCIAL MEDIA ACCOUNTS

*Robert Sprague**

TABLE OF CONTENTS

* J.D., M.B.A. Associate Professor, University of Wyoming College of Business Department of Management & Marketing. The author thanks Kellsie Jo Nienhuser, J.D. 2015, University of Wyoming College of Law, for her valuable assistance in providing background research for this article.

I. INTRODUCTION

In November 2010, Robert Collins reapplied for his job as a Corrections Supply Officer with the Maryland Department of Public Safety and Correctional Services after he had taken a leave of absence earlier that year.[1] Before they can be rehired, "corrections officers who have had a break in service [must] undergo a recertification, . . . [which] includes fingerprinting, a renewed background check, and [an] interview."[2] During his recertification interview, Collins was asked whether he uses social media and when he replied that he uses Facebook, he was then asked for his Facebook username and password.[3]

In April 2011, Kimberly Hester, an elementary school teacher's aide in Michigan, posted a photo on her Facebook page of "a coworker's pants around her ankles and a pair of shoes, with the caption 'Thinking of you.'"[4] "A parent and Facebook friend of Hester's saw the photo and complained to the school."[5] When Hester refused the school superintendent's demand for access to her Facebook account, she was placed on unpaid leave.[6]

These two incidents, one involving a job applicant and the other an employee, sparked national media attention, which evidently caught the eye of a number of state and U.S. legislators. In 2012, a total of twenty-eight bills were introduced in Congress and fourteen states prohibiting employers from requesting or requiring username and password access to employees' and job applicants' personal online accounts.[7] Four of

[1] Letter from Deborah A. Jeon, Legal Dir., ACLU of Md., to Sec'y Gary D. Maynard, Md. Dep't of Pub. Safety & Corr. Servs. 1–2 (Jan. 25, 2011), *available at* http://www.aclu-md.org/uploaded_files/0000/0041/letter-_collins_final.pdf.

[2] *Id*. at 2.

[3] *Id*. at 1. Collins was told interviewees were required to provide social media login information as "a standard part of the [Department of Corrections'] process for hiring and recertification . . . to enable the [Department] to review wall postings, email communications, photographs, and friend lists, in order to ensure that those employed as corrections officers are not engaged in illegal activity or affiliated with any gangs." *Id*. at 2.

[4] Emil Protalinski, *Teacher's Aid Fired for Refusing to Hand over Facebook Password*, ZDNET (April 1, 2012, 6:15 PM), http://www.zdnet.com/blog/facebook/teachers-aide-fired-for-refusing-to-hand-over-facebook-password/11246.

[5] *Id*.

[6] *Id*.

[7] Password Protection Act of 2012, H.R. 5684, S. 3074, 112th Cong. (2012); Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012). *See Employer Access to Social Media Usernames and Passwords: 2012 Legislation*,

the state bills passed.[8] In 2013, at total of sixty-one such bills were introduced in Congress and thirty-five states,[9] with eight states enacting legislation.[10] As of January 14, 2014, some thirty bills in sixteen states have been reintroduced or carried over, with two states, Florida and Oklahoma, introducing such legislation for the first time.[11] The two federal bills, the Password

NAT'L CONFERENCE STATE LEGISLATURES (last updated Jan. 17, 2013), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx (providing a summary of state bills, including those for California, Delaware, Illinois, Maryland, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, Pennsylvania, South Carolina, and Washington).

[8] CAL. LAB. CODE § 980 (West 2014); 820 ILL. COMP. STAT. 55/10 (2014); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2014); MICH. COMP. LAWS §§ 37.272–278 (2014). In addition, six states (California, Delaware, Illinois, Maryland, Michigan, and New Jersey) enacted similar legislation applied to educational institutions, instead of employers; analysis of the educational institution legislation is beyond the scope of this article.

[9] Password Protection Act of 2013, H.R. 2077, S. 1426, 113th Cong. (2013); Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013). *See Employer Access to Social Media Usernames and Passwords: 2013 Legislation*, NAT'L CONFERENCE STATE LEGISLATURES (last updated Jan. 14, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2013 (providing a summary of state bills, including those for Arizona, Arkansas, California, Colorado, Connecticut, Georgia, Hawaii, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, Texas, Utah, Vermont, Washington, and Wisconsin).

[10] ARK. CODE ANN. § 11-2-124 (West 2014); COLO. REV. STAT. § 8-2-127 (2014); A.B. 181, 77th Sess. (Nev. 2013) (amending NEV. REV. STAT. ANN. ch. 613 (West 2014)); N.J. STAT. ANN. §§ 34:6B-5–10 (West 2014); N.M. STAT. ANN. § 50-4-34 (West 2014); H.B. 2654, 2013 Or. Laws ch. 204 ((2013), amending OR. REV. STAT. ch. 659A)); UTAH CODE ANN. §§ 34-48-101–301 (West 2014); WASH. REV. CODE §§ 49.44.200, 205 (2014). In addition, Vermont enacted Senate Bill 7 which established a committee "to study the issue of prohibiting employers from requiring employees or applicants for employment to disclose a means of accessing the employee's or applicant's social network account." S. 7, Act 47, 2013-2014 Leg. Sess. (Vt. 2013) (to be codified at 21 VT. STAT. ANN. tit. 21, § 495(j) (2014)). In its January 14, 2014 report, the committee reported that is "members did not reach consensus on the issue of social network privacy provisions, and, therefore, were unable to make a recommendation for proposed legislation." VT. DEP'T OF LABOR, 2013 SUMMER STUDY COMMITTEE REPORT ON SOCIAL MEDIA PRIVACY (Jan. 14, 2014), *available at* http://www.leg.state.vt.us/reports/2014ExternalReports/296108.pdf.

[11] *See Employer Access to Social Media Usernames and Passwords: 2014 Legislation*, NAT'L CONFERENCE STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014 (last updated Feb. 21, 2014) (providing a summary of state bills, including those for Florida, Georgia, Hawaii, Iowa,

Protection Act of 2013 and the Social Networking Online Protection Act are still active.[12]

This article examines this recent legislative phenomenon from a variety of perspectives. First, the twelve enacted state statutes are summarized and analyzed.[13] Next, this article raises the issue of whether this legislation is even needed, from both practical and legal perspectives, focusing on: (a) how prevalent the practice is of requesting employees' and job applicants' social media access information; (b) whether alternative laws already exist which prohibit employers from requesting employees' and job applicants' social media access information; and (c) whether any benefits can be derived from this legislative output. This article then concludes with an analysis of the potential impact of this legislation on employees, job applicants, and employers.

II. EMPLOYEE PASSWORD PRIVACY LEGISLATION—SOME SIMILARITIES BUT NO UNIFORMITY

Fundamentally, the enacted statutes and proposed bills prohibit employers from requesting or requiring employees and job applicants to provide access to their personal online communications that are normally not available to the general public. While similar in concept, this "employee password privacy"[14] legislation lacks uniformity in a number of respects.

Kansas, Maine, Massachusetts, Minnesota, Mississippi, Nebraska, New Hampshire, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, and Wisconsin).

[12] While govtrack assigns a zero percent chance of enactment for the Senate version of the Password Protection Act (*see* https://www.govtrack.us/congress/bills/113/s1426 (tracking the status of the Password Protection Act of 2013, S. 1426, 113th Cong. (2013))) as well as the Social Networking Online Protection Act (*see* https://www.govtrack.us/congress/bills/113/hr537 (tracking the status of the Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013))), it does assign a two percent chance of enactment for the House version of the Password Protection Act (*see* https://www.govtrack.us/congress/bills/113/hr2077 (tracking the status of the Password Protection Act of 2013, H.R. 2077, 113th Cong. (2013)).

[13] As will be discussed below, the twelve enacted statutes provide a representative sample, in terms of content, of the various proposed statutes over the past three legislative sessions; as such, the proposed statutes will not be discussed in detail, but will be occasionally referenced to contrast against existing law. *See* discussion *infra* Part II.

[14] Only three of the statutes have formal names, which vary—"Right to Privacy in the Workplace Act" (Illinois: 820 ILL. COMP. STAT. 55/10 (2014)); "Internet Privacy Protection Act" (Michigan: MICH. COMP. LAWS §§ 37.272–278 (2014)); "Internet Employment Privacy Act" (Utah: UTAH CODE ANN. § 34-48-

Although there are currently (as of early 2014) some thirty state bills and at least two federal bills pending, with only twelve state statutes enacted, those twelve statutes provide an almost perfect sample of the variations among all the legislative attempts to address this one basic issue of employer access to employee and job applicant social media username and password information. As such, this article's analysis will focus almost exclusively on the twelve enacted statutes.[15]

It should be noted at the outset, and also serving as an example of the variations among the proposed bills and enacted statutes, that New Mexico's recently enacted law is the only one (pending or enacted) that applies just to job applicants and not to employees as well.[16] As discussed more fully below, the statutes contain different types of specific prohibitions, varying definitions, a wide range of employer activities that are exempted from coverage, and many do not articulate any remedies in the event of violation.

A. Fundamental Statutory Prohibitions

All of the employee password privacy statutes contain a fundamental prohibition against employers requiring or requesting an employee or applicant to disclose his or her username and password to his or her social media account. But that is where the similarity ends. Summarized below are the variations among the statutes' prohibitions:

Arkansas and Nevada: Not only are employers prohibited from requiring or requesting, but they also cannot suggest or cause an employee or applicant to disclose his or her username and password to his or her social media account.[17] Nevada also

101 (West 2014)). For convenience, this legislation will be generally referred to herein as "employee password privacy" legislation or statutes.

[15] ARK. CODE ANN. § 11-2-124 (West 2014); CAL. LAB. CODE § 980 (West 2014); COLO. REV. STAT. § 8-2-127 (2014); 820 ILL. COMP. STAT. 55/10 (2014); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2014); MICH. COMP. LAWS §§ 37.272–278 (2014); A.B. 181, 77th Sess. (Nev. 2013) (amending NEV. REV. STAT. ANN. ch. 613 (West 2014)); N.J. STAT. ANN. §§ 34:6B-5–10 (West 2014); N.M. STAT. ANN. § 50-4-34 (West 2014); H.B. 2654, 2013 Or. Laws ch. 204 ((2013), amending OR. REV. STAT. ch. 659A)); UTAH CODE ANN. §§ 34-48-101–301 (West 2014); WASH. REV. CODE §§ 49.44.200, 205 (2014). It is essentially impossible to predict which pending bills will pass, with or without amendments; therefore, in-depth analysis of these pending bills could to a large extent prove to be moot.

[16] N.M. STAT. ANN. § 50-4-34(A) (West 2014).

[17] ARK. CODE ANN. § 11-2-124(b)(1)(A) (West 2014); Assembly B.

prohibits direct or indirect requests.[18]

Arkansas, Colorado, and Oregon: Employers are also prohibited from requiring, requesting, or suggesting that an employee or applicant add an employee, supervisor, or administrator (or employment agency in Oregon) to the list or contacts associated with the employee's or applicant's social media account, or (excluding Oregon) change the privacy settings associated with his or her social media account.[19]

California: Employers are also prohibited from requiring or requesting an employee or applicant to access personal social media in the presence of the employer or divulge any personal social media (except as exempted elsewhere in the statute).[20]

Colorado, Maryland, and New Jersey: Employers are also prohibited from requiring, requesting, or (in Colorado, suggesting) that an employee or applicant disclose other means for accessing his or her personal account or service through his or her personal electronic communications device.[21]

Illinois and New Mexico: It 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 or to demand access in any manner to an employee's or prospective employee's account or profile on a social networking website.[22]

Michigan: An employer shall not request an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the

181, § 2(1)(a), 77th Gen. Assemb., Reg. Sess. (Nev. 2013) (amending NEV. REV. STAT. ANN. ch. 613 (West 2014)).

[18] Assemb. B. 181, § 2(1)(a), 77th Gen. Assemb., Reg. Sess. (Nev. 2013).

[19] ARK. CODE ANN. § 11-2-124(b)(1)(B), (C) (West 2014); COLO. REV. STAT. § 8-2-127(2)(a) (2014); H.B. 2654 § 1(b), 77th Leg. Assemb., Reg. Sess. (Or. 2013) (effective Jan. 1, 2014, amending OR. REV. STAT. ch. 659A).

[20] CAL. LAB. CODE § 980(b)(2), (3) (West 2014).

[21] COLO. REV. STAT. § 8-2-127(2)(a) (2014); MD. CODE ANN. LAB. & EMPL. § 3-712(b)(1) (West 2014); N.J. STAT. ANN. § 34:6B-6 (West 2014).

[22] 820 ILL. COMP. STAT. 55 / 10(b)(1) (2014); N.M. STAT. ANN. § 50-4-34(A) (West 2014). Recall, though, that New Mexico's statute only applies to prospective employees (i.e., applicants).

employee's or applicant's personal internet account.[23]

Oregon: Employers are also prohibiting from compelling 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 is accessed by the account holder's user name and password, password or other means of authentication.[24]

Washington: In the broadest enacted prohibition, employers are prohibited from requesting, requiring, or otherwise coercing an employee or applicant to: (a) disclose login information for the employee's or applicant's personal social networking account; (b) 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; (c) to add a person, including the employer, to the list of contacts associated with the employee's or applicant's personal social networking account; or (d) 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.[25]

Nine of the statutes prohibit employers from retaliating against employees and job applicants who refuse a request that is prohibited under the statutes.[26] Prohibited retaliation is usually in the form of actual or threatened, for employees, discharge, discipline, or other penalties, and for job applicants, refusal to hire. New Jersey also prohibits employers for retaliating against an individual who reports an alleged violation of the act or assists or participates in any investigation, proceeding, or action

[23] MICH. COMP. LAWS SERV. § 37.273(a) (LexisNexis 2014).

[24] H.B. 2654, § 1(c), 77th Leg. Assemb. Reg. Sess. (Or. 2013).

[25] WASH. REV. CODE ANN. §§ 49.44.200(1)(a)–(d) (West 2014).

[26] ARK. CODE ANN. § 11-2-124(c) (West 2014); COLO. REV. STAT. § 8-2-127(3) (2014); MD. CODE ANN. LAB. & EMPL. § 3-712(c) (West 2014); MICH. COMP. LAWS SERV. § 37.273(b) (LexisNexis 2014); Assemb. B. 181, § 1(b), 77th Gen. Assemb., Reg Sess. (Nev. 2013) (amending NEV. REV. STAT. ANN. ch. 613 (2013)); N.J. STAT. ANN. § 34:6B-8(a) (West 2014); H.B. 2654, § 1(d), (e), 77th Leg. Assemb., Reg. Sess. (Or. 2013); UTAH CODE ANN. § 34-48-201(2) (West 2014); WASH. REV. CODE ANN. § 49.44.200(1)(e) (West 2014).

concerning a violation of the act.[27] The statutes enacted in California, Illinois, and New Mexico do not contain any retaliation prohibitions.[28]

Finally, while the prohibitions apply to employers, Maryland's statute includes one prohibition that applies to employees: they may not download unauthorized employer proprietary information or financial data to their personal website, an Internet website, a web-based account, or a similar account.[29] Similarly, Colorado's statute prohibits an employee from disclosing information that is confidential under federal or state law or pursuant to a contract agreement between the employer and the employee.[30]

B. Definitions

The definitions contained in the statutes also reflect much of the lack of uniformity among the twelve employee password privacy statutes. While there is some commonality among the statutes, a review of just the definitions reveals the various approaches the legislative bodies have used to address employer social media access and employee password privacy.

1. Social Media & Other Personal Online Accounts

Central to the employer prohibitions is the type of employee account that is protected. The various statutes protect an employee's or job applicant's "social media account,"[31] "personal social media,"[32] "personal account or service" accessed through the employee's or applicant's "personal [in Colorado] electronic communications device,"[33] "social networking account,"[34] "account or profile on a social networking website,"[35] "personal internet

[27] N.J. STAT. ANN. §§ 34:6B-8(b)–(d) (West 2014).

[28] *See* CAL. LAB. CODE § 980(a) (West 2014); 820 ILL. COMP. STAT. 55/10(b)(1) (2014); N.M. STAT. ANN. § 50-4-34(A) (West 2014).

[29] MD. CODE ANN., LAB & EMPL. § 3-712(d) (West 2014).

[30] COLO. REV. STAT. § 8-2-127(7) (2014).

[31] ARK. CODE ANN. § 11-2-124(a)(3) (West 2014).

[32] CAL. LAB. CODE § 980(b)(1) (West 2014).

[33] COLO. REV. STAT. § 8-2-127(2)(a) (2014); MD. CODE ANN., LAB & EMPL. § 3-712(3) (West 2014). *See also* New Jersey: N.J. STAT. ANN. § 34:6B-5 (West 2014) (defining "personal account" as 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").

[34] COLO. REV. STAT. § 8-2-127(2)(a) (2014).

[35] 820 ILL. COMP. STAT. 55/10(b)(1) (2014); N.M. STAT. ANN. § 50-4-34(A) (West

account,"[36] "personal social media account,"[37] and "personal social networking account."[38] Four of the statutes define "social media" generically as an 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.[39] Otherwise, just like the prohibitions, many of the types of accounts protected vary by statute:

Illinois, New Jersey, and New Mexico: "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.[40]

Michigan: "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.[41]

New Jersey and Utah: "Personal [Internet, in Utah] 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.[42]

2014).

[36] MICH. COMP. LAWS § 37.273 (2014); UTAH CODE ANN. § 34-48-201(1) (West 2014).

[37] A.B. 181, § 4, 77th Sess. (Nev. 2013) (amending NEV. REV. STAT. ANN. § 613 (West 2014)); H.B. 2654, 77th Or. Legis. Assemb. (Or. 2013) (effective Jan. 1, 2014, amending OR. REV. STAT. § 659(A)).

[38] WASH. REV. CODE § 49.44.200(1) (2014).

[39] ARK. CODE ANN. § 11-2-124(a)(3) (West 2014); CAL. LAB. CODE § 980(a) (West 2014); A.B. 181, § 4, 77th Sess. (Nev. 2013); H.B. 2654, 77th Or. Legis. Assemb. (Or. 2013).

[40] 820 ILL. COMP. STAT. 55/10(b)(4) (2014); N.J. STAT. ANN. § 34-48-102 (West 2014); N.M. STAT. ANN. § 50-4-34(E) (West 2014).

[41] MICH. COMP. LAWS § 37.272(d) (2014).

[42] N.J. STAT. ANN. § 34:6B-5 (West 2014); UTAH CODE ANN. § 34-48-102(4)(a) (West 2014).

In addition, New Jersey and Utah expressly exclude 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.[43] Illinois followed suit, differentiating between personal and "professional" accounts in a 2013 amendment to its statute.[44] Similarly, Arkansas's statute excludes from its definition of a "social media account" 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 e-mail account or other software program owned or operated exclusively by an employer; (iii) Set up by an employee on behalf of an employer; or (iv) Set up by an employee to impersonate an employer through the use of the employer's name, logos, or trademarks.[45] However, Arkansas's statutes notes that the definition of "social media account" includes without limitation an account established with Facebook, Twitter, LinkedIn, MySpace, or Instagram.[46] Finally, Illinois's statute expressly excludes e-mail from its definition of "social networking website."[47]

2. Employer, Employee, & Applicant

Half of the statutes define an employer as both a private business as well as a public entity,[48] and none require a minimum number of employees, other than the obvious at least one, for the statute to apply.[49] The remaining half do not define "employer",[50] though New Jersey's statute states that

[43] N.J. STAT. ANN. § 34:6B-5 (West 2014); UTAH CODE ANN. § 34-48-102(4)(b) (West 2014).

[44] Pub. Act 98-501 § 3.5, Ill. Gen. Assem. (Ill. 2014).

[45] ARK. CODE ANN. § 11-2-124(a)(3)(B) (West 2014).

[46] *Id*. at § 11-2-124(a)(3)(C).

[47] 820 ILL. COMP. STAT. 55/10(b)(4) (2014).

[48] ARK. CODE ANN. § 11-2-124(a)(2) (West 2014); COLO. REV. STAT. § 8-2-127(1)(c) (2014); MD. CODE ANN. LAB. & EMPL. § 3-712(a)(4)(i) (West 2014); MICH. COMP. LAWS § 37.272(c) (2014); UTAH CODE ANN. § 34-48-102(2) (West 2014); WASH. REV. CODE § 49.44.200(5)(d) (2014).

[49] Utah and Washington include businesses that employ one or more workers in their definitions. UTAH CODE ANN. § 34-48-102(2) (West 2014); WASH. REV. CODE § 49.44.200(5)(d) (2014).

[50] California attempted to amend its statute in 2013 to define an employer as a private employer or a public employer, but the bill failed to pass. A.B. 25, 2013-2014 Leg. Sess. (Cal. 2012). The bill appears to still be active in the 2014 legislative session. *See* http://legiscan.com/CA/bill/AB25/2013.

"'[e]mployer' means an employer or the employer's agent, representative, or designee."[51] Two state statutes, Colorado and New Jersey, state expressly that "employer" does *not* include the department of corrections or any state or local law enforcement agency.[52] Only Arkansas's statute defines employee ("an individual who provides services or labor for wages or other remuneration for an employer"),[53] and only two statutes, Colorado and Maryland, define an "applicant", though merely as "an applicant for employment."[54]

C. Exemptions

The majority of employee password privacy statutes provide numerous exemptions from coverage—many actually provide more exemptions than prohibitions. The most common exemption is that the statutes do not prevent 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, particularly as defined under the Security and Exchange Act of 1934.[55] Many statutes contain a similar exemption providing that the statute does not affect the employer's rights or obligations to request an employee to disclose his or her username and password to access a social media account if the employee's social media account activity is reasonably believed to be relevant to a formal investigation or

[51] N.J. STAT. ANN. § 34:6B-5 (West 2014). Nevada cross-references to a separate section within its Employment Practices chapter (NEV. REV. STAT. ANN. § 613.440(1) (West 2014) (providing that an "[e]mployer" "includes any person acting directly or indirectly in the interest of an employer in relation to an employee or prospective employee")). 2013 Nev.Legis. Serv. 548 (§1.5) (West). In addition, the definitions of "employer" for Arkansas, Colorado, Maryland, Michigan, and Washington include an agent, representative, or designee of the employer. ARK. CODE ANN. § 11-2-124(a)(2) (West 2014); COLO. REV. STAT. § 8-2-127(1)(c) (2014); MD. CODE ANN. LAB. & EMPL. § 3-712(a)(4)(ii) (West 2014); MICH. COMP. LAWS § 37.272(c) (2014); WASH. REV. CODE § 49.44.200(5)(d) (2014).

[52] COLO. REV. STAT. § 8-2-127(1)(c) (2014); N.J. STAT. ANN. § 34:6B-5 (West 2014).

[53] ARK. CODE ANN. § 11-2-124(a)(1) (West 2014).

[54] COLO. REV. STAT. § 8-2-127(1)(a) (2014); MD. CODE ANN. LAB. & EMPL. § 3-712(a)(2) (West 2014).

[55] ARK. CODE ANN. § 11-2-124(e)(1) (West 2014); COLO. REV. STAT. § 8-2-127(4)(a) (2014); 820 ILL. COMP. STAT. 55/10(b)(3.5) (2014); MD. CODE ANN. LAB. & EMPL. § 3-712(e)(1) (West 2014); MICH. COMP. LAWS § 37.275(e)(2) (2014); 2013 NEV. STAT. ch. 548, A.B. 181, § 2(3) (2013); N.J. STAT. ANN. § 34:6B-10(a) (West 2014); 2013 OR. LAWS 204 §4(c) (2013); UTAH CODE ANN. § 34-48-202(3) (West 2014); WASH. REV. CODE § 49.44.200(3)(d) (2014).

related proceeding by the employer of allegations of an employee's violation of federal, state, or local laws or regulations, or employee misconduct or violation of the employer's written policies,[56] provided that, in two states, the employee's username and password shall only be used for the purpose of the formal investigation or a related proceeding.[57] Another common exemption is that the statutes will not preclude 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 or account, or the employer's computer system.[58]

Six of the statutes do not prohibit an employer investigating, discharging, or disciplining an employee for transferring the employer's proprietary, confidential, or financial information to the employee's personal social networking or web-based account.[59] Six of the statutes also do not apply to information available in the public domain.[60] Three of the statutes do not prohibit an employer from accessing electronic data, including electronic communications, stored on, or monitoring employees' use of, the employer's computer system.[61] Two statutes expressly absolve employers from liability for failing to request or require an employee or applicant to disclose or provide access to his or

[56] ARK. CODE ANN. § 11-2-124(e)(2)(A) (West 2014); CAL. LAB. CODE § 980(c) (West 2014); MICH. COMP. LAWS § 37.275(1)(c)(i) (2014); N.J. STAT. ANN. § 34:6B-10(c)(1) (West 2014); 2013 OR. LAWS 204 §4(c) (2013); UTAH CODE ANN. § 34-48-202(1)(c)(i) (West 2014); WASH. REV. CODE § 49.44.200(2)(b)–2(c)(i) (2014).

[57] ARK. CODE ANN. § 11-2-124(e)(2)(A)–(B) (West 2014); CAL. LAB. CODE § 980(c) (West 2014). Washington has a unique twist on this exemption, in that the employer can request the employee to share content from his or her personal social networking account, but the employer cannot request or require the employee to provide his or her login information. WASH. REV. CODE § 49.44.200(2)(a)–(d) (2014).

[58] CAL. LAB. CODE § 980(d) (West 2014); MICH. COMP. LAWS § 37.275(1)(a)(i) (2014); 2013 NEV. STAT.ch. 548, A.B. 181, § 2(2); UTAH CODE ANN. § 34-48-202(1)(a) (West 2014); WASH. REV. CODE § 49.44.200(3)(b) (2014).

[59] COLO. REV. STAT. § 8-2-127(4)(b) (2014); MD. CODE ANN. LAB. & EMPL. § 3-712(e)(2) (West 2014); MICH. COMP. LAWS § 37.275(1)(b) (2014); N.J. STAT. ANN. § 34:6B-10(c)(2) (West 2014); UTAH CODE ANN. § 34-48-202(1)(b) (West 2014); WASH. REV. CODE § 49.44.200(2)(c)(ii) (2014).

[60] 820 ILL. COMP. STAT. 55/10(b)(3) (2014); MICH. COMP. LAWS § 37.275(3) (2014); N.J. STAT. ANN. § 34:6B-10(d) (West 2014); N.M. STAT. ANN. § 50-4-34(C) (West 2014); 2013 OR. LAWS 204 §5 (2013); UTAH CODE ANN. § 34-48-202(4) (West 2014).

[61] 820 ILL. COMP. STAT. 55/10(b)(2)(B) (2014); N.M. STAT. ANN. § 50-4-34(B)(2) (West 2014); UTAH CODE ANN. § 34-48-202(1)(e) (West 2014).

her personal social media account,[62] and two statutes hold harmless an employer which inadvertently receives the user name and password to an employee's personal social media account, as long as it does not use the information to access the employee's personal social media account.[63]

D. Remedies

Interestingly, only half the enacted employee password privacy statutes expressly provide remedies in the event of a violation by an employer. Three statutes provide civil action remedies by individuals who are subject of a violation of the statute,[64] while the remaining three provide only state enforcement actions.[65] Michigan's statute provides both.[66] Washington, however,

[62] 2013 OR. LAWS 204 §3 (2013); UTAH CODE ANN. § 34-48-203(2) (West 2014).

[63] 2013 OR. LAWS 204 §6 (2013); WASH. REV. CODE § 49.44.200(4) (2014).

[64] Michigan: "An individual who is the subject of a violation of this act may bring a civil action to enjoin a violation . . . and may recover not more than $1,000.00 in damages plus reasonable attorney fees and court costs." MICH. COMP. LAWS § 37.278(2) (2014). Utah: A person aggrieved by a violation of the act may bring a civil cause of action against an employer in a court of competent jurisdiction and if the court finds a violation of the act, the court shall award the aggrieved person not more than $500. UTAH CODE ANN. § 34-48-301 (1)–(2) (West 2014). Washington: An employee or applicant aggrieved by a violation of the act may bring a civil action in which the court may award a prevailing employee or applicant injunctive or other equitable relief, actual damages, a penalty in the amount of $500, and reasonable attorneys' fees and costs. WASH. REV. CODE § 49.44.205(1) (2014).

[65] Colorado: "A person who is injured by a violation of the act may file a complaint with the department of labor and employment. The department shall investigate the complaint and issue findings thirty days after a hearing. The department may promulgate rules regarding penalties that include a fine of up to $1,000 for the first offense and a fine not to exceed $5,000 for each subsequent offense." COLO. REV. STAT. § 8-2-127(5) (2014). Maryland: "Whenever the Commissioner determines that the act has been violated, the Commissioner shall: (i) try to resolve any issue involved in the violation informally by mediation; or (ii) ask the Attorney General to bring an action on behalf of the applicant or employee", and "[t]he Attorney General may bring an action . . . for injunctive relief, damages, or other relief." MD. CODE ANN. LAB. & EMPL. § 3-712(f) (West 2014). New Jersey: "An employer who violates any provision of the act shall be subject to a civil penalty in an amount not to exceed $1,000 for the first violation and $2,500 for each subsequent violation, collectible by the Commissioner of Labor and Workforce Development . . ." N.J. STAT. ANN. § 34:6B-9 (West 2014).

[66] "A person who violates [the act] is guilty of a misdemeanor punishable by a fine of not more than $1,000.00." MICH. COMP. LAWS SERV. § 37.278(1) (LexisNexis 2014). "An individual who is the subject of a violation of this act may bring a civil action to enjoin a violation . . . and may recover not more than $1,000.00 in damages plus reasonable attorney fees and court costs." MICH. COMP. LAWS SERV. § 37.278(2) (LexisNexis 2014).

includes a provision allowing a court to award a prevailing party expenses and attorneys' fees upon a finding that the action was frivolous and advanced without reasonable cause.[67]

III. IS THIS LEGISLATION EVEN NEEDED?

Not only does the employee password privacy legislation vary widely in exactly what is prohibited and what is exempted, the legislation may not even be needed. First, there is little evidence of widespread requests or requirements by employers for employees' and job applicants' personal online account access information. Second, in those instances where employers have improperly accessed personal accounts or need access to those accounts, it has usually not been under scenarios contemplated by the legislation and existing law often already provides a remedy.

A. To What Extent Are Employers Requesting Restricted Access to Employees' & Job Applicants' Social Media Accounts?

According to the media, employers have recently been demanding Facebook passwords from job applicants and employees.[68] This meme appears to have begun with a March 2012 AP article.[69] Subsequently a number of media outlets reported a "trend" in employers requesting social media account access from job applicants.[70] Yet a close reading of the articles

[67] WASH. REV. CODE ANN. § 49.44.205(2) (West 2014).

[68] Manuel Valdes & Shannon McFarland, *Job Seekers Getting Asked for Facebook Passwords*, YAHOO! FINANCE, (Mar. 20, 2012, 7:55 AM), http://finance.yahoo.com/news/job-seekers-getting-asked-facebook-passwords-071251682.html.

[69] *Id*. (recounting two incidents with named job applicants, including Robert Collins in Maryland (*see supra* notes 1–3 and accompanying text), and identifying three separate government entities that have currently or in the past asked for job applicant social media access. "In their efforts to vet applicants, some companies and government agencies are going beyond merely glancing at a person's social networking profiles and instead asking to log in as the user to have a look around.").

[70] *See, e.g.* Sarah Shemkus, *Employers Asking for Facebook Passwords: Privacy Concern or Evolution of the Job Interview?*, SALARY.COM, http://www.salary.com/employers-asking-for-facebook-passwords-privacy-concern-or-evolution-of-the-job-interview/ (last visited Feb.. 21, 2014) (noting the "uproar" caused by Valdes's and McFarland's article that "reported on the trend of employers demanding access to applicants' Facebook accounts"); James Poulos, *Employers Demanding Facebook Passwords Aren't Making Any Friends*, FORBES (Mar. 22, 2012, 12:12 PM), http://www.forbes.com/sites/jamespoulos/

reveals that when it comes to reporting actual incidents of an employer demanding access to an employee's or job applicant's social media account, it appears there are only seven documented incidents, including the two reported in the Introduction to this article.[71] And while anecdotal evidence suggests that some college undergraduate and graduate students have been asked to login to their Facebook account in front of an employment recruiter, all the related incidents appear to have happened to a "friend of a friend"—the classic indicator of an urban legend.[72]

The few surveys that have asked the question directly reflect

2012/03/22/employers-demanding-facebook-passwords-arent-making-any-friends (suggesting that employers are "increasingly" requesting access to job applicants' Facebook pages as a condition of employment).

[71] *Supra* notes 1–6 and accompanying text; Tuan C. Nguyen, *Want to Get Hired? Please Provide Your Facebook Password*, SMARTPLANET (Dec. 20, 2011), http://www.smartplanet.com/blog/thinking-tech/want-to-get-hired-please-provide-your-facebook-password/9557 (reporting that a woman applying for work as a phone operator at a local police department in North Carolina was asked to provide usernames and passwords to her online social media accounts on the application form; providing also a picture of the application form). *See* City of Bozeman, Montana, *Consent and Release to Conduct Criminal Background and Reference Checks*, ERBLAWG.COM, http://www.erblawg.com/wp-content/uploads/2009/06/erblawbozeman.pdf (last visited Feb. 21, 2014) (displaying copy of Consent and Release to Conduct Criminal Background and Reference Checks form for job applicants to the City of Bozeman, Montana, reflecting a request for usernames and passwords to social media accounts); Matt Gouras, *City Drops Request for Internet Passwords*, NBCNEWS.COM (June 19, 2009, 8:42 PM), http://www.nbcnews.com/id/31446037/ns/technology_and_science-security/#.UZU1WkoSr7I (reporting that "[a] flood of criticism . . . prompted a Montana city [Bozeman] to drop its request that government job applicants turn over their user names and passwords to Internet social networking and Web groups"); Valdes & McFarland, *supra* note 68 (reporting that in addition to Robert Collins, Justin Bassett, a New York City statistician, had been asked to log into his Facebook account in the presence of a job interviewer, and that in addition to the city of Bozeman, Montana, the McLean County, Illinois, and Spotsylvania County, Virginia, sheriff's offices had routinely requested online access information). *But see infra* note 122, at 107–08 and accompanying text (presenting evidence that employers may be asking for access to employees' online social networks, though not by requesting usernames and passwords).

[72] *See* JAN HAROLD BRUNVAND, ENCYCLOPEDIA OF URBAN LEGENDS, UPDATED AND EXPANDED EDITION 154 (2012) (noting that "friend of a friend"—often denoted by the acronym FOAF—is "the oft-mentioned supposed original source of the incidents described in urban legends"); Mary B. Nicolini, *Is There a FOAF in Your Future? Urban Folk Legends in Room 112*, 78 ENG. J. 81, 81 (1989) ("A necessary component of the folk legend is the FOAF: a friend of a friend, as in 'This didn't happen to me, but it happened to a friend of a friend of mine. . . .' This is designed to lend authenticity to the tale and the teller; while not a firsthand witness, the teller has it from very good sources.") (alteration in original).

that, particularly in the private sector,[73] employers are not routinely asking for access to job applicants' social media accounts. For example, Littler Mendelson, a large labor and employment law firm, asked nearly 1000 C-suite executives, corporate counsel, and human resources professionals from corporations throughout the United States and ranging in market capitalization from less than $1 billion to more than $4 billion the following question: "Has your organization requested social media logins as part of the hiring or onboarding process?"[74] Ninety-nine percent of respondents answered the question in the negative.[75] In March 2013, an Ohio employment law attorney conducted an admittedly unscientific poll among his blog readers. Based on "hundreds" of responses, he reported the following results:

> Has your company ever asked a job applicant or employee to provide the login or password to a social media or other online account? No: 90%, Yes, an employee: 5%; Yes, an applicant: 3%; Yes, both: 1%. Have you ever been asked by an employer to provide the login or password to a social media or other online account? No: 95%; Yes: 5%. Has your company ever denied employment, or fired an employee, because an individual refused to disclose the login or password of a social media or other online site? No: 98%; Yes: 2%.[76]

And while there have been a very few reported cases involving employers requesting access to employees' Facebook or other social networking accounts,[77] as discussed below, they haven't

---

[73] Although Valdes and McFarland do not identify the employer Justin Bassett, the New York statistician, was interviewing with, all other documented incidents have involved a governmental entity. *See* Valdes & McFarland, *supra* note 69; *supra* notes 1–6 and accompanying text.

[74] LITTLER MENDELSON, EXECUTIVE EMPLOYER SURVEY REPORT 15–17 (June 2012), *available at* http://www.littler.com/files/Littler%20Mendelson%20Executive%20Employer%20Survey%20Report%202012_06-25-12.pdf.

[75] *Id*. at 15. *See also* PHILLIP L. GORDON ET AL., SOCIAL MEDIA PASSWORD PROTECTION AND PRIVACY—THE PATCHWORK OF STATE LAWS AND HOW IT AFFECTS EMPLOYERS 3 (2013), *available at* http://www.littler.com/files/press/pdf/LittlerReportSocialMediaPasswordProtectionaAndPrivacyThePatchworkOfStateLawsAndHowItAffectsEmployers.pdf ("Both the available anecdotal and empirical evidence, albeit limited, compel the conclusion that private employers are not asking applicants or employees for personal social media log-in credentials.").

[76] Jon Hyman, *The Results Are In: Social Media Password Survey*, OHIO EMPLOYER'S LAW BLOG (Apr. 4, 2013), http://www.ohioemployerlawblog.com/2013/04/the-results-are-in-social-media.html (concluding "this supposed practice is not much more than an answer in search of a problem").

[77] *See* GORDON ET AL., *supra* note 75, at 3 (explaining that some supervisors and executives may be requesting employees "Friend" them and suggestions as

necessarily involved the exact scenarios envisioned by the employee password privacy legislation.[78]

It is not surprising that Maryland—home to the first widely publicized request for a job applicant's social media access information—was the first state to enact protective legislation. Michigan—home to the only widely publicized request for an employee's social media access information—became the fourth state to enact protective legislation eight months later. It is also not surprising that most of the documented incidents arise from law enforcement-type government agencies attempting to perform extensive background checks on applicants,[79] which arguably require more extensive background checks.[80]

Why the interest in enacting protective legislation in so many states, as well as the U.S. Congress? It appears that publicity surrounding the two incidents reported at the beginning of this article and a few additional incidents sparked a concern over employee and job applicant privacy, and coupled with the fact that a few states had begun enacting and considering protective legislation, legislators felt compelled to address the issue.[81] And a

to why employees comply).

[78] *Id.*

[79] *See* Neal Augenstein, *Md. AG: Requiring Employees' Personal Passwords Is Legal*, WTOP.COM (Feb. 23, 2011, 7:15 PM), http://wtop.com/?nid=46&sid=2282721 (reporting that Maryland's Attorney General defended the social media screening practice of the Department of Corrections as necessary to ferret out possible gang affiliations of applicants); Valdes & McFarland, *supra* note 68 (reporting two sheriff's departments that use social media access to screen applicants). Colorado's and New Jersey's statutes expressly exclude law enforcement agencies from the definition of employer. COLO. REV. STAT. ANN. § 8-2-127(1)(c) (West 2014); N.J. STAT. ANN. § 34:6B-5 (West 2014).

[80] Mark B. Gerano, Note, *Access Denied: An Analysis of Social Media Password Demands in the Public Employment Setting*, 40 N. KY. L. REV. 665, 687 (2013) (noting that in some cases, such as in hiring a prison guard, a more intrusive background check may be justified).

[81] *See, e.g.*, Shemcus, *supra* note 70 (reporting that in March 2012, Senators Richard Blumenthal (D-Conn.) and Charles E. Schumer (D-N.Y.) "sent letters to the U.S. Equal Employment Opportunity Commission and the U.S. Department of Justice asking the agencies to launch investigations into the legality of what they called 'the disturbing trend'" of employers requesting social media passwords); California A.B. 1844 Synopsis (2011-2012 Sess.) (codified at CAL. LAB. CODE § 980 (West 2014)) ("[r]ecent media accounts have reported that some employers may have demanded access to the private social media accounts of employees and prospective employees, and these reports have naturally generated significant public concern across California and the entire nation about such potential encroachments on individual privacy. In response, several states including Maryland, Texas and Illinois are also considering similar legislation to prohibit this practice."); *LD 1194—Ought to Pass: Hearing*

few commentators have advocated for the need for such legislation.[82]

So, if there is minimal need for this type of legislation from a practical level, is it even necessary from a legal perspective—in other words, do laws already exist to protect employees and job applicants from the conduct outlawed in the newly enacted and proposed employee password privacy legislation?

B. Do Existing Laws Already Protect Employees & Job Applicants from Prying Employers?

While Brian Pietrylo worked at a Hillstone Restaurant Group-owned Houston's restaurant as a server, he created an access-controlled MySpace page called the "Spec-Tator" for invited employees to "vent about any BS we deal with [at] work without any outside eyes spying in on us."[83] Pietrylo invited other past

on H.P. 838 [L.D. 1194] Before the Joint Standing Comm. on Judiciary, 126th Leg., 1st Reg. Sess. (Me. 2013) (testimony of Shenna Bellows, ACLU Maine) (asserting that "[a] growing number of employers and schools are demanding that job applicants, employees, and students hand over the passwords to their private social media accounts such as Facebook" but identifying only one actual incident—Maryland's Robert Collins as described *supra* notes 1–3 and accompanying text); *Bus. & Labor Comm.*, 103rd Leg., 1st Sess. (Ne. 2013) (statement of Sen. Larson) ("[s]ix other states including Michigan, Illinois, and California, have passed laws similar to [Nebraska's L.B. 58] with the intent to protect the privacy of employees and applicants on the Internet."); A.B. 443, 2013-2014 Reg. Sess. (N.Y. 2014) Justification ("Recently, there have been reports of employers demanding login information, including username and password information to popular social media websites such as Facebook, Twitter [sic] as well as login information to email accounts and other extremely personal accounts."); S.B. 5211 (Wash. 2013) (Comm. Rep) (noting that "six states enacted legislation in 2012 to prohibit employers or institutions of higher education from requiring an employee, applicant, or student to provide a username or password to a social media account" and that "Washington law does not address requests by an employer to access to an employee's or prospective employee's social networking accounts").

[82] *See, e.g.*, Michelle Poore, *A Call for Uncle Sam to Get Big Brother Out of Our Knickers: Protecting Privacy and Freedom of Speech Interests in Social Media Accounts*, 40 N. KY. L. REV. 507, 507–08 (2013) (arguing that legislatures need to create statutes specifically tailored to the unique privacy concerns created by social media); Timothy J. Buckley, Note, *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, 877 (2013) (suggesting language for a federal bill gleaned from state bills). *But see* Gerano, *supra* note 80, at 687 (arguing that an outright ban on password demands fails to address special concerns in the public employment context where a more thorough background check is justified).

[83] Pietrylo v. Hillstone Rest. Grp., No. 06–5754 (FSH), 2008 WL 6085437, at

and present Houston's employees to join the group, including Karen St. Jean, a greeter at Houston's, who became an authorized participant in the MySpace group.[84] At some point, Robert Anton, a Houston's manager, asked St. Jean to provide him the password to access the Spec-Tator, which she did. Although St. Jean stated that she was never explicitly threatened with any adverse employment action, she stated she gave her password to a member of management solely because he was a member of management and she thought she might get in some sort of trouble if she didn't.[85] "Anton used the password provided by St. Jean to access the Spec-Tator from St. Jean's MySpace page."[86] Houston's managers considered the posts on Spec-Tator to be offensive and Pietrylo and another employee, Doreen Marino, were fired.[87] Pietrylo and Marino then sued Hillstone Restaurant Group for, inter alia, violation of the Stored Communications Act[88] and common law invasion of privacy.[89]

The Stored Communications Act (SCA) prohibits unauthorized access to electronic communications while in electronic storage.[90] However, there is no violation of the SCA if access is authorized by a user of the service storing the electronic communications "with respect to a communication of or intended for that user."[91] The District Court for the District of New Jersey upheld the jury's verdict that the restaurant manager had violated the SCA because St. Jean's purported authorization was coerced.[92] This unreported decision supports the argument that an employer who coerces or compels an employee to turn over social media access information can possibly violate the SCA.[93] One could

*1 (D.N.J. July 25, 2008). The MySpace page also stated "This group is entirely private, and can only be joined by invitation." *Id*.

84 *Id*.

85 *Id*.

86 *Id*.

87 *Id*. at *2.

88 *Id*.

89 *Id*.

90 18 U.S.C. § 2701(a) (2013).

91 *Id*. § 2701(c)(2).

92 Pietrylo v. Hillstone Rest. Grp., No. 06–5754 (FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009). The jury, however, rejected the plaintiffs' common law invasion of privacy claim. *Id*. at *1.

93 *Cf*. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002) (holding that management's access to an employee's restricted-access website by requesting access information from authorized users violated the SCA because the users had never actually "used" the website in question and therefore were not technically "users" who could authorize access under 18

certainly argue that just as an employee may be coerced into providing social media access information out of fear of losing her job, a job applicant may be just as coerced out of fear of being disqualified for a job.[94]

In June 2009, Deborah Ehling, a registered nurse employed by the Monmouth-Ocean Hospital Service Corporation ("MONOC") since 2004, posted a comment on Facebook regarding a shooting that took place at the Holocaust Museum in Washington, DC, stating:

> An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards. . .go to target practice.[95]

Only Ehling's Facebook Friends could view the post and Ehling had not "Friended" any of MONOC's management.[96] Ehling alleged that MONOC management became aware of the posting through a supervisor "coercing, strong-arming, and/or threatening [an] employee [who was a Facebook Friend with Ehling] into accessing his Facebook account on the work computer in the supervisor's presence."[97] The District Court for the District of New Jersey refused to dismiss Ehling's common law privacy claim against MONOC, concluding that she "may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to

U.S.C. § 2701(c)(2)).

[94] "This practice is coercion if you need a job." Joshua Waldman, *What to Do if a Company Asks for Your Facebook Password in a Job Interview*, THE LADDERS (quoting Lori Andrews, IIT Chicago-Kent College of Law professor), http://www.theladders.com/career-advice/what-to-do-if-company-asks-for-facebook-password-in-job-interview (last visited Jan. 30, 2014). Waldman presents a compelling scenario for coercion: "Imagine you've been on the job market for about six months. You are paying your mortgage on your credit cards at this point. Your unemployment benefits are about to run out and your job prospects remain dismal, no matter what you seem to do. Finally, you land a killer opportunity, pass the phone screen and show up to an interview with a hiring manager. Just as you think you're about to close the deal, she spins her computer screen around and asks you to login to your Facebook account." *Id*.

[95] Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 370 (D.N.J. 2012).

[96] *Id*.

[97] *Id*.

protect her Facebook page from public viewing."[98]

Ehling provides an argument that coercing an employee to access a Facebook account could potentially violate the employee's common law right of privacy.[99] The problem with applying *Pietrylo* and *Ehling* to the current and proposed employee password privacy legislation is that in both *Pietrylo* and *Ehling*, the employer did not demand access from the plaintiff-employee. The employers did not request access directly to Pietrylo's and Ehling's personal accounts—which is what is prohibited in the employee password privacy legislation—they allegedly merely viewed communications stored on those accounts through other employees' authorized access.[100] A plain reading of a majority of the enacted and proposed employee password privacy legislation—prohibiting employers from requesting usernames and passwords and other means of access to employees' and job applicants' own social media accounts, and, in most cases, prohibiting employers from taking adverse action against employees or refusing to hire applicants who do not comply—does not appear to address the scenarios presented by *Pietrylo* and *Ehling*.[101] In *Pietrylo* and *Ehling*, the employees who were disciplined or fired were never themselves requested to provide access information.[102]

---

[98] *Id*. at 374.

[99] The District Court for the District of New Jersey subsequently dismissed Ehling's invasion of privacy claim on the basis that she failed to produce sufficient evidence that her co-worker was compelled to access the information at issue. *See* Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659 (D.N.J. 2013) ("The evidence does not show that Defendants obtained access to Plaintiff's Facebook page by, say, logging into her account, logging into another employee's account, or asking another employee to log into Facebook. Instead, the evidence shows that Defendants were the passive recipients of information that they did not seek out or ask for. Plaintiff voluntarily gave information to her Facebook friend, and her Facebook friend voluntarily gave that information to someone else.").

[100] *See* Pietrylo v. Hillstone Rest. Grp., No. 06–5754 (FSH), 2008 WL 6085437, at *1 (D.N.J. July 25, 2008) (explaining that manager Robert Anton gained access to the account by asking St. Jean, not the Plaintiff, for the password); *see also Ehling*, 872 F. Supp. 2d at 370 (noting that MONOC gained access to the Plaintiff's account by having a fellow employee, who was also the Plaintiff's Facebook friend, grant them access).

[101] *But see supra* notes 19 and 25 and accompanying text (discussing statutes enacted by Arkansas, Colorado, Oregon, and Washington that would prohibit employers from accessing an employee's or job applicant's social networking profile or account indirectly through any other person who is a social networking contact of the employee or applicant).

[102] *See Pietrylo*, 2008 WL 6085437, at *1–2 (explaining that the Plaintiff was terminated after St. Jean, another employee, provided the password to access

There have been two reported cases in which an employer has accessed a former employee's personal e-mail account, not by requesting or requiring a username and password, but because the username and password were automatically saved for login.[103] In *Pure Power Boot Camp, et al,. v. Warrior Fitness Boot Camp*, the employer accessed a former employee's personal Hotmail account which the employee had accessed using the employer's computer equipment.[104] The employee's username and password were pre-saved on the employer's computer.[105] The court concluded that the former employee had a reasonable expectation of privacy in his "personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords . . . ."[106] The court also concluded that the employer violated the SCA by accessing the former employee's personal e-mail accounts—rejecting the employer's argument the employee had given "implied consent" to access by leaving the username and password saved on the employer's computer.[107]

In a similar case, an employer accessed a personal AOL e-mail account used by a former employee for both personal and business communications, again using login information pre-saved on the employer's computer.[108] In this case, the former employee had originally installed access to her personal AOL

the account); *see also Ehling*, 872 F. Supp. 2d at 370 (noting that Plaintiff was terminated in July, 2011 after another employee provided MONOC with access to view Plaintiff's account).

[103] Pure Power Boot Camp, et al., v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 561 (S.D.N.Y. 2008); Borchers v. Franciscan Tertiary Province of the Sacred Heart, Inc., 962 N.E.2d 29, 34 (Ill. App. Ct. 2011).

[104] *Pure Power Boot Camp,* 587 F. Supp. 2d at 552.

[105] *Id*. The employer was also able to access the former employee's personal Gmail account because the employee had e-mailed his Gmail username and password to his Hotmail account. *Id*. The employer also "guessed" the former employee's password for his e-mail account at the new, competing business he had opened. *Id*.

[106] *Id*. at 561.

[107] *Id*. at 562. "There is no sound basis to argue that [the former employee], by inadvertently leaving his Hotmail password accessible, was thereby authorizing access to all of his Hotmail e-mails, no less the e-mails in his two other accounts. If he had left a key to his house on the front desk at [Pure Power Boot Camp], one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings. And, to take the analogy a step further, had the person rummaging through the belongings in [the employee's] house found the key to [his] country house, could that be taken as authorization to search his country house. We think not. The Court rejects the notion that carelessness equals consent." *Id*. at 561.

[108] *Borchers*, 962 N.E.2d at 34.

account on her employer's computer while the employer was transitioning to a new e-mail system.[109] The former employee used her AOL account for some business communications during the transition, but later used her employer's new e-mail account exclusively for business communications and her own AOL account exclusively for personal communications—including communications with her attorney when she was considering a sexual harassment action against the employer.[110] The Illinois Appellate Court reversed the trial court's granting of the employer's motion to dismiss the former employee's SCA and common law privacy claims.[111] In general, courts have recognized privacy rights in personal online accounts versus accounts provided by the employer.[112]

One might argue that these two scenarios fall within the language of a large proportion of the employee password privacy legislation that prohibits an employer from requesting or requiring disclosure of the username, password, "or other means of accessing" the employee's or job applicant's personal online account.[113] However, since the phrase is modified by a request or requirement by the employer to disclose that other means of accessing, there is a strong argument that the two scenarios above would not actually be covered by the legislation.

As discussed above, the newly enacted and proposed employee password privacy legislation contains not only prohibitions against certain employer conduct, but also provides numerous exemptions from coverage.[114] One exemption is observing information that is in the public domain.[115] This appears to be a

[109] *Id*. at 33.

[110] *Id*. at 33, 36–37.

[111] *Id*. at 697–98.

[112] *Cf*. Stengart v. Loving Care Agency, 990 A.2d 650, 663 (N.J. 2010) (holding that an employee had a privacy interest in e-mail messages stored on a personal online account), *with* Holmes v. Petrovich Dev. Co., 191 Cal.App.4th 1047, 1051 (Cal. Ct. App. 2011) (concluding that an employee had no privacy right in personal e-mail messages sent to her attorney through her employer's e-mail system; analogizing her e-mails "to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him").

[113] *See supra* note 21 and accompanying text (discussing statutes enacted by Colorado, Maryland, and New Jersey prohibiting employers from requiring, requesting, or suggesting employees or job applicants disclose other means of accessing their personal accounts).

[114] *See* discussion *supra* Part II.C.

[115] *See supra* note 60 and accompanying text (noting statutes enacted by

rather unnecessary provision, as it has been well established there is no privacy protection for information open to public viewing.[116] Most of the remaining exemptions appear to merely emphasize that the prohibitions do not supersede already existing employer rights to supervise, monitor, and maintain its information systems, as well as comply with various laws and regulations regarding employee online conduct.[117]

But can this legislation actually establish new rights? Many companies hire employees to maintain an online presence for the employer and disputes later arise as to who is entitled to access to those online accounts.[118] As discussed above, liability may rest on whether the employer exceeded its authority in violation of the SCA by accessing employee-controlled accounts.[119] Some of the new and proposed laws exclude accounts created by employees for business purposes of the employer or apply only to accounts used exclusively for personal communications unrelated to the business purposes of the employer.[120] With the growing business presence in online social media, coupled with the comingling of workplace and personal use of—sometimes employer-provided—online accounts and communications devices,[121] it is inevitable that disputes will arise as to who exactly has rights of access and content control. If the employee password privacy laws do not prohibit an employer from requesting or requiring access information for accounts used, at

Illinois, Michigan, New Jersey, New Mexico, Oregon, and Utah permitting employers to obtain information about an employee that exists in the public domain).

116 *See* Maremont v. Susan Fredman Design Grp., No. 10 C 7811, 2011 WL 6101949, at *8 (N.D. Ill. Dec. 7, 2011) (holding that an employee's posts on Facebook and Twitter were not private and therefore not subject to protection); *see also* Sumien v. CareFlite, No. 02-12-00039-CV, 2012 WL 2579525, at *3 (Tex. Ct. App. July 5, 2012) (refusing to find a right of privacy in Facebook posts viewed by a friend-of-a-friend); Gill v. Hearst Publ'g Co., 253 P.2d 441, 445 (Cal. 1953) (holding that a couple photographed at a farmer's market had no cause of action against the photograph's publisher).

117 *See* discussion *supra* Part II.C.

118 *See Maremont*, 2011 WL 6101949 at *2 (discussing an employee's use of social media accounts during their employment).

119 *See supra* notes 90–94, 107, and 111, and accompanying text.

120 *See supra* notes 42–45 and accompanying text.

121 *See* Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 64 (2012) ("Employer-provided laptops and mobile devices do not discriminate between private and professional communications or locations. These 'boundary-crossing' technologies blur the already elusive line between the private and the public, the home and the workplace.").

least to some degree, for the employer's business, would that constitute an implied authorization on the part of the employee to access those accounts sufficient to satisfy the SCA?

In *Maremont v. Susan Fredman Design Grp., Ltd.*, the defendant, an interior design firm, hired the plaintiff as its Director of Marketing, Public Relations, and E-commerce.[122] In fulfilling her duties, the defendant established a Twitter following within the design community, created a blog hosted on the employer's website, and created a Facebook account for the employer—all of which were interlinked.[123] The plaintiff also maintained her own Facebook page and the Twitter account was evidently her own personal account.[124] She also stored access information for all the accounts within the defendant's computer system.[125] After being struck by an automobile, the plaintiff ultimately stopped working for the plaintiff, but while she was hospitalized, the plaintiff alleged the defendant updated content on the plaintiff's personal Twitter and Facebook accounts.[126] The court refused to dismiss the plaintiff's SCA claim against the defendant, concluding there were disputed issues of material fact as to whether the defendant exceeded its "authority in obtaining access to Maremont's personal Twitter and Facebook accounts."[127] Although the court noted that it was "undisputed that Maremont's personal Twitter and Facebook accounts were not for the benefit of [her employer]," Maremont did promote her employer's business on those accounts, particularly the Twitter account.[128]

In contrast, in *Ardis Health, LLC v. Nankivell*, there was minimal commingling of personal and work-related accounts and the court had no difficulty declaring employer access rights.[129] In *Ardis Health*, the defendant had been hired as a Video and Social Media Producer to produce videos and maintain websites, blogs, and social media pages in connection with the online marketing

[122] Maremont v. Susan Fredman Design Grp., No. 10 C 7811, 2011 WL 6101949, at *2 (N.D. Ill. Dec. 7, 2011)

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] *Id.* at *2–3.

[127] *Id.* at *5.

[128] *Id.* at *2.

[129] Ardis Health, LLC v. Nankivell, No. 11 Civ. 5013 (NRB), 2011 WL 4965172, at *4 (S.D.N.Y. Oct. 19, 2011).

of the plaintiffs' products.[130] The defendant was fired in June 2011 but refused to turn over access information to the plaintiffs' online accounts, leaving the plaintiffs unable to access a number of their online accounts and websites to update them as needed for their marketing purposes.[131] The District Court for the Southern District of New York ordered the defendant to turn over the access information, noting the plaintiffs "depend heavily on their online presence to advertise their businesses, which requires the ability to continuously update their profiles and pages and react to online trends."[132] The court even suggested that the defendant's unauthorized retention of the access information could form the basis of a claim of conversion.[133] However, the plaintiffs had to show they were suffering irreparable harm by not having access to their online accounts.[134] The court was willing to order the defendant to turn over the access information for online accounts that were vital to the plaintiffs' business,[135] but would a court be so willing if the accounts were "merely" important? At least within the jurisdictions that have enacted or may enact legislation which does not prohibit employers to require disclosure of access information to accounts associated with the employer's business, the employer would not have a high burden to establish the right to that information. It is therefore arguable that employee password privacy legislation which includes an exemption for employers requesting access information to accounts used in part for the employer's business will allow employers to legitimately obtain that information, without having to first show any harm to the business and without violating the SCA.

However, *Ardis Health* also involved issues beyond the scope of employee password privacy legislation, such as whether the former employee had the right to display selected portions of the plaintiffs' trademarked and copyrighted material within her

130 *Id*. at *1.
131 *Id*. at *2.
132 *Id*.
133 *See Id*. at *3.
134 *Id*. at *2.
135 *Id*. ("The inability to [continuously update their profiles and pages and react to online trends] unquestionably has a negative effect on plaintiffs' reputation and ability to remain competitive, and the magnitude of that effect is difficult, if not impossible, to quantify in monetary terms. Such injury constitutes irreparable harm.").

personal online portfolio.[136] Similarly, *Maremont* involved claims beyond unauthorized access, including trademark, right of publicity, and common right to privacy claims.[137] Additional cases involving disputed ownership over "comingled" online accounts do not involve access claims per se, instead raising claims beyond the scope of the employee password privacy laws, such as unauthorized use of name, misappropriation of identity, misappropriation of publicity, conversion, tortious interference with contract, intentional and negligent interference with prospective economic advantage, and misappropriation of trade secrets.[138]

IV. CONCLUDING ANALYSIS: CAUSING MORE HARM THAN GOOD?

A privacy advocate would naturally applaud the growing number of states that are enacting employee password privacy legislation—now twelve, with bills working their way through the legislative process in an additional sixteen states and the U.S. Congress.[139] It is too soon to tell whether it is a "good" thing that this legislation, as Gordon et al. argue, overturns decades of common law jurisprudence:

> The underlying premise of these laws is that an employer invades an applicant's or employee's privacy by viewing content on a restricted access social media account without the voluntary consent of the account holder. Digging one step deeper, these laws, at their core, assume that the content of a restricted access social media account is private no matter how many people the user

[136] *See id.* at *4–5 (denying plaintiffs' motion requesting the defendant to remove the material).

[137] Maremont v. Susan Fredman Design Grp., Ltd., No. 10 C 7811, 2011 WL 6101949, at *4–5, *6–8 (N.D. Ill. Dec. 7, 2011).

[138] *See* Eagle v. Morgan, No. 11–4303, 2013 WL 943350, at *6–8, *10–11, (E.D. Pa. Mar. 12, 2013) (unauthorized use of name, invasion of privacy by misappropriation of identity, misappropriation of publicity, conversion, tortious interference with contract); PhoneDog v. Kravitz, No. C 11–03474 MEJ, 2011 WL 5415612, at *6–7 (N.D. Cal. Nov. 8, 2011) (misappropriation of trade secrets); PhoneDog v. Kravitz, No. C 11–03474 MEJ, 2012 WL 273323, at *1–2 (N.D. Cal. Jan. 30, 2012) (intentional interference with prospective economic advantage); Christou v. Beatport, L.L.C., 849 F. Supp. 2d 1055, 1074–77 (D. Colo. 2012) (theft of trade secrets); *see also* Zoe Argento, *Whose Social Network Account? A Trade Secret Approach to Allocating Rights*, 19 MICH. TELECOMM. & TECH. L. REV. 201, 223–25 (2013) (arguing that these disputes are ultimately about the right to access the accounts' followers, necessitating a trade secrets approach to their resolution).

[139] *See* discussion *supra* Part II.

> invites to view that content and regardless of the relationship between the user and the viewer. Put more plainly, these laws are based on the belief that, for example, a Facebook user who has more than 500 "Friends," including current and former supervisors and other executives at his current employer, can establish the "privacy" of his content by using Facebook's privacy settings to restrict access to "Friends Only."

No court has ever construed the tort of invasion of privacy by intrusion upon seclusion so broadly.[140] Perhaps Gordon et al. miss the point, which is that the focus of the legislation is not how many Friends an employee or job applicant has, but that the employer, except in specific instances,[141] has no business—meant in a literal sense—prying into personal communications that have been clearly restricted to individuals which do not include the employer.

There is one potential pro-privacy result from the employee password privacy legislation. One exception to the employment-at-will doctrine is that employers are prohibited from discharging employees in violation of public policy.[142] This exception arose from a California case in which an employee was fired for giving truthful, subpoenaed testimony before a legislative committee.[143] Modern applications of the exception apply only to a well-defined public policy:

> An employee seeking protection under the public-policy exception in his or her wrongful-discharge claim must prove the following elements: (1) the existence of a clearly defined and well-recognized public policy that protects the employee's activity; (2) this public policy would be undermined by the employee's discharge from employment; (3) the employee engaged in the protected activity, and this conduct was the reason the employer discharged the employee; and (4) the employer had no overriding business justification for the discharge.[144]

One could argue that the employee password privacy

---

140 GORDON ET AL., *supra* note 75, at 4.

141 *See* discussion *supra* Part II.C.

142 Petermann v. Int'l Bhd. Teamsters, 174 Cal.App.2d 184, 189 (1959) ("To hold that one's continued employment could be made contingent upon his commission of a felonious act at the instance of his employer would be to encourage criminal conduct upon the part of both the employee and employer and serve to contaminate the honest administration of public affairs. This is patently contrary to the public welfare.").

143 *Id.*

144 Dorshkind v. Oak Park Place of Dubuque II, L.L.C., 835 N.W.2d 293, 300 (Iowa 2013).

legislation represents a clear public policy within the states that have enacted such legislation and, therefore, within those states, firing an employee for refusing to provide social media access information could constitute a wrongful discharge in violation of public policy. Of course, the majority of statutes already prohibit employers from doing just that;[145] however, three of the statutes—enacted by California, Illinois, and New Mexico—are silent in this regard.[146] Those same three states also do not provide for remedies within their statutes.[147] As such, employees fired for refusing to provide personal social media access information would have to rely upon a public policy argument for any relief.

On the other hand, the sporadic passage of employee password privacy legislation could actually diminish a public policy exception in the remaining states that have not enacted such legislation—in other words, it could be argued that at least thirty-eight states have had the opportunity to codify a clear public policy on the subject and have elected not to do so.

A review of the enacted and proposed employee password privacy legislation reveals similarities among them in a very broad sense, but significant inconsistencies in how they may be applied in different situations from state to state. For example, Abril et al. have published recent empirical data suggesting that while college-aged employees are "general[ly] ambivalen[t] regarding employer access" to their online social media profiles,[148] only approximately "one-third of [survey] respondents included their immediate supervisor as an online 'friend.'"[149] In addition, fifty-four percent of survey respondents "strongly or somewhat agreed that 'work life is completely separate from personal life, and what you do in one should not affect the other.'"[150] However, eighteen percent "of respondents reported a senior executive requested to [be] (and was) added as a friend or connection to an [online social network] profile."[151] Yet, "[e]ighty-

145 *See supra* note 26 and accompanying text.

146 *See generally* California: CAL. LAB. CODE § 980 (West 2014); Illinois: 820 ILL. COMP. STAT. 55/10 (2014); New Mexico: N.M. STAT. ANN. § 50-4-34(A) (West 2014) (lacking any provision prohibiting employers from firing employees for refusing to provide access to personal social media sites).

147 *See* discussion *supra* Part II.D.

148 Abril et al., *supra* note 121, at 98.

149 *Id.* at 102.

150 *Id.* at 103.

151 *Id.* at 107.

one percent of respondents considered it inappropriate for employees to be required to invite their supervisor to their [online social network] profile."[152] Abril et al. conclude that "it is likely a considerable number of employers may already have access to their employees' information on an" online social network.[153]

Only four of the enacted statutes directly or indirectly address employees "Friending" their employer.[154] While Arkansas expressly prohibits an employer from requiring or requesting that an employee or job applicant add an employee, supervisor, or administrator to the list or contacts associated with the employee's or applicant's social media account,[155] Colorado, Oregon, and Washington merely prohibit an employer from "compelling" an employee or job applicant to do so.[156] Abril et al.'s survey respondents reported requests by employers, not requirements, and the respondents complied because "it is clear that respondents were not willing to forgo participation in social networks to achieve privacy or separation of work and personal life. They displayed a strong desire to socialize, to interact, and to share truthful information about themselves on social networks."[157] If many young employees generally accept that supervisors, and even executives, expect to be made Friends with employees within their online social network worlds, is the employer engaging in overly-intrusive monitoring or merely just finding another way for workers, along the chain of command, to connect with each other? In either event, employers' asking to become employee's online Friends, to the extent it is occurring, is apparently now illegal in three, and possibly four, states.[158]

It was suggested earlier that the enacted employee password privacy legislation does not directly apply to scenarios such as those presented in *Pietrylo* and *Ehling* where employers have

152 *Id.*

153 *Id.* at 107–08.

154 *See supra* notes 19 and 25 and accompanying text (discussing statutes enacted by Arkansas, Colorado, Oregon, and Washington that prohibit employers from accessing an employee's or job applicant's social networking profile or account indirectly through any other person who is a social networking contact of the employee or applicant).

155 ARK. CODE ANN. § 11-2-124(b)(1)(B) (West 2014).

156 COLO. REV. STAT. § 8-2-127(2)(a) (2014); H.B. 2654, § 2(1)(b), 2013 Or. Laws ch. 204 (effective Jan. 1, 2014, amending OR. REV. STAT. ch. 659A); WASH. REV. CODE § 49.44.200(1)(c) (2014).

157 Abril et al., *supra* note 121, at 109.

158 *See supra* notes 155–56 and accompanying text.

viewed private online communications by allegedly "coercing" another employee to provide the employer access to those communications.[159] And consider whether Illinois's statute, which expressly excludes personal e-mail accounts,[160] would overrule cases such as *Pure Power Boot Camp*[161] and *Borchers*,[162] both of which found that a former employer had improperly accessed an employee's personal e-mail account?[163]

Finally, New Jersey's statute prohibits employers from requiring an individual to waive or limit any protection granted under its act as a condition of applying for or receiving an offer of employment.[164] "An agreement to waive any right or protection under this act is against the public policy of the State and is void and unenforceable."[165] Since the remaining eleven enacted statutes are silent in this regard,[166] does that mean employers can request employees and job applicants to waive their rights in those states under their respective employee password privacy statutes? This would completely negate the purpose of the legislation. The European Union, for example, recognizes the impracticality of true consent by an employee due to the power imbalance between the employer and the employee.[167] While U.S. jurisprudence does not formally adopt this approach, the EU's approach does point out the reality that when presented with such a consent agreement, most employees and job applicants will feel compelled to sign it.[168]

Courts generally enforce employee waivers of statutory rights,

159 *See supra* note 99 and accompanying text.

160 820 ILL. COMP. STAT. 55/10(4) (2014).

161 *See supra* notes 104–07 and accompanying text.

162 *See supra* notes 108–11 and accompanying text.

163 *Pure Power Boot Camp* and *Borchers* raise an additional issue. Both cases involved former employees, so arguably their former employers would no longer be considered "employers" for purposes of applying the legislation. Or would "employer" status relate back to when the employee actually worked for the employer since the employer's access to the account arose from the original employment relationship?

164 N.J. STAT. ANN. § 34:6B-7 (West 2014).

165 *Id*.

166 *See supra* notes 13 and 15 and accompanying text.

167 *See* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1027-28 (2011) (discussing that employee consent is actually "involuntary" due to the typical balance of power in the employment relationship).

168 *See, e.g.*, Waldman, *supra* note 94 (describing a "coercion" scenario for a "typical" job applicant).

particularly relating to employment separation agreements.[169] However, courts will not enforce such waivers against third-party public enforcement agencies, such as the Equal Employment Opportunity Commission.[170] It could be argued, therefore, that where an employee password privacy statute provides public-agency enforcement—such as in Colorado, Maryland, Michigan, and New Jersey[171]—waivers against enforcement by those agencies would be unenforceable; but waivers would otherwise be enforceable in the remaining eight states that have enacted employee password privacy statutes.

This article posits that the enacted employee password privacy statutes will have minimal practical effect for employees and job applicants for three reasons: (1) the conduct proscribed does not appear to be actually happening to any meaningful extent; (2) existing law, particularly the SCA, already provides legally enforceable prohibitions against a employer requiring or compelling an employee or job applicant to grant access to password-protected personal online accounts; and (3) an argument can be made that in at least eight of the states employers may be able to request that employees waive their rights under the legislation. The practical effect on employers will, however, be more profound. Multi-state employers are now faced with essentially twelve different sets of statutory requirements—with more to possibly come.[172]

In one sense, going forward employers can continue with the status quo: not requesting access information to employee's and job applicant's personal online accounts, except in specific instances. But it is those specific instances that may cause the most trouble for employers. As noted previously, it appears most of the exemptions in the enacted and proposed employee password privacy legislation are included merely to reaffirm that the prohibitions do not supersede already existing rights, such as

169 *See, e.g.*, E.E.O.C. v. SunDance Rehab. Corp., 466 F.3d 490, 499 (6th Cir. 2006) ("This court has upheld employees' waivers of claims under [the Age Discrimination in Employment Act], [the Equal Pay Act], and Title VII where the waiver was executed voluntarily and intelligently.").

170 *See id*. ("Whether a waiver of the right to file a charge with the E.E.O.C. is enforceable, however, is a different question. Given the importance of charge-filing to the E.E.O.C.'s investigatory and enforcement responsibilities, particularly under Title VII and [the Americans with Disabilities Act], . . . it may be that [a] charge-filing ban in [a] [s]eparation [a]greement . . . is unenforceable.") (emphasis omitted).

171 *See supra* notes 64–65 and accompanying text.

172 *See supra* note 15 and accompanying text.

supervising, monitoring, and maintaining the employer's information systems, or complying with various laws and regulations regarding employee online conduct.[173] But as a review of the enacted statutes reveals, there are significant inconstancies among the various laws regarding what conduct is exempted. Could it be argued that whichever exemptions exist prescribe the only circumstances in which an employer can require disclosure of an employee's personal online account access information? Could it then be argued that where an exemption does not exist, the employer would not have the access right, even if it might have existed without the legislation? Could it be argued that if a state omits an exemption, while other states include it, the former state's legislature intended that it not be a right of the employer?

As noted previously, the primary motivation underlying the employee password privacy legislation is to protect employees' and job applicants' personal online communications from the prying eyes of (prospective) employers—in other words, to protect one aspect of individual privacy.[174] "A statute should represent 'timely responsiveness'; that is, it should be responsive to the needs of the people—it should be protective of their interests. . . ."[175] But this legislation appears to be responsive not to the needs of the people—employees, current and prospective, and employers alike—but to a media meme that had very little factual basis and a "me-to" attitude among the states that if other states are passing this legislation then they ought to too. Ultimately, the enacted and proposed employee password privacy legislation is an answer in search of a problem.[176] The result is legislation that raises more questions than it answers.

---

[173] *See supra* note 146 and accompanying text.

[174] *Cf.* Kenneth N. Waltz, *Kant, Liberalism, and War*, 56 AM. POL. SCI. REV. 331, 332 (1956) ("The purpose of legislation is negative: to 'hinder hindrances' to freedom so that each may enjoy his antecedently existing rights unmolested.").

[175] Howard Newcomb Morse, *Theories of Legislation*, 14 DEPAUL L. REV. 51, 51 (1964).

[176] *See* Hyman, *supra* note 77.